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

Інститут електроенергетики
Факультет інформаційних технологій
Кафедра безпеки інформації та телекомунікацій

ПОЯСНЮВАЛЬНА ЗАПИСКА
кваліфікаційної роботи ступеня магістра

студента Гулої Жанни Володимирівни
(ПІБ)

академічної групи 125м-19-1
(шифр)

спеціальності 125 Кібербезпека
(код і назва спеціальності)

спеціалізації _____

за освітньо-професійною програмою Кібербезпека
(офіційна назва)

на тему Ризико-орієнтований підхід до забезпечення кіберстійкості з використанням інтелектуальних систем аналітики

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

Рецензент				

Нормоконтроль	**ст. в. Тимофєєв Д.С.**			

Дніпро
2020

ЗАТВЕРДЖЕНО:
завідувач кафедри
безпеки інформації та телекомунікацій
_____ д.т.н.,проф. Корнієнко В.І.
«____» _____2020 року

ЗАВДАННЯ
на кваліфікаційну роботу
ступеню _____магістра_____
(бакалавра, спеціаліста, магістра)

студенту Гулій Жанні Володимирівні **академічної групи** 125м-19-1
(прізвище та ініціали) (шифр)

спеціальності 125 Кібербезпека_____
спеціалізації _____
за освітньо-професійною програмою Кібербезпека_____
на тему Ризико-орієнтований підхід до забезпечення кіберстійкості з використанням інтелектуальних систем аналітики.

Затверджену наказом ректора НТУ «Дніпровська політехніка» від 22.10.2020 р. №888-с

Розділ	Зміст	Термін виконання
Розділ 1	Процес управління ризиками кібербезпеки з використанням інтелектуальних систем аналітики	20.11.2020
Розділ 2	Мінімізація ризиків, пов'язаних із забезпеченням кіберстійкості	3.12.2020
Розділ 3	Економічний розділ	7.12.2020

Завдання видано _____ Тимофєєв Д.С.

Дата видачі завдання: 01.09.2020

Дата подання до екзаменаційної комісії: 07.12.2020

Прийнято до виконання _____ Гула Ж. В.

РЕФЕРАТ

Пояснювальна записка: *108* с., *13* рис., *10* табл., *4* додатки, *44* джерела.

Об'єкт дослідження: інтелектуальні системи аналітики.

Предмет дослідження: використання інтелектуальних систем аналітики з метою забезпечення кіберстійкого стану підприємства.

Метою дипломної роботи є: забезпечення кіберстійкості інформаційних систем підприємства з використанням інтелектуальних систем аналітики.

У першому розділі дипломної роботи розглянуто процес управління ризиками кібербезпеки з використанням інтелектуальних систем аналітики. Проаналізовано основні загрози безпеці інформації та тенденції забезпечення протидії ризикам, пов'язаними із забезпеченням кіберстійкості. Розглянуто існуючі підходи до реалізації інтелектуальних систем аналітики.

У другому розділі дипломної роботи проведено порівняння типових рішень з аутсорсингу послуг з кібербезпеки, виконано аналіз характеристик відомих рішень SIEM. Розглянуто процес мінімізації ризиків, пов'язаних із забезпеченням кіберстійкості шляхом впровадження SIEM на підприємстві. Розроблено алгоритм вибору функціональної SIEM та запропоновано рекомендації для провадження системи, критерії угоди про рівень обслуговування.

У третьому розділі дипломної роботи обґрунтовано економічну ефективність запропонованого методу при впровадженні його на типовому підприємстві.

Ключові слова: КІБЕРСТІЙКІСТЬ, ІНТЕЛЕКТУАЛЬНА СИСТЕМА АНАЛІТИКИ, РИЗИК, УПРАВЛІННЯ РИЗИКАМИ, MSSP, MDR, SIEM, SLA.

ABSTRACT

Explanatory note: *108* pages, *13* figures, *10* tables, *4* appendices, *44* sources.

Object of study: intelligent analytics systems.

Research subject: the use of intelligent analytics systems for ensuring the cyber resilience of the enterprise.

The purpose of the work is to warrant the cyber resilience of enterprise information systems through deploying intelligent analytics systems.

The first section of the thesis examines the cybersecurity risk management process using intelligent analytics systems. The main threats to information security and trends in countering the risks associated with ensuring cyber resilience have been analyzed. The existing approaches to the implementation of intelligent analytics systems are considered.

The second section of the thesis compares typical solutions for outsourcing cybersecurity services, analyzes the characteristics of known SIEM solutions. The process of minimizing the risks associated with ensuring cyber resilience through the implementation of SIEM in the enterprise is considered. An algorithm for choosing a functional SIEM has been developed and recommendations for implementing the system, criteria for a service level agreement have been proposed.

In the third section of the thesis, the economic efficiency of the proposed method is substantiated when it is implemented in a typical enterprise.

Keywords: CYBER RESILIENCE, INTELLIGENT ANALYTICAL SYSTEM, RISK, RISK MANAGEMENT, MSSP, MDR, SIEM, SLA.

СПИСОК УМОВНИХ СКОРОЧЕНЬ

ДСТУ – державний стандарт України

ІТ – інформаційні технології

ІТС - інформаційно-телекомунікаційна система

ОТ - операційні технології

СУІБ - системи управління інформаційною безпекою

ШІ - штучний інтелект

ATT&CK - (англ. adversarial tactics, techniques, and common knowledge) - тактики, прийоми та загальновідомі знання супротивників

APT (англ. advanced persistent threat) - розвинена стійка загроза

APM (англ. alerts per month) - сповіщення/тривоги на місяць

BCMS (анг. business continuity management system) - управління безперервністю бізнесу

BCP (англ. business continuity planning) - планування безперервності бізнесу

BIA (англ. business impact analysis) - аналізу впливу на бізнес

BYOD (англ. bring your own device) - принеси свій власний пристрій

COBIT (англ. control objectives for information and related technologies) - цілі управління інформаційними та суміжними технологіями

COSO (англ. the committee of sponsoring organizations of the Treadway commission) - комітет спонсорських організацій комісії Тредвей

CRE (англ. custom rules engine) - механізм спеціальних правил

CSRM (англ. cybersecurity risk management) - управління ризиками кібербезпеки

DRP (англ. disaster recovery plan) - план ліквідації наслідків катастрофи

ENISA (англ. The European Union Agency for Cybersecurity) - Агентство Європейського Союзу з кібербезпеки

EPS (англ. events per second) - події в секунду

ERM (англ. enterprise risk management) - управління ризиками підприємств

ERR (англ. enterprise risk register) - реєстр ризиків підприємства

FFIEC (англ. Federal Financial Institutions Examination Council) - Екзаменаційна рада Федеральних фінансових установ

HIDS (англ. host-based intrusion detection system) - система виявлення вторгнень на основі хоста

IAM (англ. identity and access management) - управління ідентифікацією та доступом

ICS (англ. industrial control systems) - промислові системи управління

IDS (англ. intrusion detection system) - система виявлення вторгнень

IEC (англ. International Electrotechnical Commission) - Міжнародна електротехнічна комісія

IOC (англ. indicators of compromise) - індикатори порушень

IoT (англ. Internet of Things) - інтернет речей

ISACA (англ. Information Systems Audit and Control Association) - асоціація контролю і аудиту інформаційних систем

ISO (англ. International Organization for Standardization) - Міжнародна організація стандартизації

MDR (англ. Managed Detection and Response) - служба керованого виявлення та реагування

MITRE (англ. Massachusetts Institute of Technology Research & Engineering) - Массачусетський інститут технологічних досліджень та інженерії

MSSP (англ. Managed Security Service Provider) - провайдер керованих послуг безпеки

NAC (англ. network access control) - контроль доступу до мережі

NIST (англ. National Institute of Standards and Technology) - Національний інститут стандартів і технологій

OPM (англ. offenses per month) - правопорушення/інциденти на місяць

OTX (англ. open threat exchange) - відкритий обмін загрозами

PCI DSS (англ. Payment Card Industry Data Security Standard) - Стандарт безпеки даних про платіжну картку

PDCA (англ. Plan, Do, Check, Act) - Планування - Реалізація - Перевірка - Дія (ПРПД)

PLC (англ. programmable logic controllers) - програмовані логічні контролери

SaaS (англ. Software as a service) - програмне забезпечення як послуга

SCADA (англ. Supervisory Control And Data Acquisition) - диспетчерське управління і збір даних

SEM (англ. Security Event Management) - управління подіями безпеки

SIEM (англ. Security Information and Event Management) - управління інформаційною безпекою та подіями

SIM (англ. Security Information Management) - управління інформацією про безпеку

SLA (англ. Service Level Agreements) - угоди про рівень обслуговування

SOAR (англ. Security Orchestration, Automation and Response) - інструментування безпеки, автоматизація та реагування

SOC (англ. Security Operation Center) - операційний центр безпеки

SoW (англ. statement of work) - звіт про роботу

STIX (англ. structured threat information eXpression) - структуроване висловлення інформації про загрози

TAXII (англ. trusted automated eXchange of intelligence information) - довірений автоматизований обмін розвідувальною інформацією

TTP (англ. tactics, techniques and procedures) - тактики, техніки та процедури

UEBA (англ. user and entity behavior analytics) - аналітика поведінки користувачів та сутності

VPN (англ. virtual private network) - віртуальна приватна мережа

ЗМІСТ

ВСТУП

Актуальність роботи. За останні роки кількість можливих загроз та ризиків інформаційної безпеки зросла у десятки разів. Можливість забезпечення кібербезпеки організацій ускладнюється з кожним роком наразі із еволюцією відповідних загроз. Неможливість створення абсолютно захищеної системи, призводить до використання підходу забезпечення кіберстійкості як можливості мінімізації ризиків.

Кіберстійкість стає необхідною умовою успішності міжнародних компанії, діяльність яких пов'язана з інформаційними технологіями чи обробкою персональних даних. Концепція має міжнародне значення, її важливість складно переоцінити, адже забезпечення стійкого стану за адекватних витрат використовуються на всіх рівнях забезпечення кіберзахисту.

Управління ризиками шляхом забезпечення кіберстійкості здатне перекрити критичні ризики підприємства у актуальні моменти часу. Недостатня захищеність інформаційних систем може призвести до тяжких результатів – аварій ІТС, втрати конфіденційних даних, розкриттю комерційної таємниці, санкціям регуляторів, втраті репутації чи загальній втраті функціональності підприємства.

Через відсутність необхідної нормативно-правової бази на даний момент ринок послуг інформаційної безпеки задля забезпечення кіберстійкості в Україні не сформований, проте попри складне економічне та політичне становище ІТ-сфера країни стрімко розвивається, тому варто очікувати, що дана вимога буде користуватися попитом.

Сучасний стан проблеми. Сьогодні окрім стандартних проблем захищеності інформаційно-телекомунікаційних систем, таких як віруси, шпигунське програмне забезпечення, фішинг, шкідливі вкладення електронної пошти, небезпеку представляють розвинуті атаки, що складаються з декількох фаз та вимагають попереднього планування. Зловмисниками демонструється загальна трудомістка підготовка розвинених загроз, що результує у більш масштабних

втратах для організацій будь-якого напрямку функціонування - від медицини, сектору фінансів та страхування до роздрібної торгівлі та транспортування.

Так у 2019 році багато атак було здійснено атаку на інфраструктури різних профільних підприємств, що понесли багатомільйонні збитки, серед яких Orvibo, LightInTheBox, First American, Facebook та Zynga. Також спостерігається збільшення атак на операційні технології різноманітних об'єктів.

Дослідженням проблеми забезпечення кіберстійкості займалися такі установи та організації, як NIST, ISO, IEC, Open Group, ISACA та інші. Результати їх роботи створюють теоретичну основу вивчення питання підходів забезпечення кіберстійкого стану організації. Більш детального аналізу потребують тенденції актуальних загроз, сучасних підходів до управління ризиками та можливостей забезпечення кіберстійкості організацій за збалансованих витрат.

Метою дипломної роботи є забезпечення кіберстійкості інформаційних систем підприємства з використанням інтелектуальних систем аналітики.

Для досягнення відповідної мети необхідно дослідити аспекти стратегії управління ризикам, пов'язаними із забезпеченням кіберстійкості та методи, що використовуються для її забезпечення.

Об'єктом дослідження є застосування інтелектуальних систем аналітики для управління ризиками.

Предметом дослідження є функції кіберстійкості та методи її забезпечення.

РОЗДІЛ 1 ПРОЦЕС УПРАВЛІННЯ РИЗИКАМИ КІБЕРБЕЗПЕКИ З ВИКОРИСТАННЯМ ІНТЕЛЕКТУАЛЬНИХ СИСТЕМ АНАЛІТИКИ

1.1 Актуальність впровадження управління ризиками кібербезпеки

Визначення головних тенденцій потенційних загроз є фундаментом для адекватного та своєчасного проведення аналізу ризиків для підприємства, оскільки визначає можливий вплив реалізацій загроз для функціонування підприємства.

Для визначення тенденцій загроз необхідно виконати зведений аналіз головних напрямків реалізації використання вразливостей систем та можливих актуальних загроз.

З цією метою розглядаємо річні звіти різних компаній-постачальників послуг у сфері кібербезпеки, а також звіти незалежних представників організацій.

За показниками системного аналітичного звіту The European Union Agency for Cybersecurity (англ. ENISA - Агентство Європейського Союзу з кібербезпеки) щодо середовища кіберзагроз [31] визначені тенденції:

1. Поверхня атак в кібербезпеці продовжує розширюватися, оскільки відбувається входження у новий етап цифрової трансформації.

2. Після пандемії COVID-19 з'явиться нова соціальна та економічна норма, яка ще більше буде залежати від безпечного та надійного кіберпростору.

3. Використання платформ соціальних медіа для цілеспрямованих атак є серйозною тенденцією і охоплює різні домени та типи загроз.

4. Чітко цілеспрямовані та постійні атаки на цінні дані ретельно плануються та виконуються суб'єктами, що фінансуються державами.

5. Масово розподілені атаки з короткою тривалістю та широким впливом використовуються з різними цілями, такими як крадіжка облікових даних.

6. Мотивація більшості кібератак все ще є фінансовою.

7. Програми-вимагачі (англ. Ransomware) залишаються широко розповсюдженими з значними наслідками для багатьох організацій.

8. Багато інцидентів кібербезпеки залишаються непоміченими або виявляються довго.

9. Завдяки більшій автоматизації безпеки організації будуть демонструвати більше готовності, використовуючи інформацію про кіберзагрози як свою здатність.

10. Кількість жертв фішингу продовжує зростати, оскільки він використовує людський фактор, що є найслабшою ланкою.

З урахуванням усіх змін, що спостерігаються в ландшафті кіберзагроз, та змін, створених пандемією COVID-19, залишається довгий шлях, перш ніж кіберпростір стане надійним та безпечним середовищем.

Відповідно до ENISA 15 головних загроз у 2020 році становлять техніки, наведені на рисунку 1.1.

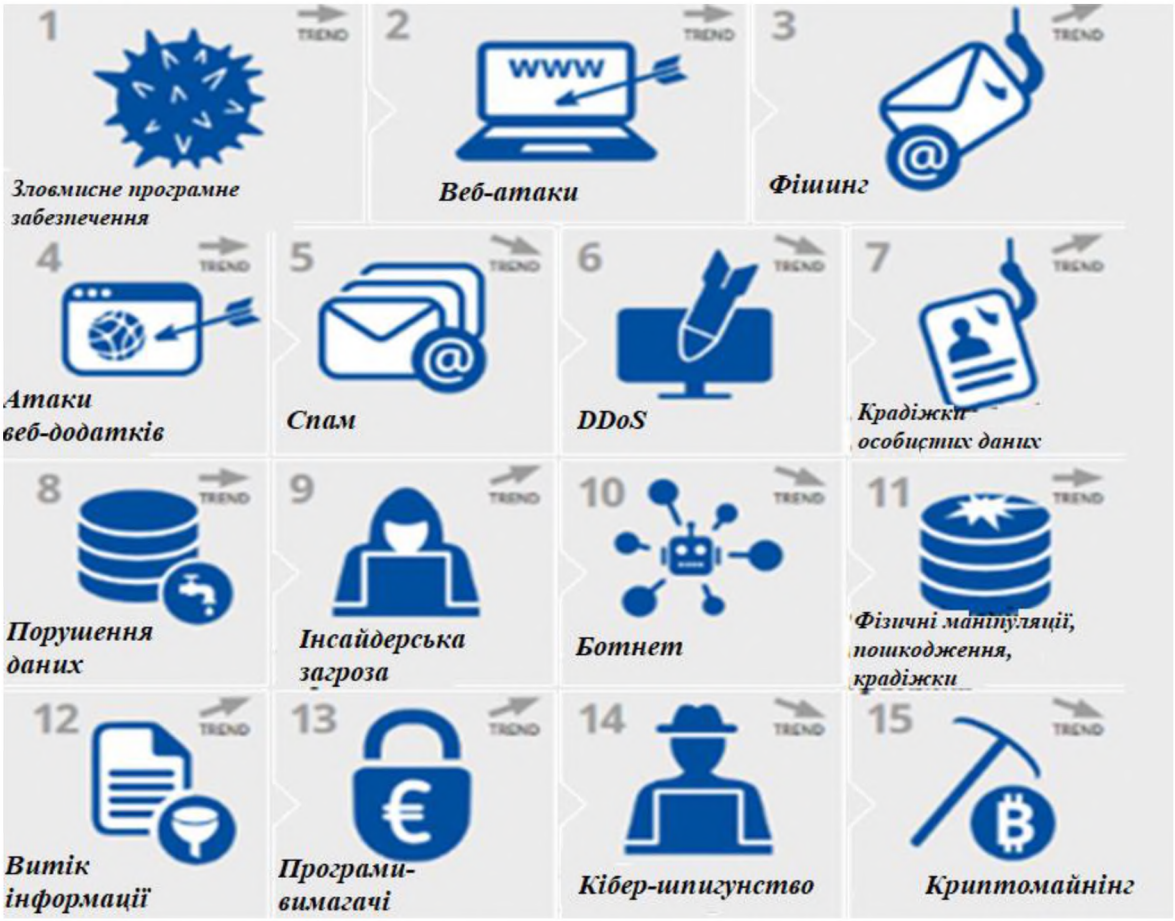

Рисунок 1.1 - Тенденції технік, що застосовуються кіберзлочинцями у 2020 році

ENISA також пропонує картографування ландшафту актуальних загроз на сьогодні. Експлуатація кіберзлочинцями стійких загроз поточної глобальної пандемії COVID-19 зображена на рисунку 1.2.

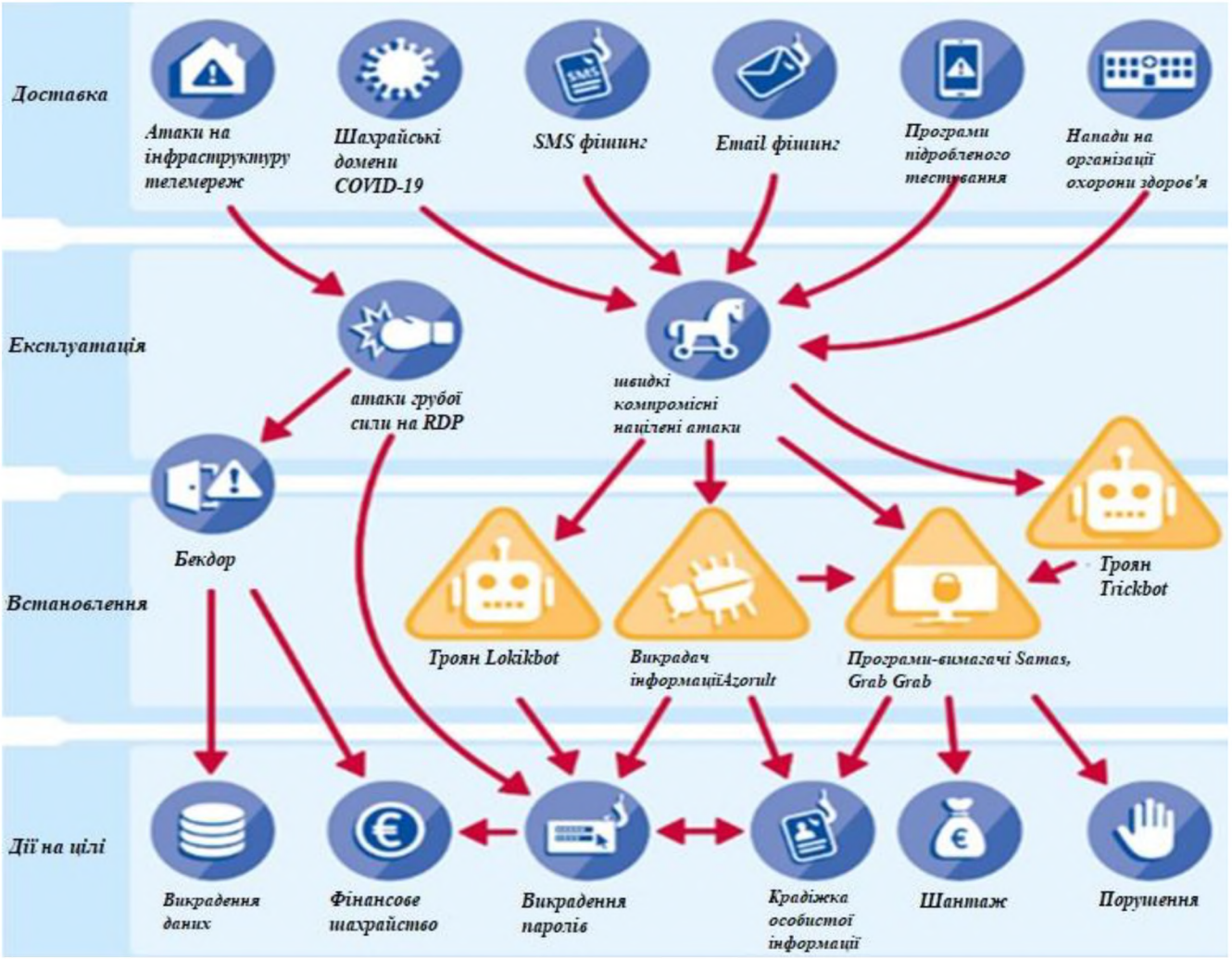

Рисунок 1.2 - Ландшафт актуальних загроз на час поточної глобальної пандемії COVID-19

Основними тенденціями за Check Point Software Security report [7] є:

1. Різноманітність фішингових атак. Окрім електронної пошти, кіберзлочинці використовують обмін текстовими повідомленнями на мобільні телефони або використання повідомлень у соціальних мережах та на ігрових платформах.
2. Еволюція атак мобільного шкідливого програмного забезпечення. У першій половині 2019 року кількість атак зловмисного програмного забезпечення

мобільного банкінгу зросла. Таке програмне забезпечення може викрадати платіжні дані, облікові дані та кошти з банківських рахунків жертв.

3. Зростання кіберстрахування. Андеррайтери продають більше полісів кіберстрахування для підприємств та державних установ. Страхові компанії можуть направляють страхувальників виплачувати викуп, оскільки це, як правило, дешевше, ніж необхідність оговтуватися від програм-вимагачів.
4. Ризиковий бізнес із пристроями Internet of Things (англ. IoT - Інтернет речей) - із розвитком мереж 5G, використання підключених пристроїв IoT збільшується. Пристрої IoT є слабкою ланкою безпеки - важко отримати видимість таких пристроїв, також такі пристрої не мають безпеки у цілому.
5. Штучний інтелект (ШІ) прискорює реакції безпеки - значно прискорює виявлення нових загроз та відповіді на них, проте кіберзлочинці також починають користуватися тими ж методами, з ціллю дослідження мережі, знаходження вразливих місць та розроблення більш ухильні шкідливі програми.
6. Хмарні технології. Зростає залежність від інфраструктури загальнодоступних хмар, схильність підприємств до ризику перебоїв. Це змушує організації шукати рішення в існуючих центрах обробки даних та хмарних розгортаннях. Неправильна конфігурація хмарних ресурсів є причиною номер один для атак на хмарні інфраструктуру, наразі також спостерігається збільшення кількості атак, спрямованих безпосередньо на постачальників хмарних послуг.

Статистичні дані категорій кібератак за регіонами за звітами різних передових компаній як «Check Point Software Security report» [7], надають змогу побачити, що у глобальному масштабі переважають криптомайнери, бот-мережі та атаки на мобільні пристрої. У контексті підприємства, такі загрози мають великий вплив, оскільки ціллю нападників є отримання вигоді від ресурсів інформаційних систем підприємства.

Атаки на мобільні пристрої зазнають розвитку через збільшення Bring your own device (англ. BYOD - Принеси свій власний пристрій). У випадку BYOD,

підприємство не має змоги контролювати властивості та характеристики пристроїв робітників, проте може зменшити вплив таких атак за допомогою сегментації мережі та нових технологій, як Network Access Control (англ. NAC - Контроль доступу до мережі).

Захист від потенційного порушення мережі зловмисниками, що надалі може стати результатом ботнету або криптомайнінгу повинен забезпечуватися не лише встановленням «бар'єрів», але і постійним моніторингом систем.

Порівнюючи річні звіти з кіберзагроз Sonicwall, IBM (International Business Machines) X-Force, Check Point Software та McAfee [37], визначаємо наступні статистичні тенденції.

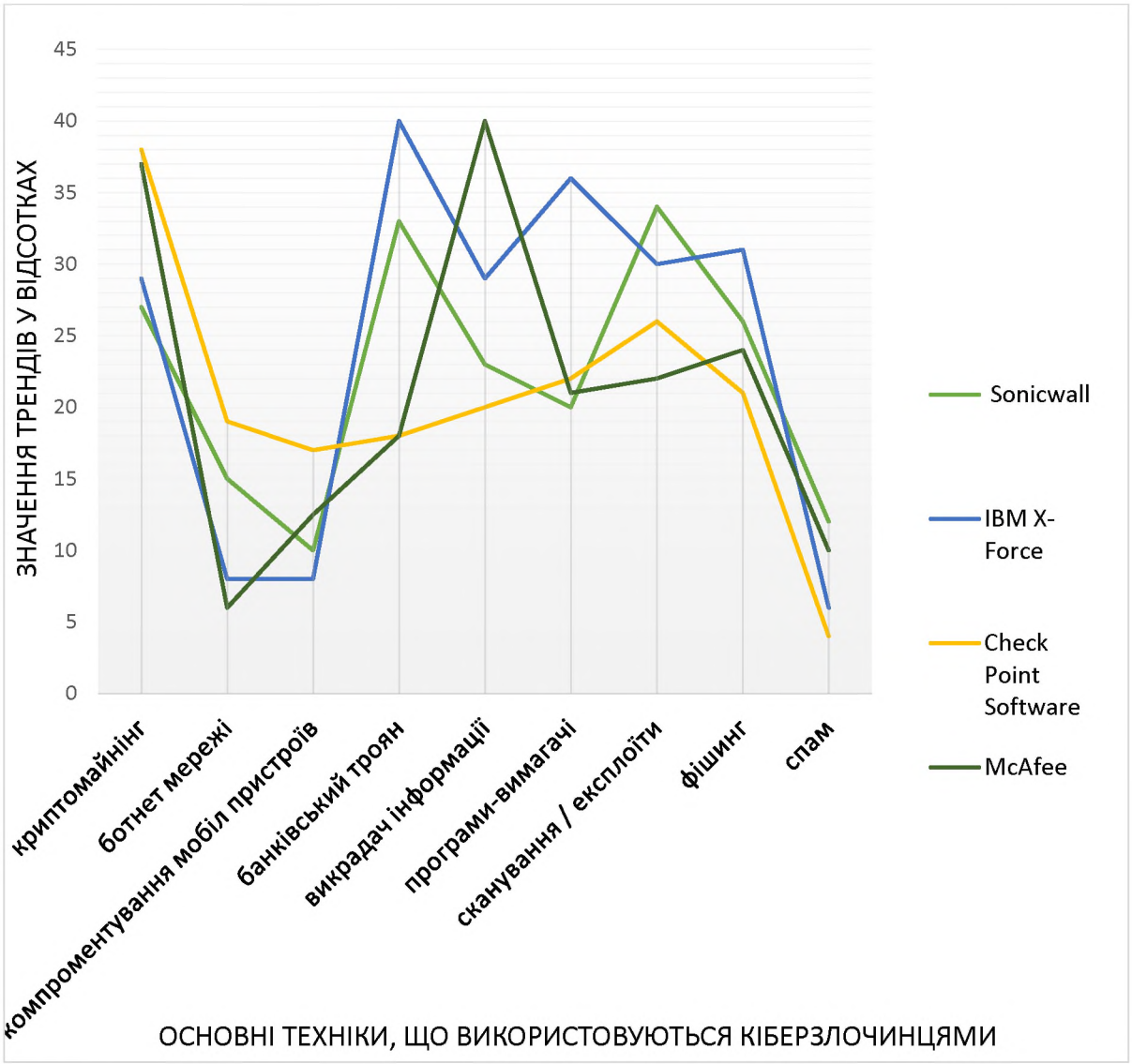

Рисунок 1.3 - Тенденції основних технік кібератак

Найбільший розвиток набувають криптомайнери, банківські трояни, викрадачі інформації, програми-вимагачі та експлойти/ веб-атаки. Також розвитку набувають загрози шифрування та впровадження зловмисного програмного забезпечення у Інтернеті речей. Це, в свою чергу, визначає необхідність постійного моніторингу інформаційно-телекомунікаційної системи (ІТС) підприємства і своєчасне реагування на можливі інциденти.

Витоки даних несуть великі збитки як для репутації підприємств, так і грошові втрати. Дані [6] визначають серйозні інциденти витоків даних у 2019 році, наведених у таблиці нижче.

Таблиця 1.1 - Найбільші інциденти витоків даних у 2019 році за SonicWall

Установа	***Категорія***	***Дата повідомлення***	***Викрито,*** *дол. США*
Orvibo	Інтернет речей	01.07.2019	2 млрд
LightInTheBox	Інтернет магазин	16.12.2019	1,6 млрд
Verifications.io	Бізнес	29.03.2019	980 млн
First American	Банківська справа	25.05.2019	885 млн
Collection #1	Технології	17.01.2019	773 млн
Facebook	Соціальні мережі	21.03.2019	600 млн
Facebook	Соціальні мережі	02.04.2019	540 млн
Facebook	Соціальні мережі	14.12.2019	267 млн
Zynga	Розваги	12.09.2019	170 млн
Canva	Освіта	24.05.2019	139 млн

Визначаючи тенденції атак на операційні технології (ОТ) підприємств, дані IBM X-Force вказують на збільшення загроз промисловим системам управління (англ. ICS - Industrial control systems) та аналогічним активам ОТ, що зросли більш ніж на 2000 відсотків з 2018 року [9].

Більшість виявлених атак, зосереджено навколо використання комбінації відомих вразливостей в апаратних компонентах Supervisory Control And Data Acquisition (англ. SCADA - диспетчерське управління і збір даних) та ICS.

Перекриття між IT-інфраструктурою та OT, такі як programmable logic controllers (англ. PLC - програмовані логічні контролери) та ICS, продовжують представляти ризик для організацій, які покладаються на гібридні інфраструктури. На рисунку 1.4 зображено динаміку кількості атак в цільовій інфраструктурі.

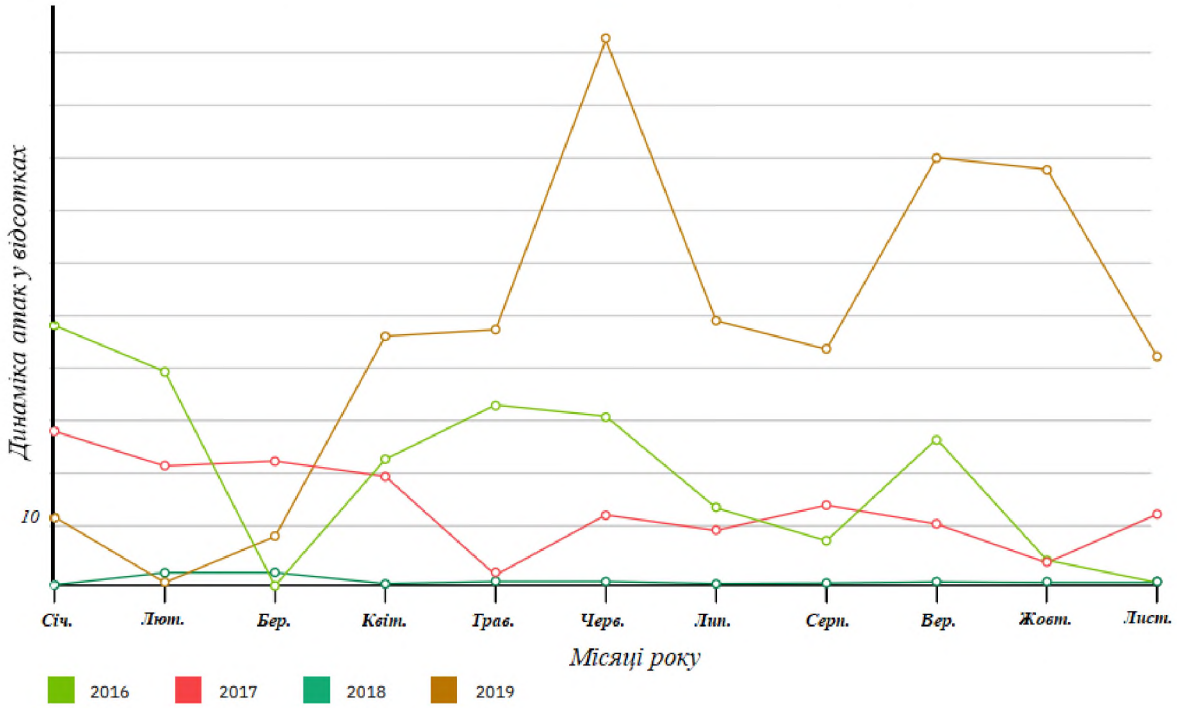

Рисунок 1.4 - Динаміка кількості атак в цільовій інфраструктурі операційних технологій за 2016-2019 роки

Аналізуючи основні галузі промисловості на які націлено кібератаки за даними звітів IBM X-Force, McAfee та FireEye Mandiant [8], визначаються тенденції, зображені на рисунку 1.5.

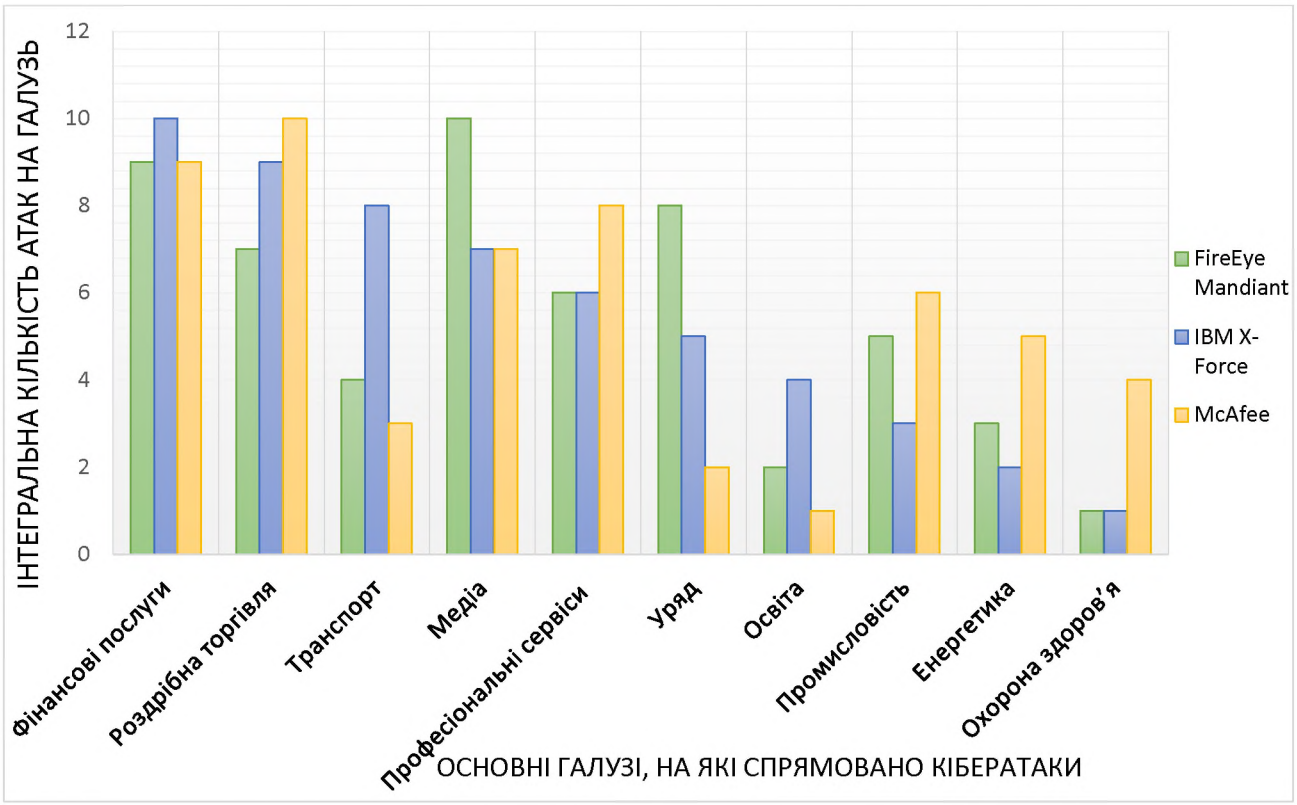

Рисунок 1.5 - Основні галузі, на які спрямовано кібератаки

Таким чином, найбільш націленими галузями вважаються:

- сектор фінансів та страхування був найбільш атакованою галуззю протягом чотирьох років. Цілком ймовірно, що фінансово мотивовані кіберзлочинці становлять найбільшу частину активних суб'єктів кіберзагрози;
- роздрібна торгівля була другою серед найбільш атакованих з усіх галузей. Найбільш поширеним типом акторів загроз, націлених на роздрібні організації, є фінансово мотивовані кіберзлочинці, які націлені на галузь, щоб отримати інформацію, що ідентифікує споживача, дані платіжних карток, фінансові дані, історію покупок та інформацію про програму лояльності;
- медіа та розваги включають гучні підгалузі, такі як телекомунікації, а також компанії, що виробляють, обробляють та розповсюджують засоби масової інформації та розваги. Індустрія засобів масової інформації та розваг є цільовою метою для кібератак, які прагнуть впливати на громадську думку, контролювати інформаційні потоки або захищати репутацію своєї організації чи країни;

- транспортування вважається частиною критичної інфраструктури будь-якої країни. Компанії в цьому секторі мобілізують економіку за допомогою основних видів транспорту - наземний, морський та повітряний транспорт, як для промислових, так і для споживчих послуг. Рейтинг підкреслює зростаючу привабливість даних та інфраструктури, що експлуатуються транспортними компаніями. Ці активи приваблюють як кіберзлочинців, так і суб'єктів загрози національної держави. Інформація, що зберігається транспортними компаніями, є привабливою метою, яка може включати особисту інформацію, біографічну інформацію, номери паспортів, інформацію про програму лояльності, дані платіжних карток та маршрути подорожей.

Таким чином, можна зробити висновок, що ландшафт загроз для підприємства будь-якої галузі та розміру зростає, збільшуються атаки, що мають зовнішнє походження, з метою порушення внутрішнього обладнання, що надалі може служити для безлічі різних цілей, починаючи від використання заліза у власних цілях нападників до викрадення конфіденційно інформації підприємства.

Комплексна протидія загрозам реалізується шляхом впровадження процесу управління ризиками. Управління ризиками - це виявлення, оцінка та визначення пріоритетності ризиків [4], (визначених в ДСТУ ISO/IEC 27005:2015 як вплив невизначеності на цілі) з подальшим узгодженим та економним використанням ресурсів для мінімізації, моніторингу та контролю ймовірності чи впливу нещасних подій або максимально можливості реалізації.

Ризики можуть виникати з різних джерел, включаючи невизначеність на фінансових ринках, загрозу від невдач проекту (на будь-якій фазі проектування, розробки, виробництва чи підтримання життєвих циклів), юридичних зобов'язань, кредитного ризику, аварії, природних причин та катастроф, навмисних нападів від супротивника чи подій невизначеної чи непередбачуваної першопричини.

Існує два типи подій - негативні події можна класифікувати як ризики, тоді як позитивні події класифікуються як можливості. Стандарти управління ризиками були розроблені різними міжнародними установами.

Більшість юрисдикцій впроваджують ключові концепції міжнародних та галузевих стандартів, таких як NIST SP 800-39, ISO/IEC 27005, ISO 31000, COBIT та інші [23] .

Методи, визначення та цілі сильно відрізняються залежно від того, чи є метод управління ризиками в контексті конкретної бізнес операції - управління проектами, безпекою, машинобудуваннями, промисловими процесами, фінансовими портфелями, актуальними оцінками або громадським здоров'ям та безпекою.

Різні компанії стикаються з різними видами та рівнями загроз залежно від галузі та інших конкретних для компанії факторів (таких як розмір та структура організації). Не існує єдиного підходу до створення плану управління кібер-ризиками. За умови, що компанія починає з нуля і ще не має стратегії управління ризиками в кібербезпеці, National Institute of Standards and Technology (англ. NIST - Національний інститут стандартів і технологій) пропонує вирішення – Фреймворк кібербезпеки (англ. Cybersecurity Framework).

Проте навіть з використанням Cybersecurity Framework, компаніям необхідно пристосувати контроль та процеси безпеки до унікальних потреб їх конкретних галузей бізнесу або функцій.

Незалежно від галузі, функції або будь-якої структури процесна модель управління ризиками в кібербезпеці організації, визначається стандартом ДСТУ ISO/IEC 27005:2015 [4]. Оскільки процеси управління ризиками є складовою частиною загальної системи організації, для їх опису використовується також процесна модель, яка визначається чотирма етапами: Планування - Реалізація - Перевірка - Дія (ПРПД) (англ. PDCA – Plan, Do, Check, Act), що відображає стандартний цикл управління, вперше описаний в роботах Демінга.

На етапі планування визначаються політика, контекст і методологія управління ризиками, інвентаризуються активи і визначається їх цінність, формуються профілі загроз і вразливостей, оцінюється ефективність контрзаходів і проводиться обробка ризиків. Керівництво організації приймає відповідні рішення і затверджує план обробки ризиків.

На етапі реалізації проводиться впровадження необхідних механізмів безпеки та інші дії по реалізації плану обробки ризиків, які можуть включати в себе укладання договорів страхування, угод про рівень сервісу, коригування планів розвитку бізнесу з метою уникнення певних ризиків.

На етапі перевірки відслідковуються функціонування реалізованих механізмів безпеки, контролюється зміна факторів ризику (активів, погроз, вразливостей), проводяться аудити і виконуються різні контролюючі процедури.

На етапі дії здійснюється вдосконалення процесів управління ризиками за результатами моніторингу та аудиту, в разі необхідності, переглядаються певні ризики, використовуванні підходи і методи їх оцінки, вносяться зміни в нормативну і операційну документацію організації, уточнюється контекст управління ризиками. Постійне вдосконалення є суттєвою частиною безперервних дій з управління ризиками, що вживаються з метою підвищення ефективності впроваджених механізмів контролю для досягнення цілей, які були встановлені для системи управління інформаційною безпекою (СУІБ).

Керівництво будь-якої організації, незалежно від того, працює вона в державному секторі чи в приватному секторі, має на меті досягнення своїх цілей для моніторингу та зменшення ризиків. Контроль ризиків досягається шляхом ефективного управління ними, а саме впровадженням адекватної системи управління ризиками.

Управління ризиками є важливою концепцією, пов’язаною з безпекою та фінансовою цілісністю організації, а оцінка ризиків є важливою частиною її стратегічного розвитку.

Процес управління ризиками є постійним, і результати його втілюються у рішеннях щодо прийняття, зменшення або усунення ризиків, що впливають на досягнення цілей. Мета полягає в оптимізації ризику організації для запобігання втрат, уникнення загроз та використання можливостей. Досягнення очікуваного результату діяльності відбувається під впливом випадкових факторів, що супроводжують організацію на всіх етапах розвитку, незалежно від сфери діяльності.

Імовірність виникнення ризику - можливість того, що ризик матеріалізується, і його можна оцінити або визначити шляхом вимірювання, коли характер ризику та наявна інформація дозволяють таку оцінку.

Вплив ризику є наслідком результатів (цілей), коли ризик матеріалізується. Якщо ризик представляє загрозу, наслідки для результатів негативні, а якщо ризик представляє можливість, наслідки позитивні.

Управління ризиками - превентивне ставлення до усунення або обмеження збитків, якщо існує можливість реалізації ризику, а саме процес виявлення, аналізу та реагування на потенційні ризики організації.

Покладання виключно на неформальний аналіз ризику може погіршити ефективну підтримку прийняття рішень щодо управління ризиками кібербезпеки. Для більш точної оцінки доступний широкий спектр методологій аналізу ризиків, включаючи NIST SP 800-30 [18], Міжнародну електротехнічну комісію (IEC) 31010: 2019 [13] та стандарти Open FAIR Open Group [25].

Методи аналізу ризику включають [39]:

- якісний аналіз базується на призначенні дескриптора, такого як низький, середній або високий. Шкала може бути сформована або скоригована відповідно до обставин, а різні описи можуть використовуватися для різних ризиків. Якісний аналіз корисний як первинна оцінка або коли слід враховувати нематеріальні аспекти ризику. Для поліпшення якості якісного аналізу можна використовувати значення та дані із зовнішніх джерел, таких як галузеві орієнтири або стандарти, показники з подібних попередніх сценаріїв ризику або висновки інспекцій та оцінок;
- кількісний аналіз включає числові значення, які присвоюються як впливу, так і ймовірності. Ці значення базуються на статистичних ймовірностях та монетизованій оцінці збитків. Якість аналізу залежить від точності призначених значень та використовуваних статистичних моделей. Наслідки можуть виражатися у фінансовому, технічному чи людському впливі.

Перевага впровадження системи управління ризиками в організації полягає в забезпеченні економічної ефективності. Для досягнення цієї вимоги керівництво

організації несе відповідальність повідомляти про ризики, з якими вони стикаються, та належним чином управляти ними, щоб уникнути наслідків для їх матеріалізації.

Переваги впровадження процесу управління ризиками включають:

- більша ймовірність досягнення цілей суб'єкта господарювання;
- вдосконалення розуміння ризиків та їх наслідків;
- підвищена увага до основних питань;
- обмеження наслідків шляхом впровадження адекватного внутрішнього контролю;
- певна прийнята толерантність до ризику;
- ширша інформація для прийняття адекватних рішень з точки зору ризиків.

Сьогодні моніторинг та управління ризиками у всіх аспектах у світі стає дедалі важливішим. Система управління ризиками будується на компонентах внутрішнього контролю / управління, структурованих відповідно до моделей COSO (англ. The Committee of Sponsing Organisations of the Treadway Commission - Комітет спонсорських організацій Комісії Тредвей) [10], за п'ятьма елементами, реалізація яких передбачає створення інструментів / пристроїв внутрішнього контролю та функціонування за призначенням.

Ці компоненти визначені як:

- середовище контролю, специфічне для організації, є тим, яке встановлює основи системи внутрішнього контролю, впливаючи на обізнаність працівників щодо контролю та представляє основу для інших компонентів;
- оцінка ризиків здійснюється керівництвом, здійснюється як на корпоративному, так і на рівні діяльності та включає виявлення та аналіз ризиків, що впливають на досягнення цілей;
- контрольна діяльність - політика та процедури для забезпечення дотримання положень керівництва. Цим забезпечується вжиття всіх необхідних заходів для управління ризиками та досягнення цілей, поставлених керівництвом;

- інформація та комунікації допомагають іншим компонентам шляхом належного інформування працівників про їхні обов'язки щодо внутрішнього контролю та надання відповідної, надійної, порівнянної та зрозумілої інформації, щоб вони могли виконувати свої обов'язки та завдання;
- моніторинг передбачає перевірку, здійснену керівництвом засобами здійснення внутрішнього контролю, або відповідальність, яка проводиться, якщо внутрішній контроль, працює і є достатнім для того, щоб діяльність чи дії відбувалися, як планувалося.

З часом, складність та комплексність інформаційних систем, їх складників, поширення та полегшення доступу до Інтернету, збільшення навантаження на ІТС, а також розширення систем організацій призводять до значного ускладнення процесу управління ризиками. Помітно це серед невеликих організацій, де комплексність та вартість процесу внутрішнього управління ризиками часто перевищує адекватність можливих збитків (у контексті окремого персоналу, пристроїв, програм), та великих корпорацій, для яких складність власних ІТС та їх місткість, можливість різноманітності загроз, є першоплановою проблемою, де найбільш сприятливим рішення є об'єктивного, комплексного та націленого управління окремим підрозділом, що, також, повинен мати новітні канали розвідки кібербезпеки.

Таким чином, із розвитком ландшафту можливих загроз, технік, що використовуються кіберзлочинцями, на сьогодні не існує остаточного рішення забезпечення кібербезпеки для підприємств, єдиною є можливість впровадження процесу управління ризиками, який надає змогу тримати стан певної організації під контролем.

1.2 Визначення основних аспектів стратегії управління ризикам, пов'язаними із забезпеченням кіберстійкості

Стандарт ISO 22301: 2019 Безпека та кіберстійкість - Системи управління безперервністю бізнесу – Вимоги (англ. Security and resilience — Business

continuity management systems — Requirements) [24] забезпечує основу для планування, створення, впровадження, експлуатації, моніторингу, перегляду, підтримки та постійного вдосконалення business continuity management system (анг. BCMS - системи управління безперервністю бізнесу).

За [5] операційна стійкість (англ. operational resilience) - властивість організації, яка характеризує можливість продовжувати виконувати місію за наявності операційних стресів та збоїв, що не перевищують експлуатаційні межі організації.

Збої та стреси беруться з реалізованого ризику. Управління ризиками безпеки таким чином стає управлінням стійкістю підприємства, у контексті безперервності бізнесу операцій (англ. Business continuity of Operations). Вводиться термін кіберстійкість (англ. resilience). Відбувається перехід від гарантування захисту до забезпечення стійкості, оскільки не існує ідеального захищеного рішення, лише можливість відповіді на ризики, з врахуванням сучасних тенденцій. Паралельно з цим, також існує поняття failover.

Відмовостійкість (англ. failover) - процес переходу від звичайної операційної спроможності до версії безперервності бізнес-операцій. Необхідна швидкість і гнучкість відмовостійкості залежить від типу бізнесу, починаючи від безперебійного для більшості фінансових сайтів і закінчуючи дещо відкладеним процесом, коли один процес замінюється іншим.

Кіберстійкі (еластичні) системи (англ. Resilient Systems) - це ті, які можуть повернутися до нормальних робочих умов після збою. Підвищення стійкості таких систем результує у зменшенні ризику, пов'язаному з їх виходом з ладу. Можливо це за допомогою належного використання різних стратегій конфігурації та налаштування, таких як моментальні знімки операційних систем, можливість повернення до відомих станів, а також шляхом впровадження надлишкових та відмовостійких систем. Автоматизація використовується для підвищення ефективності та точності керування хостами за допомогою команд. Проте головною умовою забезпечення кіберстійкості є використання єдиного централізованого рішення для управління ризиками підприємства. Таке рішення

може існувати як внутрішній апарат організацій, або бути переданим до виконання зовнішній організації, що може забезпечити більш комплексний та якісний наглядовий підхід.

Планування безперервності бізнесу (планування безперервності бізнесу та стійкості) є процесом створення систем запобігання та відновлення для боротьби з потенційними загрозами для компанії, де метою є забезпечення постійних операцій до та під час виконання аварійного відновлення.

У сфері інформаційної безпеки існує кілька основних стандартів, що визначають вимоги до планування безперервності бізнесу.

Спеціальна публікація NIST 800-34 Rev. 1 [22] являє собою посібник з планування на випадок надзвичайних ситуацій для Федеральних інформаційних систем , що розглядає основні задачі створення BCP (англ. Business continuity planning - Планування безперервності бізнесу) та DRP (англ. Disaster recovery plan - План ліквідації наслідків катастрофи) для критичних систем.

NIST SP 800-34 [22] визначає різні типи IT-планів на випадок непередбачених ситуацій та окреслює шестиступеневий процес планування для створення планів на випадок надзвичайних ситуацій:

1. Розроблення Положення про політику планування на випадок надзвичайних ситуацій.
2. Проведення аналізу впливу на бізнес (англ. BIA - Business Impact Analysis).
3. Визначення профілактичного контролю (англ. Preventative Controls).
4. Створення стратегій на випадок непередбачених ситуацій (англ. Contingency Strategies).
5. Планування тестування, навчання та вправи (англ. Testing, Training and Exercises).
6. Планування технічного обслуговування плану (англ. Maintenance).

Кіберстійкість забезпечує поєднання забезпечення безперервності бізнесу і аварійної стійкості водночас [17]. У інформаційній безпеці не існує єдино

захищеного рішення, що вимагає переходу від гарантування захисту до забезпечення кіберстійкості.

В минулому організації зосереджувались на створенні рівнів захисту мереж, систем та даних окремо. Ці підходи призначені для забезпечення виявлення та реагування. Такі методи мають цінність, проте без єдиної централізованої системи не є настільки ефективними, навіть підхід «багаторівневого» захисту стає малоефективним, бо загальна картина використовуваних засобів безпеки не є чітко зазначеною.

Визначаючи пріоритетність відповіді на інциденти – реалізовані ризики, метою є забезпечення кіберстійкого стану підприємства, що і розуміє під собою можливість мінімізації наслідків та адекватної пріоритерізації, за якої система повертається до «рівноваги» при збалансованих витратах.

Основні ідеї кіберстійкості включають:

1. Визначення мети супротивника: викрасти, знищити та / або змінити дані, взяти під контроль ІТС організації. Неможливо повністю передбачити, коли і як кіберзлочинці можуть ініціювати атаку, але є можливість робити щось постійно: організацію важко знайти; важко атакувати; важко пошкодити – організація є кіберстійкою. Забезпечити ці вимоги можливо спроектувавши таку систему, що навіть якщо нападаючі досягнуть успіху, забезпечить можливість мінімізувати шкоду та забезпечити безперервні операції.

2. Кіберстійкість = ІТ стійкість = Стійкість місії підприємства. Поєднання перевірених сильних сторін NIST Framework (ідентифікуйте, захищайте, виявляйте, реагуйте та відповідайте) з інженерною структурою стійкості (вивчайте, реагуйте, контролюйте та передбачайте), щоб створити нову структуру, рис. 1.6, що підтримує не лише кібер, але і стійкість до ІТ та місій.

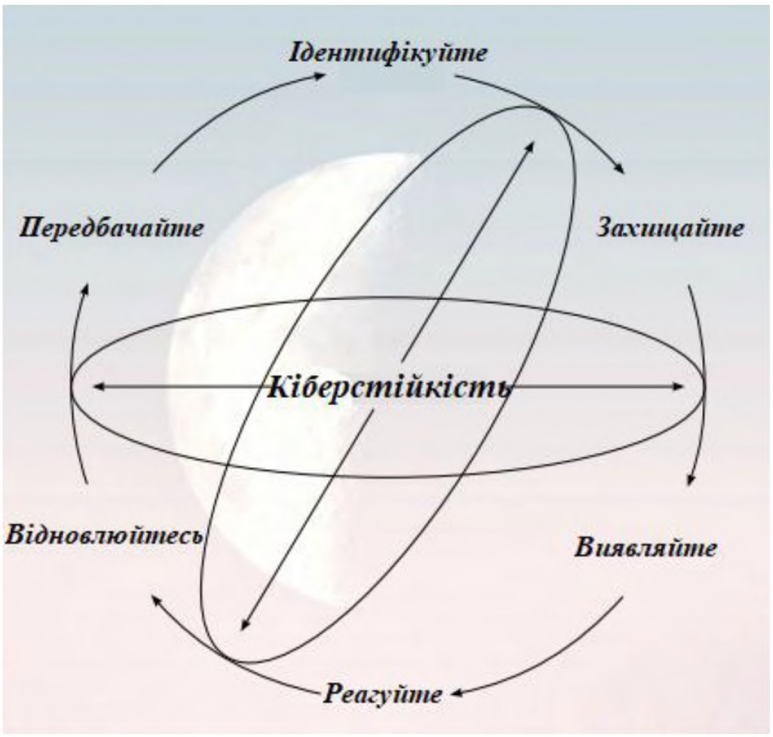

Рисунок 1.6 - Структура процесу забезпечення кіберстійкості

Таким чином стійкість означає «здатність підготуватися до змінних умов і пристосуватися до них, витримати та швидко відновитися від зривів».

Ефективне збалансування переваг технології з потенційними ризиками та наслідками події загрози, призводить до створення інтеграції управління ризиками кібербезпеки (англ. CSRM - cybersecurity risk management) та управління ризиками підприємств (англ. ERM - enterprise risk management). Підприємствам, організаціям та практикам слід враховувати вплив ризиків кібербезпеки на досягнення стратегічних цілей, операцій, звітності та дотримання цілей підприємства. Фахівці з питань ризиків на підприємстві повинні чітко повідомляти цілі підприємства, щоб фахівці з кібербезпеки могли вживати заходів та надавати відповідні дані щодо ризику для програм ERM, враховуючи відповідні рішення політик та регулятивні наслідки.

Для цілей ERM кожна організація повинна мати реєстр ризиків кібербезпеки, який чітко фіксує та повідомляє рішення про ризик з урахуванням стратегії ризику підприємства. На вищих рівнях підприємства вміст цих реєстрів слід узагальнювати, нормувати та розставляти пріоритети. Це дозволяє легко

передати знання про ризики кібербезпеки від CSRM до ERM. Для формування даних ризиків кібербезпеки для кращого узгодження з ризиками підприємств, організації повинні використовувати реєстр ризиків кібербезпеки для наступних заходів з управління ризиками:

1. Сукупні ризики від супротивників та системних збоїв, що призводять до негативних наслідків.
2. Нормалізація інформації між організаційними підрозділами, задля надавання вищим керівникам інформацію, необхідну для вимірювання ризиків кібербезпеки.
3. Пріоритеризація заходів з реагування на операційний ризик, поєднуючи інформацію про ризик з місією підприємства та бюджетними настановами для реалізації відповідних заходів.

У публікації NISTIR 8286 [39] наведено умовний шаблон реєстру ризиків кібербезпеки. Реєстр ризиків містить опис ризику, вплив, властивий за реалізації, ймовірність його виникнення, стратегії пом'якшення, власників, і рейтинг для виявлення більш пріоритетних ризиків.

Шаблон також посилається на властивий ризик, який описує «умови за відсутності дій з управління ризиками». Часто існують принаймні деякі елементи, які допомагають пом'якшити ризики, тому посилання відбувається на поточний ризик (а не на внутрішній ризик), який представляє базовий стан ризику.

NIST пропонує публікацію NISTIR 8286 «Інтеграція кібербезпеки та управління ризиками підприємств», яка містить специфікації та особливості програм управління ризиками підприємств. Документ призначений допомогти окремим організаціям на підприємстві покращити інформацію про ризики кібербезпеки, яку вони надають як вхідні дані до процесів ERM підприємства за допомогою комунікацій та обміну інформацією про ризики. Зосереджуючись на використанні реєстрів ризиків для встановлення ризику кібербезпеки, документ пояснює значення загальних показників ризику, які зазвичай розглядаються на нижчих рівнях системи та організації до більш широкого рівня підприємств. Шаблон реєстру ризиків може бути застосований як джерело даних для

уніфікованої центральної системи управління ризиками, для автоматизації процесу переліку та контролю ризиків, характерних для організації.

Поточний шаблон у форматі JSON (текстовий формат обміну даними, заснований на JavaScript), наведений на рисунку нижче.

```
{
    "$schema": "http://json-schema.org/draft-04/schema#",
    "title": "JSON Schema for cyberseucrity informed Enterprise Risk Management",
    "id": "https://csrc.nist.gov/1.1/erm_cybersecurity_risk_register_json.schema",
    "definitions": {
        "def_cybersecurity_risk_item": {
            "description": "Defines a cybersecurity risk.",
            "type": "object",
            "properties": {
                "riskId": {"type": "string"},
                "priority": {"type": "string"},
                "riskDescription": {"type": "string"},
                "riskCategory": {"type": "string"},
                "riskLikelihood": {"type": "string"},
                "riskImpact": {"type": "string"},
                "riskExposureRating": {"type": "string"},
                "riskResponseType": {"type": "string",

"enum":["Accept","Mitigate","Transfer","Avoid","Realize","Share","Enhance"]},
                "riskResponseCost": {"type":"number"},
                "riskResponseDescription": {"type": "string"},
                "riskOwner": {"type": "string"},
                "riskStatus": {"type": "string"}
            },
            "required": [
                "riskId",
                "priority",
                "riskDescription",
                "riskCategory",
                "riskLikelihood",
                "riskImpact",
                "riskExposureRating",
                "riskResponseType",
                "riskResponseDescription",
                "riskOwner",
                "riskStatus"
            ]
        }
    },
    "type": "object",
    "cybersecurityRiskRegister": {
        "name": {"type": "string"},
        "version": {"type": "string"},
        "description": {"type": "string"},
        "author": {"type": "string"},
        "date": {"type": "date-time"},
        "comments": {"type": "string"},
        "contact": {"type": "string"},
        "cybersecurityRisks": {
             "description": "Array of cybersecurity risks",
             "type": "array",
             "items": {"$ref": "#/definitions/def_cybersecurity_risk_item"}
        },
        "required": ["cybersecurityRisks"]
    }
}
```

Рисунок 1.7 - Шаблон реєстру ризиків кібербезпеки у форматі JSON

Реєстр ризиків підприємств складається з конкретних дисциплін (юридичних, фінансових, кібербезпеки), тому ризики кібербезпеки повинні бути задокументовані та відстежуватись у реєстрах ризиків кібербезпеки для підтримки кращого управління ризиками на рівні підприємства. Реєстр ризиків є сховищем інформації про ризики, включаючи дані, зрозумілі про ризики з часом [39]. Реєстри ризиків кібербезпеки є ключовим аспектом управління ризиками кібербезпеки на підприємстві. Кожен реєстр еволюціонує в міру того, як відбуваються інші заходи з ризику.

Підприємці з питань ризиків збирають усі дані щодо ризику, включаючи CSRM, аналізують потенційні події ризику, наслідки на рівні підприємства для створення реєстру ризиків підприємств (англ. ERR - enterprise risk register). Узагальнений результат, визначений за пріоритетом ERR - профіль ризику підприємства, який дозволяє основним зацікавленим сторонам виконавчого керівництва бути в курсі критичних ризиків, включаючи ті, що пов'язані з кібербезпекою. Таким чином, керівники підприємств мають необхідну інформацію та можливість розглядати вплив кібербезпеки як фактор для складання бюджету або звітності корпоративного балансу.

Відстежуючи стан кожного ризику, включаючи вартість експозиції, зацікавлені сторони підприємства можуть визначити найбільш відповідні ризики. Зведені звіти про найбільш пріоритетні ризики можуть бути використані для інформування зацікавлених сторін.

Як визначено у стандарті ДСТУ ISO/IEC 27005:2015 [4] існує декілька основних дій з оброблення ризиків:

1. Усунення - один із найпростіших способів зменшити ризик - припинення будь-якої діяльності, яка може поставити бізнес під загрозу. Такий підхід часто не є реалістичним варіантом для багатьох підприємств, оскільки або полягає у уникненні використання певних технологій, або у загальній відсутності підходу управління ризиками, у обох випадках результати можуть бути катастрофічними, такий підхід є найбільш дорогим.

2. Модифікація - метод управління ризиками через зменшення - вжиття заходів, необхідних для мінімізації потенціалу інциденту. За такого підходу потрібно зважити стратегії зменшення ризику з точки зору їх потенційної рентабельності інвестицій, оскільки якщо вартість зменшення ризику перевищує потенційну вартість інциденту, то такий підхід не є вигідним.

3. Прийняття ризику передбачає оцінку ризику та визначення, що вартість впливу реалізованого ризику знаходиться в обсязі прийнятних для організації. Цей варіант часто вибирають організації, що визначають, що вартість перенесення або зменшення ризику є надмірною або непотрібною.

4. Розподілення - один із найкращих методів управління ризиками, що полягає у передачі ризику іншій стороні. Прикладом цього може бути придбання комплексної страхової справи або аутсорсинг певних послуг. Передача ризику - це реалістичний підхід до управління ризиками, оскільки визнає, що інциденти трапляються, але гарантує, що бізнес організації буде готовий впоратися з наслідками цієї ситуації.

На рисунку нижче наведено основні дій з оброблення ризиків.

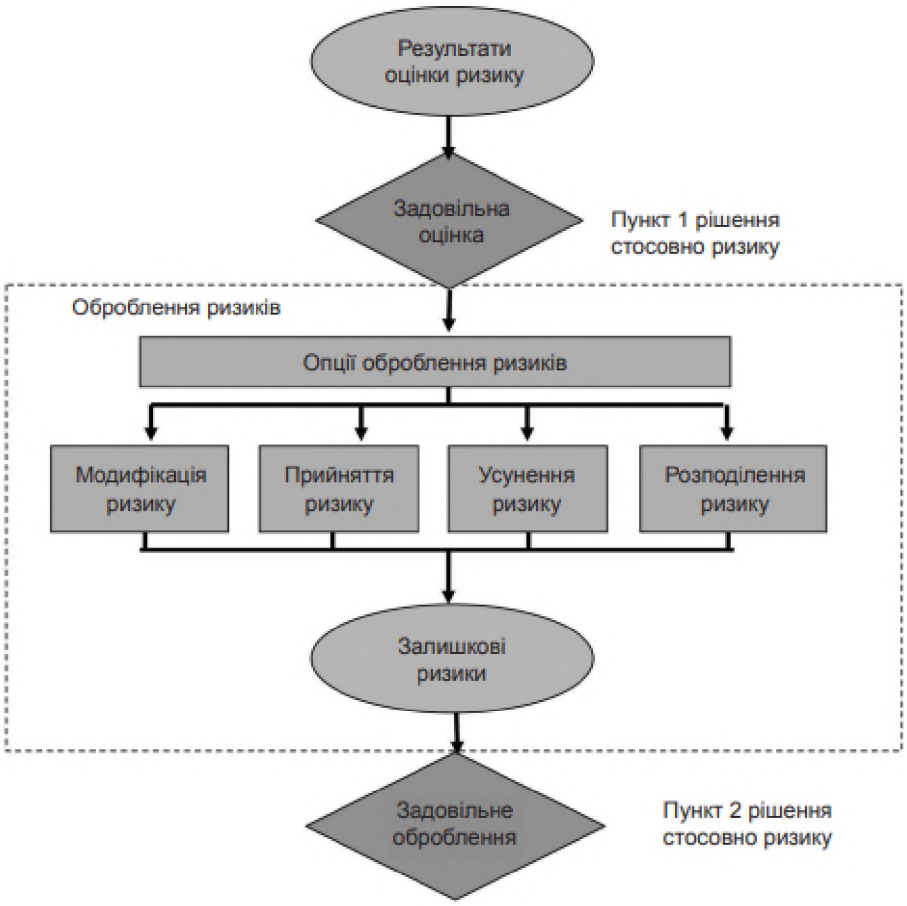

Рисунок 1.8 - Дії з оброблення ризиків

Страхування кібербезпеки захищає бізнес від комп'ютерних злочинів та втрат, включаючи цілеспрямовані атаки, такі як шкідливе програмне забезпечення та фішинг, а також втрату ноутбуків, що містять конфіденційні матеріали.

Поліс кіберстрахування призначений для покриття конфіденційності, даних та впливу мережі. Перелік нормативних актів та статутів продовжує розширюватися щодо використання та захисту інформації у сфері кібербезпеки, а також вимог щодо сповіщення у разі порушення.

Придбання відповідного полісу кіберстрахування є складною справою, оскільки потребує не лише аналізу ризиків, але і забезпечення відповідності певним стандартам, а тому може результувати організації у додаткових витратах на консультації певних спеціалістів. Придбання такого полісу також є часовим вирішенням, оскільки кожен поліс має відповідний час дії.

Із розвитком інформаційних технологій та ландшафту кіберзагроз, збільшується і кількість компаній, які надають послуги із кіберстрахування, що

також супроводжується появою шахрайських організацій у цій сфері. Велика кількість можливих постачальників страхування також зазначає, що 2020 рік характеризувався надмірним збільшенням цін на придбання відповідних полісів, що насамперед пов’язано з переходом багатьох організацій на віддалену роботу у зв’язку з пандемією COVID-19.

Як наведено у розділі 1.1, суттєві тенденції зростання загроз вимагають негайних відповідних рішень управління ризиками. Виходячи з позиції мінімізації витрат на підбір, навчання персоналу, постійних тренінгів, придбання відповідних інструментів, вводиться можливість аутсорсингу, за якої управління передається як послуга - кібербезпека як послуга. Це аутсорсингове рішення є найкращим способом створити активну, стійку оборону для захисту цифрових активів та досягнення усвідомлення розвідувальних даних про загрози в реальному часі, реагування на порушення для бізнесу будь-якого розміру.

Аутсорсинг управління та операційних ризиків - це основні напрямки, особливо у регульованих галузях, таких як банківська справа чи сектор охорони здоров'я. Згідно з дослідженням статистики IT-аутсорсингу комп'ютерної економіки останніх років, тенденція зростає на ринку аутсорсингу, що призводить до більш гнучких угод між постачальниками та клієнтами.

Аутсорсинг - засіб для досягнення вартості шляхом реалізації цілей аутсорсингу та відносин з постачальниками, мінімізуючи при цьому ризики та витрати. Ефективний підхід до управління має чітке розуміння роботи постачальника та ризиків, пов'язаних із послугою, що надається. Це гарантує, що засоби контролю пропорційні рівню вартості, що перебуває під загрозою, представленому залученням аутсорсингу [34].

Основні принципи аутсорсингу та управління відносинами з постачальниками включають:

1. Аутсорсингова компанія несе відповідальність за забезпечення безпечного та надійного ведення діяльності та з дотриманням чинного законодавства.

2. Постачальник несе відповідальність за якість своєї продукції та послуг.

3. Постачальник управляє своєю якістю на рівні системи, процесу та продукту / послуги.

4. Постачальник забезпечує точну та своєчасну звітність про результати діяльності та ризики.

5. Структура збалансовує вартість та ризик, забезпечує моніторинг та контроль, а також належну співпрацю між учасниками.

Аналізуючи техніки обробки ризиків, визначаємо, що основними перевагами зовнішнього підрядчика, що надає аутсорсинг послуг з кібербезпеки, є:

- мінімізація витрат. Аутсорсинг має на увазі періодичну плату, виключаючи накладні витрати, необхідні для створення внутрішньої команди (від витрат на персонал до програмного та апаратного забезпечення, необхідного для виконання роботи). Це відіграє роль у зменшенні навантаження на відділ кадрів компанії, оскільки немає необхідності турбуватися про підтримку колективу, а також про набір висококваліфікованих фахівців;
- постійна підтримка. Кібербезпека як послуга, що надається авторитетною компанією з перевіреним досвідом, може забезпечити постійну доступність досвідчених фахівців із безпеки цілодобово;
- доступ до досвіду групи професіоналів, які надають послуги з моніторингу та оборони для багатьох компаній різного масштабу в різних галузях;
- доступ до банку загроз, який має постачальний послуг, забезпечує адекватність та актуальність захисту від загроз більш точно та своєчасно.

Таким чином, аутсорсинг послуг кібербезпеки - практичний варіант для компаній, що не можуть дозволити собі власних експертів, які повинні самостійно створити, керувати та використовувати технологічні інструменти для самостійного виявлення нових векторів атак чи загроз задля управління ризиками підприємства.

1.3 Типові рішення з аутсорсингу послуг з кібербезпеки

У нинішньому нестабільному діловому середовищі ефективне повсякденне управління ризиками має вирішальне значення для людей, процесів та довготривалої життєздатності організації. Відділ управління ризиками виконує надзвичайно важливу роль, враховуючи його унікальну позицію в організації на перехресті операційних, фінансових, бухгалтерських та стратегічних функцій. Перевірений, структурований підхід до оцінки та розвитку культури, яка усвідомлює ризики - основна відповідальність відділу управління ризиками - може допомогти зменшити ризик у всій організації.

Аутсорсинг як підхід до управління ризиками може надати цілеспрямований досвід за потребою: від виконання щоденних завдань з управління ризиками; до реінжинірингу ключових процесів; сприйняття культури, яка усвідомлює ризики, щоб організація могла відповісти на виклики, що виникають внаслідок складних та нових ризиків.

Як зазначається у розділі 1.2, сьогодні багато організацій передають частину / всі свої операції третій стороні, що є компанією з надання послуг у сфері інформаційної безпеки. Найбільш логічними сферами безпеки для аутсорсингу є: служби моніторингу та оповіщення, тестування безпеки, реагування на інциденти, оцінки сторонніх організацій для виявлення реальних ризиків з подальшим цілеспрямованим навчанням працівників. Пояснюється це також тим, що не всі компанії можуть дозволити собі достатньо велику внутрішню команду для постійного моніторингу, а отже, час реагування на інциденти може бути повільнішим. Крім того, може виявитися неможливим знайти та працевлаштувати декількох досвідчених фахівців, тому можуть виникнути прогалини у безпеці.

Першочерговим поняттям, пов'язаним із забезпечення кібербезпеки будь-якої організації є операційний центр безпеки (англ. SOC - Security Operation Center), розроблений для захисту системної інфраструктури організацій для виявлення та запобігання вторгненням у мережу ІТС.

Для управління власним операційний центром безпеки (SOC) організація може прийняти рішення про створення Хмарного операційного центру безпеки (англ. Cloud SOC) [26] для забезпечення видимості та контролю за допомогою віртуалізованої інфраструктури, яка може надавати рішення для будь-яких сфер, що викликають занепокоєння, і забезпечувати адекватний кіберзахист активів.

У такому випадку організація передає свої ключові функції та вибирає Провайдера керованих послуг безпеки (англ. MSSP - Managed Security Service Provider), щоб бути у захисті від постійних загроз у кіберпросторі.

Аутсорсингові завдання включають:

- моніторинг ризиків кібербезпеки до того, як вони стануть справжніми проблемами. Проведення оцінок вразливості та аудиту IT, де ризики визначаються, вимірюються та управляються з часом;
- сканування, що допомагає виявити зони, вразливі до комп'ютерних загроз (віруси, зловмисне програмне забезпечення, шпигунське програмне забезпечення) та надавати реалістичні оцінки загроз;
- тестування заходів безпеки та існуючих засобів контролю та процесів безпеки для забезпечення стану захищеності організації від будь-якого типу вразливості.

MSSP є попередником Служби керованого виявлення та реагування (англ. MDR - Managed Detection and Response) [26]. Провайдери керованих послуг безпеки (MSSP) відстежують події безпеки мережі та надсилають сповіщення, коли виявляються аномалії. MSSP не досліджують аномалії для усунення помилкових позитивних даних, а також не активно реагують на загрози безпеці. Деякі MSSP можуть надавати різноманітні додаткові мережеві послуги, як захист від вірусів та управління брандмауером.

На рисунку 1.9 наведено загальні можливості та відмінності у підходах надання послуг MSSP та MDR.

Рисунок 1.9 - Порівняльна характеристика можливостей MSSP та MDR

Рішення керованого постачальника послуг безпеки має кілька переваг, особливо для клієнтів у сфері малих та середніх підприємств. MSSP можуть допомогти зосередити зусилля на розслідуванні, але усе інше залишається за клієнтом - проведення фактичних розслідувань, усунення помилково-позитивних інцидентів та підготовка відповідей на інциденти.

Служба керованого виявлення та реагування (MDR) дозволяє здійснювати постійний моніторинг кібер-активів, з точки зору сучасних загроз, які постійно розвиваються, та можливих експлуатацій, а також забезпечує швидке реагування на підтверджені інциденти.

MDR - це служба кібербезпеки IT, яка виявляє вторгнення, зловмисне програмне забезпечення та шкідливі дії у мережі та допомагає оперативно реагувати на усунення та зменшення цих загроз. Якісні послуги MDR використовують поєднання людських аналітиків та технологій для усунення помилково-позитивних даних, виявлення реальних загроз безпеці та розробки реагування на інциденти в режимі реального часу.

Значна потреба в MDR [26] є серед організацій, які мають нормативно-правові вимоги щодо забезпечення ефективного виявлення та реагування

(охорона здоров'я, фінансові послуги), але не мають повністю штатного оперативного центру безпеки (SOC). Керовані сервіси (Managed services), в свою чергу, фактично забезпечують доступ за не дуже велику плату до команди досвідчених професіоналів та спеціалізованого програмного забезпечення, яке неможливо придбати при створенні внутрішньої структури, гарантуючи охоплення 24x7x365.

Притаманні недоліки включають щомісячні витрати, які можуть бути стабільними або збільшувати понаднормові роботи, тоді як внутрішній SOC може потенційно дешевшати з часом. Безпека та конфіденційність також викликають занепокоєння, оскільки довіряти субпідрядникам постачальника є необхідністю. Такий ризик можна зменшити, розробивши надійні угоди про рівень обслуговування (англ. SLAs - Service Level Agreements).

Методології реагування на MDR та MSSP на порушення відрізняються. Якщо організація працює з третьою стороною, питання переходить від нагляду до аналізу. MSSP приймає дані про події та події з SIEM (англ. Security Information and Event Management - Управління інформаційною безпекою та подіями) клієнта та контролює їх цілодобово. Рішення MSSP визначають, що клієнт надає відповіді на інциденти безпеки. MDR пропонують більш комплексні відповіді на порушення. Ефективні MDR мають глибший та складніший план реагування на виявлення як вразливостей, так і загроз, та динамічне реагування на пом'якшення цих проблем.

Наступна таблиця відображає подібність та відмінності між постачальниками послуг MSSP та MDR [26].

Таблиця 1.2 - Порівняльна характеристика Провайдера керованих послуг безпеки та Служби керованого виявлення та реагування

Характеристика	**MSSP**	**MDR**
Журнал подій безпеки та джерела контексту	Агностичне джерело події. Дані, що надсилаються провайдеру, визначаються замовником.	Надається запатентований технологічний стек та мережевий датчик, що розгортається в приміщенні замовника.
Віддалене керування пристроями	Пропонує контроль найпоширеніших засобів безпеки (брандмауерів, систем виявлення / запобігання вторгнень, веб-шлюзів).	Управляє лише власними технологічними провайдерськими стеками.
Звітність про відповідність	Так	Так
Сервісний інтерфейс	Портал та електронна пошта виступають основними інтерфейсами, а вторинний доступ до аналітиків надається через функції чату та телефон.	Більш пряме спілкування (голосове або електронне повідомлення) з аналітиками, проте можливі і портали.
Підтримка реагування на інцидент	Надається як віддалена, так і підтримка на місці.	Легка віддалена підтримка відповіді на інциденти входить до базових послуг. Відповідь на інциденти на місці надається постачальником.
Стримання інциденту (англ. Incident containment)	Надається віддалено, бо постачальник часто керує всіма засобами контролю безпеки для клієнта. Також може пропонувати послуги типу MDR - такі як керовані виявлення та реагування на кінцеві точки (англ. EDR - managed endpoint detection and response).	Забезпечується використання стеку технологій або технологій, що належать замовникам, використання сценаріїв та API (англ. application programming interface - інтерфейс прикладного програмування) для програмного внесення змін.
Угоди про рівень обслуговування (SLA) для виявлення та реагування на інциденти	Так	Рідко

Альтернативною послугою, ефективної цінової категорії є Управління інформаційною безпекою та подіями (SIEM). Багато організацій використовують SIEM як послугу для посилення своїх існуючих кіберзахистних рішень у якості найефективнішої стратегії кіберстійкості - управління ризиками, пом'якшення наслідків інтегрованої розвідки про загрозу, можливості мати змогу прискорити виявлення загроз. Оскільки рішення SIEM прагнуть генерувати значну кількість даних та подій організації використовують аутсорсинг до керованих служб безпеки (MSS).

Термін SIEM відноситься до широкого спектру продуктів і послуг, що варіюються від рішень, що стосуються лише технології, технологій з адміністративним управлінням, а також керованої обробки IT-подій та оповіщення. Рішення SIEM поєднують дані про мережевий трафік / події з різних джерел і співвідносять ці дані, щоб виділити елементи, які потребують подальшого дослідження.

Керовані рішення SIEM дешевші, ніж MDR або MSSP, і відповідають ряду нормативних вимог, таких як Payment Card Industry Data Security Standard. Організації, які мають надійні внутрішні команди із захисту IT та зацікавлені у додатковому визначенні пріоритетності розслідувань, можуть добре обслуговуватися рішеннями SIEM, оскільки ця технологія вимагає ефективну взаємодію з оператором/аналітиком для ефективності. Продукти SIEM забезпечують аналіз у реальному часі, попередження про безпеку, що генерується додатками та мережевим обладнанням.

Цей термін є певною мірою основною структурою для програмних пакетів безпеки, починаючи від систем управління журналом (англ. Log Management Systems) до журналів безпеки (англ. Security Log) / управління подіями (англ. Event Management), управління інформацією про безпеку (англ. Security Information Management) та співвідношення безпеки подій (англ. Security Event correlation).

Поняття Управління інформацією про безпеку (англ. SIM - Security Information Management) визначає збір, моніторинг та аналіз даних, пов'язаних із безпекою з комп'ютерних журналів.

Управління подіями безпеки (англ. SEM - Security Event Management) - практика управління мережевими подіями, включаючи аналіз загроз у реальному часі, візуалізацію та реагування на інциденти.

SIEM, SIM та SEM часто використовуються взаємозаміно, але є ключові відмінності. У таблиці нижче наведено порівняльну характеристику понять SIEM, SIM та SEM.

Таблиця 1.3 - Порівняльна характеристика понять SIM, SEM та SIEM

	Security Information Management (SIM)	**Security Event Management (SEM)**	**Security Information and Event Management (SIEM)**
Загальна характеристика	Збір та аналіз даних про безпеку з комп'ютерних журналів.	Аналіз загроз у реальному часі, візуалізація та реагування на інциденти.	Поєднує можливості SIM та SEM.
Особливості	Простота розгортання, потужні можливості управління журналом.	Більш складні для розгортання, покращені в режимі моніторингу в режимі реального часу.	Складні для розгортання, проте забезпечують повний функціонал та захист на 360 градусів.
Приклади інструментів	OSSIM	NetIQ Sentinel	SolarWinds Log & Event Manager

Основні можливості SIEM включають:

- колекціонування журналів (англ. log collection);
- нормалізацію (англ. normalization) - збирання журналів та їх нормалізація у стандартний формат;
- сповіщення та оповіщення (англ. notifications and alerts) - повідомлення користувача, коли виявляються загрози безпеці;
- виявлення інцидентів безпеки (англ. security incident detection);
- потік реагування на загрозу (англ. threat response workflow) - робочий процес для обробки минулих подій безпеки.

Система працює за статистичною моделлю для аналізу записів журналу. SIEM поширює агенти збору та відкликає дані з мережі, пристроїв, серверів та брандмауерів. Інформація передається в консоль управління, де аналізується для вирішення виникаючих загроз. В більш досконалих системах SIEM використовуються автоматизовані відповіді, аналітика поведінки суб'єктів та організація безпеки.

Після надходження до консолі управління, інформація переглядається аналітиком, який надає зворотній зв'язок про загальний процес. Це є важливим фактором, оскільки зворотний зв'язок допомагає розвивати систему SIEM з точки зору машинного навчання та підвищувати її ознайомлення з середовищем. Коли система SIEM виявляє загрозу, вона зв’язується з іншими системами безпеки на пристроями, щоб зупинити небажану діяльність.

Основні функції системи SIEM:

1. Управління даними журналу (англ. Log Data Management) з метою об'єднання інформації журналів з різних джерел даних, для розпізнавання зловмисної поведінки та сповіщення порушення безпеки.

2. Звітність про відповідність (англ. Compliance Reporting) - система генерації звітів, яка допомагає відповідати встановленим вимогам.

3. Розвідувальні дані про загрози (англ. Threat Intelligence) визначає можливість використання певного банку загроз, визначаючи актуальні тенденції вразливостей.

4. Умови налаштування сповіщення (англ. Tuning Alert Conditions) - здатність встановлювати критерії подальших сповіщень про безпеку має важливе значення для підтримки ефективної системи SIEM за допомогою розвідки про загрози; є головним способом оновлювати систему SIEM проти нових загроз.

5. Панель приладів (англ. Dashboard) з простим користувальницьким інтерфейсом значно полегшує ідентифікацію загроз. Це дозволяє аналітику набагато швидше визначати аномалії.

Розглядаючи процес впровадження функціонування SIEM на підприємстві, вибір організаційної моделі може допомогти визначити бюджет реалізації, а також сформувати проект звіту про роботу (англ. SoW - statement of work). У таблиці 1.4 викладено чотири організаційні моделі, які варіюються від повністю власної до повністю переданої на аутсорсинг.

Самообслуговування, самокерування - основна модель розгортання застарілих SIEM. Ця модель є складною і дорогою в обслуговуванні, навіть якщо організація виділяє належні ресурси та бюджет.

Сьогодні існує безліч варіантів, які дозволяють організації вибрати модель, яка найкраще відповідає операційним, діловим та фінансовим потребам. Важливо оцінювати підхід і вибрати найкращу модель на основі реалістичної оцінки того, як планується підтримка SIEM з часом.

Таблиця 1.4 - Організаційні моделі для впровадження робочого процесу SIEM

Модель	***Організація***	***Провайдер керованих послуг безпеки (MSSP)***
Самостійно влаштована, самокерована	SIEM розміщена в центрі обробки даних організації (виділена платформа SIEM, підтримується відповідне обладнання та системи зберігання, SIEM є керованою за допомогою навченого персоналу служби безпеки).	Не використовується.
Само-обслуговувана, гібридне управління	Організація купує та підтримує програмно-апаратну інфраструктуру. Відбувається спільне управління збором/ агрегуванням подій SIEM, кореляцією, аналізом, попередженням та інформаційними панелями.	Розгортання та спільне управління збором / агрегуванням подій SIEM, кореляцією, аналізом, попередженням та інформаційними панелями
Хмарна SIEM, самокерована	Організація обробляє та аналізує інформацію попереджень процесів безпеки з використанням даних SIEM.	Постачальник виконує збір, агрегування та обробку подій безпеки.
SIEM-як-послуга (повністю передана в аутсорсинг)	Організація лише обробляє процеси безпеки, використовуючи дані SIEM.	Постачальник виконує збір даних за подіями, агрегування, кореляцію, аналіз попереджень.

Для найбільш повного перекриття цілей управління ризиками, з метою пришвидшення реакцій на інциденти, розширення актуальної бази загроз, використання досвіду більш практично досвідчених спеціалістів, спрощення технічного обслуговування системи та за адекватного придбання послуг за ціновою категорією, найкращим рішенням є SIEM-як-послуга (повністю передана в аутсорсинг).

Щоб бути ефективною, SIEM [15] повинна залишатися актуальною перед новими загрозами, а також змінами як технічними, так і інфраструктурної підтримки організації. SIEM наступного покоління доповнює традиційні можливості (автоматизоване управління журналами, кореляцію, розпізнавання шаблонів та оповіщення) за допомогою нових та гнучких технологій: хмарної аналітики; інструментування безпеки, автоматизації та реагування (англ. Security Orchestration, Automation and Response - SOAR); аналітики поведінки користувачів та сутності (англ. UEBA - user and entity behavior analytics); машинного навчання та штучного інтелекту.

Аналізуючи можливі варіанти впровадження SIEM на підприємстві, визначаємо основні характеристики актуальної системи, що забезпечують кіберстійкість організації, наведені у таблиці 1.5.

Таблиця 1.5 - Типові характеристики SIEM, для задоволення потреб кіберстійкості

Рівень управління даними (Data Management Layer) побудовано навколо архітектури великого обсягу даних, архітектури обчислень та зберігання, яка збирає та управляє великими наборами даних безпеки для індексації та пошуку, що забезпечує аналіз даних у режимі реального часу.	
Функція	*Опис*
Збір даних	Збирає дані журналу з різних джерел, включаючи мережеві та захисні пристрої, програми та різні кінцеві точки-хости.
Агрегація даних	Нормалізує зібрані дані.
Кореляція та аналіз даних	Пов'язує події та пов'язані дані з інцидентами безпеки, загрозами або висновками розслідуваних інцидентів.
Зберігання	Забезпечує онлайн-доступ до поточних та заархівованих даних журналу, додаткових артефактів.
Утримання	Зберігає довгострокові історичні дані, що використовуються для дотримання та проведення розслідувань інцидентів.
Рівень моніторингу / аналітики (Monitoring/Analytics Layer) розширені аналітичні можливості є ключовими для виявлення прихованих загроз, включають як виявлення складних сценаріїв, так і поведінкове моделювання для виявлення та встановлення пріоритетів загроз.	
Функція	*Опис*
Моніторинг / аудит	Забезпечує автоматизовані засоби виявлення аномальних форм поведінки; працює з інструментами аналітики; перекриває аудит різних журналів на відповідність стандартам, як PCI DSS, GDPR, HIPAA.
Аналітика	Використовує статистичні моделі та машинне навчання для виявлення більш глибоких взаємозв'язків між даними та елементами поведінки, подає інформацію в контексті.
Інформація про загрози	Поєднує внутрішні дані зі сторонніми даними про загрози та вразливості.
Рівень робочого процесу / автоматизації (Workflow/Automation Layer) автоматизує та визначає пріоритети дій, що дозволяють покращити робочий процес та продуктивність організації (реагування на аварії, кращий аналіз тривог).	
Функція	*Опис*
Операції: Автоматизація	Інтегрується з іншими рішеннями безпеки за допомогою API, визначаючи автоматизовані робочі процеси у відповідь на конкретні випадки. Сумісна з інструментами SOAR.
Операції: Полювання на загрози / розслідування	Дозволяє співробітникам служби безпеки запускати запити як до структурованих, так і до неструктурованих журналів та даних про події для попереднього виявлення загроз або вразливостей
Операції: Відповідь на інцидент	Допомагає командам безпеки виявляти та реагувати на інциденти, швидко передаючи всі відповідні дані.
Відповідність	Спирається на дані аудиту для формування звітів на відповідність нормам та стандартам.
Аналіз інцидентів/ «форензіка» (Forensic analysis)	Дозволяє вивчати журнали та дані про події, щоб виявити деталі інциденту безпеки.

Продовження таблиці 1.5 - Типові характеристики SIEM, для задоволення потреб кіберстійкості

Рівень взаємодії користувачів (User Interaction Layer) Інструменти наступного покоління надають у реальному часі уявлення про закономірності, тенденції та співвідношення, що може безпосередньо перетворитися на своєчасне виявлення та розпізнавання проблемних проблем або подій, які інакше могли б залишитися непоміченими.	
Функція	*Опис*
Попередження	Аналізує події та надсилає попередження про негайні проблеми.
Візуалізація	Створює візуалізації на основі даних у реальному часі, чи на основі історичних подій, для точнішого визначення закономірностей та аномалій.
Звітність	Створює стандартні та спеціальні звіти для підтримки відповідного робочого процесу.

Політика безпеки та аналіз робочих процесів допомагають визначити початкову стратегію розгортання системи з метою забезпечення кіберстійкості. Використовуючи цю інформацію та основні властивості актуальної системи, наведені у таблиці вище, впровадження SIEM на репрезентативній підмножині існуючої інфраструктури стає більш однорідним та легшим процесом.

1.4 Постановка задачі

Відповідно до розділу 1, для розроблення підходу забезпечення кіберстійкості інформаційних систем підприємства, формулюємо основні завдання дослідження:

- аналіз підходів до реалізації інтелектуальних систем аналітики;
- розробка основних вимог до систем, що забезпечують кіберстійкість;
- дослідження процесу впровадження SIEM на підприємстві та процесу функціонування;
- аналіз отриманих результатів порівняння відомих рішень SIEM та ефективності роботи моделей;
- розробка алгоритму вибору функціональної SIEM;
- формування рекомендацій для впровадження системи та вимог до критеріїв угоди про рівень обслуговування.

Висновки до Розділу 1

Однією з основних проблем будь-якого підприємства є забезпечення його кіберстійкості за збалансованих витрат. Оскільки можливість вирішення цього полягає саме у розумінні можливості реалізації різних сценаріїв розвитку для підприємства, має бути впровадженим процес управління ризиками, метою якого є знаходження балансу між витратами на забезпечення інформаційної безпеки організації та збитками, що може понести підприємство при реалізації відповідних ризиків.

Неможливість створення абсолютно захищеної системи, призводить до використання підходу забезпечення кіберстійкості як можливості мінімізації ризиків.

Кіберстійкість стає необхідною умовою успішності міжнародних компанії, діяльність яких пов'язана з інформаційними технологіями чи обробкою персональних даних. Концепція має міжнародне значення, її важливість складно переоцінити, адже забезпечення стійкого стану за адекватних витрат використовуються на всіх рівнях забезпечення кіберзахисту.

Аналізуючи можливі дії з обробки ризиків, приходимо до висновку, що розподілення ризиків є одним з найкращих методів управління, бо забезпечує реалістичний підхід, що визнає можливість реалізації інцидентів, але гарантує, що бізнес організації буде готовий впоратися з наслідками.

Вибір постачальника та виду послуг з кібербезпеки має вирішальне значення для ефективного управління ризиками кібербезпеки організації: включає ретельний аналіз бізнес-вимог, управління ризиками при передачі активів, наслідки, які компанія готова прийняти при аутсорсингу та потенційну вартість порушення інформаційної безпеки.

За результатами проведеного аналізу, було встановлено необхідність розробки підходу забезпечення стану кіберстійкості організації.

РОЗДІЛ 2 МІНІМІЗАЦІЯ РИЗИКІВ, ПОВ'ЯЗАНИХ ІЗ ЗАБЕЗПЕЧЕННЯМ КІБЕРСТІЙКОСТІ

2.1 Підходи до реалізації інтелектуальних систем аналітики

На сьогодні багато різних компаній-виробників пропонує різноманітні рішення SIEM систем, що відповідають вимогам організацій різних розмірів та сфер діяльності, є рішення майже для кожного розміру та галузі роботи компанії, серед них є і безкоштовні варіанти з відкритим кодом, що, як результат, мають мізерні бюджети розвитку.

Перед вибором інструменту SIEM, оцінюються цілі, що є визначними для окремого підприємства. Найкращими інструментами SIEM на 2020 рік є:

1. *ManageEngine EventLog Analyzer* [36]

Операційна система: Windows та Linux

Аналізатор подій ManageEngine EventLog Analyzer фокусується на управлінні журналами та вибору з них інформації про безпеку та ефективність. Інструмент здатний збирати журнал подій Windows та повідомлення Syslog, повідомлення організовуються у файли і зберігаються у довірених каталогах. Аналізатор подій EventLog захищає файли від підробки. Система має аналітичні функції, які інформують про несанкціонований доступ до ресурсів компанії. Інструмент також оцінює ефективність основних програм та служб, таких як веб-сервери, бази даних, сервери DHCP (англ. Dynamic Host Configuration Protocol - Протокол динамічної конфігурації хосту) та черги друку.

2. *Splunk Enterprise Security* [43]

Операційна система: Windows та Linux

Splunk - одне з найпопулярніших рішень управління SIEM у світі. Головна відмінність - аналітика є ядром функціонування SIEM. Дані мережі та хостів відстежуються в режимі реального часу, система шукає потенційні вразливості і одразу вказує на аномальну поведінку. Функція примітки відображає сповіщення, які також можна уточнювати.

3. *SolarWinds Security Event Manager* [42]

Операційна система: Windows

Кращий інструмент SIEM початкового рівня - SolarWinds Security Event Manager (SEM), що втілює основні функції, які очікуються від системи SIEM, з широкими функціями управління журналами та звітності. Детальна відповідь на інцидент в реальному часі робить інструмент активного управління мережевою інфраструктурою проти майбутніх загроз через журнали подій Windows. Простота інструментів візуалізації полегшує користувачеві виявлення будь-яких аномалій. Компанія пропонує цілодобову підтримку задля можливості зв'язатися з оператором, при виникненні помилок.

4. *LogRhythm NextGen SIEM Platform* [35]

Операційна система: Windows та Linux

LogRhythm є одним з найбільш довірених компаній. Ця платформа має все необхідне - від поведінкового аналізу до кореляції журналів та штучного інтелекту для машинного навчання. Система сумісна з величезним набором пристроїв та типів журналів, більшість видів діяльності управляється через диспетчер розгортання (майстер хостів Windows). Цінова вартість платформи робить її вибором для середніх організацій, які прагнуть впроваджувати нові заходи безпеки.

5. *RSA NetWitness* [41]

Операційна система: Red Hat Enterprise Linux

Платформа RSA NetWitness – посередній варіант SIEM, пропонує повне рішення мережевої аналітики, однак, складний у використанні Початкове налаштування займає досить багато часу в порівнянні з іншими рішеннями SIEM, що розглядаються у дипломній роботі. Проте, всебічна документація користувача допомагає у процесі налаштування. Інструкції з установки не допомагають у всьому, але надають достатньо інформації для складання фрагментів.

6. *McAfee Enterprise Security Manager* [38]

Операційна система: Windows та Mac OS

McAfee Enterprise Security Manager вважається однією з найкращих платформ SIEM з точки зору аналітики. Користувач може збирати різноманітні журнали на широкому діапазоні пристроїв через систему Active Directory.

Нормалізація реалізується механізмом кореляції McAfee, такий підхід значно спрощує виявлення, коли відбувається інцидент.

Користувачі мають доступ як до технічної підтримки McAfee Enterprise. Платформа McAfee спрямована на середні та великі компанії, які шукають повне рішення щодо управління подіями в галузі безпеки.

7. IBM QRadar [32]

Операційна система: Red Hat Enterprise Linux

Протягом останніх кількох років рішення SIEM QRadar від IBM зарекомендувало себе як один з найкращих продуктів на ринку. Платформа пропонує набір функцій управління журналом, аналітики, збору даних та виявлення вторгнень, що допомагає підтримувати критичні системи. Весь процес керування журналом проходить через один інструмент - QRadar Log Manager. QRadar є повним рішенням з точки зору аналітики.

У системі існує аналітика моделювання ризиків, яка може імітувати потенційні атаки. Функцію можна використовувати для моніторингу різноманітних фізичних та віртуальних середовищ у мережі. Різноманітна функціональність цієї системи SIEM зробила її галузевим стандартом для багатьох великих організацій.

8. OSSEC [40]

Операційна система: Windows, Linux, Unix та Mac

OSSEC є провідною системою профілактики вторгнень на базі хостів (англ. HIDS - Host-based Intrusion Detection System), що є вільним у використанні рішенням. Методи HIDS взаємозамінні з послугами, що виконуються SIM-системами, тому OSSEC також є рішенням інструменту SIEM. OSSEC є безкоштовним фрагментом програмного забезпечення, тому правильним вибором є встановлення OSSEC у багатьох місцях мережі.

Програмне забезпечення фокусується на інформації, доступній у файлах журналів для пошуку доказів вторгнення. Окрім читання файлів журналів, програмне забезпечення відстежує контрольні суми файлів для виявлення фальсифікацій. Враховуючи, що різні операційні системи мають різні системи

реєстрації, OSSEC має можливість вивчати журнали подій Windows, Linux, Unix та Mac OS. Поведінка OSSEC диктується попередньо затвердженим політиками.

9. *AT&T Cybersecurity AlienVault Unified Security Management* [29]

Операційна система: Windows та Mac OS

AlienVault є одним з найбільш конкурентоспроможних рішень SIEM. Це традиційний продукт SIEM із вбудованою системою виявлення вторгнень, моніторингом поведінки та оцінкою вразливості, має вбудовану аналітику. Одним з унікальних аспектів платформи є біржа відкритих загроз (англ. OTX - Open Threat Exchange) - веб-портал, який дозволяє користувачам завантажувати індикатори порушень (англ. IOC - indicators of compromise), щоб допомагати іншим користувачам виявляти загрози. Низька ціна цієї системи робить її рішенням для малого та середнього бізнесу, який прагне покращити свою інфраструктуру безпеки.

Результати більш детального аналізу систем, за критеріями, визначеними у таблиці 1.5, з метою задоволення потреб кіберстійкості підприємств, наведено в узагальнюючій таблиці 2.1.

Рішення SIEM / Функція	*Manage Engine EventLog Analyzer*	*Splunk Enterprise Security*	*SolarWinds Security Event Manager*	*LogRhythm NextGen SIEM Platform*	*RSA NetWitness*	*McAfee Enterprise Security Manager*	*IBM QRadar*	*OSSEC*	*AT&T Cybersecurity AlienVault Unified Security Management*
Рівень управління даними (Data Management Layer)									
Збір даних									
Стандартна інфраструктура централізованого управління хостом	+	+	+	+	+	-	+	+	-
Журнали даних мережевих пристроїв	-	+	+	+	+	+	+	-	+
Журнали даних приладів безпеки	-	+	+	+	-	-	+	-	+
Агрегація даних									
На основі заздалегідь визначених правил	+	+	+	+	+	+	+	+	+
Зведене індексування, при структуруванні ризиків	-	+	-	-	-	+	+	-	-
Багатозадачність	-	+	+	+	-	-	+	-	+
Використання ШІ	-	+	-	+	-	-	+	-	+

Таблиця 2.1 - Порівняльна характеристика відомих рішень SIEM

Продовження таблиці 2.1 - Порівняльна характеристика відомих рішень SIEM

Рішення SIEM / Функція	***Manage Engine EventLog Analyzer***	***Splunk Enterprise Security***	***SolarWinds Security Event Manager***	***LogRhythm NextGen SIEM Platform***	***RSA NetWitness***	***McAfee Enterprise Security Manager***	***IBM QRadar***	***OSSEC***	***AT&T Cybersecurity AlienVault Unified Security Management***
Кореляція та аналіз даних									
Попередньо налаштовані алгоритми/ шаблони	+	+	+	+	+	+	+	+	+
Розширена кореляція	-	+	+	-	+	-	+	-	+
Фільтрація шуму	-	-	-	+	-	-	+	-	-
Історична кореляція	-	+	-	-	-	-	+	+	-
Окремий механізм кореляції	-	+	+	+	+	+	+	-	-
Зберігання									
Необмежений період зберігання	-	+	-	+	-	-	+	-	+
Можливість хмарного рішення	-	+	-	+	-	-	+	-	+
Окрема база даних	+	+	+	+	+	+	+	-	+
Додаткові метадані, збагачені контекстом безпеки	-	-	-	-	+	+	+	+	-
Можливість уніфікації формату	-	+	+	+	+	+	+	+	+

Рішення SIEM / Функція	***Manage Engine EventLog Analyzer***	***Splunk Enterprise Security***	***SolarWinds Security Event Manager***	***LogRhythm NextGen SIEM Platform***	***RSA NetWitness***	***McAfee Enterprise Security Manager***	***IBM QRadar***	***OSSEC***	***AT&T Cybersecurity AlienVault Unified Security Management***
Утримання (за замовчуванням та можливістю налаштування)									
1 місяць	+	-	-	-	-	-	-	-	-
3 місяці	-	-	-	-	-	-	-	+	-
1 рік	-	-	+		-	+	-	-	-
1,5 роки	-	-	-	+	+	-	-	-	-
Безстроково (залежності від стандартів відповідності)	-	+	-	-	-	-	+	-	+
Рівень моніторингу / аналітики (Monitoring/Analytics Layer)									
Моніторинг / аудит									
Моніторинг багатьох хостів	+	+	+	+	+	+	+	-	+

Продовження таблиці 2.1 - Порівняльна характеристика відомих рішень SIEM

Рішення SIEM / Функція	***Manage Engine EventLog Analyzer***	***Splunk Enterprise Security***	***SolarWinds Security Event Manager***	***LogRhythm NextGen SIEM Platform***	***RSA NetWitness***	***McAfee Enterprise Security Manager***	***IBM QRadar***	***OSSEC***	***AT&T Cybersecurity AlienVault Unified Security Management***
Підтримка різнорідних форматів	-	+	-	+	+	-	+	-	-
Попередньо налаштовані шаблони аномалій	+	+	+	+	+	+	+	+	+
Визначення відхилень у режимі реального часу	-	+	+	-	-	-	+	-	+
Аналітика									
Застосування шаблонів	+	+	+	+	+	+	+	+	+
Окремий аналізатор	+	+	-	-	+	-	+	+	+
Поєднання аналітики з інформацію про загрози від різних постачальників	-	+	-	+	-	+	+	-	-
Застосування машинного навчання	-	+	-	-	+	-	+	-	-

Продовження таблиці 2.1 - Порівняльна характеристика відомих рішень SIEM

Рішення SIEM / Функція	*Manage Engine EventLog Analyzer*	*Splunk Enterprise Security*	*SolarWinds Security Event Manager*	*LogRhythm NextGen SIEM Platform*	*RSA NetWitness*	*McAfee Enterprise Security Manager*	*IBM QRadar*	*OSSEC*	*AT&T Cybersecurity AlienVault Unified Security Management*
Інформація про загрози									
Власне вирішення довідки про загрози	+	+	-	-	+	-	+	-	+
Підтримка основних сумісних із STIX / TAXII каналів та каналів з відкритим кодом	-	-	+	+	-	+	+	-	-
Використання внутрішніх медіакарт	-	+	-	-	-	-	+	-	-
Рівень робочого процесу / автоматизації (Workflow/Automation Layer)									
Автоматизація									
Часткова автоматизація	+	-	+	-	+	+	-	+	+
Повна автоматизація	-	+	-	+	-	-	+	-	-
Полювання на загрози / розслідування	-	-	-	-	+	+	+	-	+
Відповідь на інцидент									
Відповідь на попередньо визначені сценарії	+	+	+	+	+	+	+	+	+

Продовження таблиці 2.1 - Порівняльна характеристика відомих рішень SIEM

Рішення SIEM / Функція	***Manage Engine EventLog Analyzer***	***Splunk Enterprise Security***	***SolarWinds Security Event Manager***	***LogRhythm NextGen SIEM Platform***	***RSA NetWitness***	***McAfee Enterprise Security Manager***	***IBM QRadar***	***OSSEC***	***AT&T Cybersecurity AlienVault Unified Security Management***
Розширена відповідь з використанням ШІ	-	+	-	-	+	-	+	-	-
Відповідність									
Основні звіти про відповідність, необхідні для IT-галузі	+	+	+	-	+	+	+	+	+
Власні спеціальні звіти	-	+	-	+	-	-	+	-	-
Аналіз інцидентів/ «форензіка» (Forensic analysis)	+	+	-	+	-	-	+	-	+
Рівень взаємодії користувачів (User Interaction Layer)									
Попередження									
На основі попередньо визначених правил	+	+	+	+	+	+	+	+	+

Продовження таблиці 2.1 - Порівняльна характеристика відомих рішень SIEM

Рішення SIEM / Функція	*Manage Engine EventLog Analyzer*	*Splunk Enterprise Security*	*SolarWinds Security Event Manager*	*LogRhythm NextGen SIEM Platform*	*RSA NetWitness*	*McAfee Enterprise Security Manager*	*IBM QRadar*	*OSSEC*	*AT&T Cybersecurity AlienVault Unified Security Management*
Виявлення аномалій зі ШІ	-	+	-	-	+	-	+	-	-
Візуалізація									
Стандартна інформаційна панель	+	+	+	+	+	+	+	+	+
Можливість створення власної інформаційної панелі	-	+	-	-	-	-	+	-	+
Багато-панельність	-	+	-	-	+	+	+	-	-
Звітність									
Попередньо визначені шаблони	+	+	+	+	+	+	+	+	+
Можливість створення власних звітів	-	+	-	-	-	-	+	-	-
∑	17	40	22	27	27	22	43	16	27

Продовження таблиці 2.1 - Порівняльна характеристика відомих рішень SIEM

Виконуючи аналіз технічних характеристик, можливостей, цін на запропоновані рішення SIEM, функціоналу, що реалізує виконання гарантування функцій забезпечення кіберстійкості системи, визначаємо:

1. Універсальними рішенням інтелектуальних систем аналітики є QRadar від компанії IBM, McAfee Enterprise Security Manager та Splunk Enterprise Security, що визначаються особливістю – аналітика є ядром функціонування SIEM.

2. Початковим рішенням для будь-якої організацій, що забезпечує основні функції на належному рівні є SolarWinds Security Event Manager

3. Для малих та середніх підприємств з невеликим бюджетом вибором може стати LogRhythm NextGen SIEM Platform або AT&T Cybersecurity AlienVault Unified Security Management

Рішення інтелектуальної системи аналітики забезпечує швидкий результат у випадках:

- розширеного виявлення загроз;
- критичного захисту даних;
- моніторингу загроз від інсайдерів;
- управління ризиками та вразливостями;
- самовільного виявлення трафіку;
- криміналістичного розслідування.

Будь-яке рішення управління загрозами безпеки може мати додаткові вдосконалені сервіси, серед яких:

- інструментування безпеки, автоматизація та реагування (англ. SOAR), яке захищає від загроз і прискорює реагування на інциденти у організації за допомогою динамічних, автоматизованих сценаріїв можливого розвитку подій;
- платформа розвідки про загрози;
- операції та консалтингові послуги, що оцінюють, проектують, створюють та оптимізують середовище безпеки організацій для кращих показників;

- послуги тестування на проникнення та управління окремими вразливостями;
- служби керування загрозами, що забезпечує експертизу безпеки - від тестування засобів захисту до захисту на передовій проти кібератак;
- служби реагування на інциденти та розвідувальні послуги, які надають глибоку розвідку щодо безпеки та перевірку дій на випадок посилення засобів захисту, відповіді на загрози та відновлення рівноваги після атак.

Визначаючи пріоритетність відповіді на інциденти – реалізовані ризики, метою є забезпечення кіберстійкого стану підприємства, що розуміє під собою можливість мінімізації наслідків та пріоритерізації, за якої система повертається до «рівноваги» при збалансованих витратах.

Сучасні кібератаки проводяться в різних векторах і використовують різноманітні техніки, такі як віруси, шпигунське програмне забезпечення, фішинг, шкідливі вкладення електронної пошти [Розділ 1.1]; інциденти складаються з декількох фаз, які вимагають попереднього планування. З'являється необхідність мати видимість у багаторівневому захисті для своєчасного виявлення загроз, разом з можливістю управління ризиками. Задля зменшення зростаючої вразливості до кіберзагроз, світогляд змінюється до забезпечення кіберстійкого стану. Забезпечується це єдиною централізованою системою безпеки - впровадженням рішення Управління інформаційною безпекою та подіями (англ. SIEM).

Результати аналізу контролю заходів безпеки ДСТУ ISO-IEC 27005-2015 [9] (англ. security controls), що охоплюється впровадженням системи SIEM, наведено у таблиці 2.2.

Таблиця 2.2 - Класифікація заходів безпеки, контроль яких охоплюється впровадженням системи SIEM

Мета заходу	**Опис заходу**	**Приклади та практики, що контролюються SIEM**	**Приклади підходів тестування**
Обмеження доступу	Доступ обмежений дозволом на основі посадових обов'язків та принципу найменших привілеїв.	Управління ідентифікацією та доступом (англ. IAM - Identity and Access Management), ідентифікація та аутентифікація користувачів, фізичний захист, обізнаність та навчання співробітників	Тести соціальної інженерії
	Користувач аутентифікується, завдяки чому розмір доступу відповідає чутливості активу, до якого здійснюється доступ.	Політика щодо паролів, контроль автентифікації системи.	Аудити доступу користувачів
	Мережі захищені від несанкціонованого трафіку.	Брандмауери, маршрутизатори, сегментація мережі.	Тести на проникнення.
	Системи захищені від зловмисних атак.	Фільтрація шкідливого програмного забезпечення, Інтернету та електронної пошти.	Нефункціональне тестування.
	Зв'язок між системами (включаючи обмін даними) захищений від несанкціонованого доступу та використання.	Шифрування, управління ключами.	Огляд управління ключами.

Продовження таблиці 2.2 - Класифікація заходів безпеки, контроль яких охоплюється впровадженням системи SIEM

Мета заходу	**Опис заходу**	**Приклади та практики, що контролюються SIEM**	**Приклади підходів тестування**
Виявлення несанкціонованого доступу та використання	Своєчасне виявлення несанкціонованого доступу та використання систем.	Журнали безпеки, рішення для виявлення вторгнень (IDS), рішення щодо виявлення змін цілісності, аналіз подій та процедури ескалації.	Тести на проникнення, тести Red team.
Реагування на несанкціонований доступ та використання	Впорядковане реагування на кіберінциденти.	Процедури з реагування на кібератаки, використання SIEM при управлінні кризисними ситуаціями, безперервності бізнесу.	Настільні вправи, державно-приватні вправи.
Забезпечення максимізування часу безвідмовної роботи систем	Системи здатні впоратися з виходом з ладу окремих компонентів.	Активно-активні, активно-пасивні розгорнуті рішення, укладені рішення, архітектура нульової довіри, актуальність стану яких автоматизовано контролюється SIEM.	Тестування Chaos Monkey, огляд архітектури, тестування відмов.
Забезпечення відновлення, де це можливо	Відновлення з резервних копій, збережених способом, який не може бути скомпрометований одним і тим кіберінцидентом.	Плани відновлення, заходи та випробування, що контролюються SIEM.	Тести на технічне відновлення.

Продовження таблиці 2.2 - Класифікація заходів безпеки, контроль яких охоплюється впровадженням системи SIEM

Мета заходу	Опис заходу	Приклади та практики, що контролюються SIEM	Приклади підходів тестування
Зменшення вразливостей, мінімізуючи впровадження нових вразливостей та вживання заходів для зменшення ризиків	Забезпечення контролю за впровадженням, задля мінімізації введення нових вразливостей внаслідок змін системи; системи захищені конструкцією.	Безпечна розробка програмного забезпечення, нефункціональне тестування, контроль змін, зміцнення системи автоматизована вирішенням управління безпекою та подіями.	Огляд контролю змін, сканування коду, огляд архітектури.
	Нові вразливі місця своєчасно виявляються та усуваються.	Автоматизований та підконтрольний патчінг (англ. patching).	Сканування вразливості, тестування на проникнення, fuzzing
	Нові загрози своєчасно виявляються та усуваються.	Кіберрозвідка, стратегія інформаційної безпеки.	Незалежна перевірка можливостей.
Контроль та керування процесом управління кіберризиками	Особи, що приймають рішення, інформуються щодо достатності кіберконтролю та безпосередньої діяльності за необхідності.	Звіти, форуми з управління, внутрішній аудит також забезпечується SIEM.	Огляди управління, консультаційні огляди, незалежний аудит.

2.2 Алгоритм вибору функціональної SIEM, задля забезпечення кіберстійкості

Кібербезпека передбачає безліч різних технічних та інформаційних рішень, необхідних для захисту та стійкості, проте їх неможливо досягти в повному обсязі без правильного підходу.

Як зазначається, кіберстійкість спрямована на динамічний захист організації з метою своєчасних відповідей на інциденти та підтримки кіберрівноваги [17]. В процесі написання дипломної роботи, визначаємо основні критерії забезпечення кіберстійкості:

1. Захист від загроз. Чим більше технологій прогресує, тим більше розвиваються кіберзлочинці. Застосування лише заходів безпеки не допоможе захистити організацію. Організація повинна спланувати кроки для захисту від різного роду загроз - необхідність постійного моніторингу та реагування на передові загрози.

2. Відновлюваність. Після порушення даних, дані відновлення - повернення організації до регулярної роботи. Організація повинна мати повне резервне копіювання даних, що активно перекриває результати таких інцидентів, коли будь-які/всі дані втрачено. Також рекомендується проводження імітацій кібератак, з метою покращення навчання.

3. Адаптованість. Важливо, щоб організація могла розвиватися та пристосовуватися до нової тактики кіберзлочинців. Вони постійно розвиваються, адаптованість допомагає організаціям в разі загрози.

4. Довговічність. Довговічність організації вимірюється здатністю ефективно вести регулярний та звичайний бізнес після порушення безпеки. Завдяки вдосконаленням системи, регулярним звітам та оновленням, покращиться кіберстійкість організації.

5. Експлуатаційні вимоги. Визначення як платформа аналітики впишеться у процеси управління, пов'язані з операціями, дотриманням вимог, реагуванням на інциденти та загрози та управління ризиками, а також наскільки простим буде управління платформою, чи зможе вона відповідати

вимогам до продуктивності та масштабуватися в міру розширення інфраструктури.

6. Технічні вимоги. Визначення як запропоноване рішення SIEM інтегрується з корпоративною інфраструктурою. Існує завдання задокументувати існуючу технічну інфраструктуру настільки глибоко, щоб постачальник розумів середовище, існувала надійна основа для оцінки реакції постачальника.

7. Вимоги бізнесу. Необхідно зібрати вимоги бізнесу, такі, як витрати в порівнянні з умовами покриття, підтримка та навчання та відповідність законодавству, розглянути відповідну модель розгортання SIEM для організації.

На підставі необхідності прийняття рішення щодо вибору системи забезпечення кіберстійкості при управлінні інформаційною безпекою, визначається потреба у формуванні уніфікованої методики прийняття рішень. Перевага цього полягає у рішенні без додаткових розрахунків. Однак, недоліком є неможливість забезпечення максимально ефективного захисту, оскільки, відповідь на відповідний ризик окремої організації є унікальним. Тобто, методика прийняття рішень для кожної організації може корегуватися із відповідністю до основних бізнес цілей та особливостей інфраструктури.

Очевидно, що ціни на різні рішення SIEM, не завжди будуть вигідними для організації. Тому необхідно порівнювати пропозиції, виходячи із критичності функціональних критеріїв-вимог до системи аналітики.

Узагальнюючи вищенаведене, було розроблено алгоритм вибору інтелектуальної системи аналітики із врахуванням критеріїв кіберстійкості рис. 2.1.

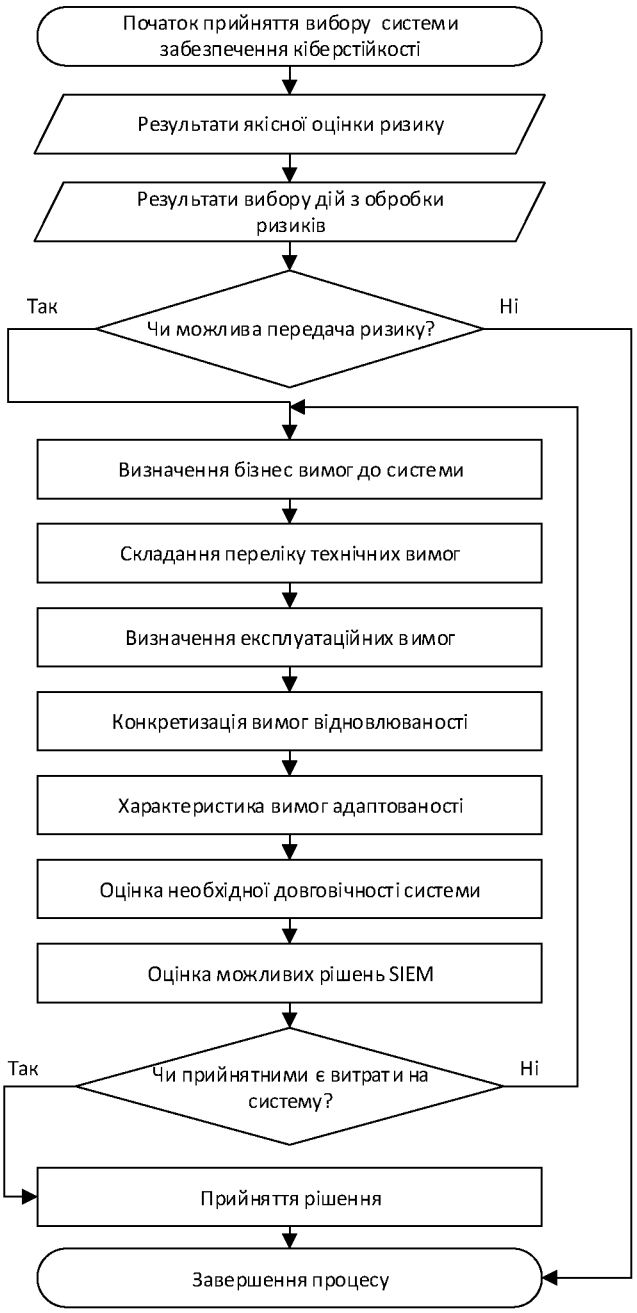

Рисунок 2.1 - Алгоритм методики прийняття рішень щодо вибору системи аналітики з метою забезпечення кіберстійкості

Також необхідно мати можливість тестування заходів безпеки [9] (англ. security controls), діяльність яких контролюється централізованим рішенням. Виконаємо порівняльний аналіз характеристик кіберстійкості ІТС організації та визначмо події, при яких моніторинг діяльності основних заходів є критичним [1] задля своєчасного корегування з метою розвитку системи. Результати аналізу наведено у таблиці 2.3.

Таблиця 2.3 - Події та контрольні цілі тестування діяльності заходів безпеки

	Подія	**Контрольні цілі чи результати тестувань**
До порушення безпеки	- Зовнішнє сканування заблокованих з'єднань (кількість) - Нові вразливості (за типом OWASP (Open Web Application Security Project) (кількість) - Зловмисне програмне забезпечення, що було зупинено (кількість) - Перехід до фішинг-сайтів (кількість) - Видалення результатів відвідування фішинг-сайту (кількість, години роботи) - Націлювання на зловмисне програмне забезпечення (кількість) - Виявлені події безпеки (кількість)	- Тестування на проникнення (за типом: підрахунок та рейтинг знаходження) - Аудит системи, захищених Управлінням ідентифікацією та доступом - Аудит внутрішньо розроблених системи, які неможливо оновити - Аудит систем з компонентами підтримки, що не постачаються - Аудит систем без рішень проти зловмисного програмного забезпечення - Оцінка відповідності конфігурації інформаційної безпеки (% покриття) - Вправи на обізнаність (охоплення%, кількість) - Тестування персоналу, на визначення обізнаності - кількість робітників, хто ведеться на фішинг-тести (% від загальної кількості персоналу) - Огляд доступу користувачів (охоплення%) - Оцінка безпеки постачальників протягом 12 місяців (% охоплення) - Аудит стану патчів (старіння за критичністю: дні) - Звіт про достовірність інформаційної безпеки (результати за рейтингом, старіння до виправлення)
Порушення безпеки	- Виявлені хости зі зловмисним програмним забезпеченням (кількість) - Виявлене шкідливе програмне забезпечення на серверах (кількість) - Порушені інтернет-каталоги, що містять інформацію про персонал / клієнта (кількість) - Тип інциденту протягом періоду (відмова в обслуговуванні, зловмисний код, соціальна інженерія, несанкціонований доступ)	- Розроблені плани вирішення та відновлення (кількість) - Репетиції інцидентів (кількість)

Продовження таблиці 2.3 - Події та контрольні цілі тестування діяльності заходів безпеки

	Подія	**Контрольні цілі чи результати тестувань**
Після порушення безпеки	- Виявлена APT (англ. advanced persistent threat - розвинена стійка загроза) (кількість) - Заблоковані підключення до шкідливих веб-сайтів (кількість) - Виявлені порушення даних (кількість) - Банківські збитки (вартість) - Втрати клієнта (вартість)	- Звіти після інциденту (кількість)

Розглядаючи процес інтеграції платформи SIEM у IT-середовище, слід зауважити, що найкращим способом є поступове впровадження. Це означає прийняття будь-яких рішень окремо. Повинна бути можливість мати функції моніторингу в режимі реального часу та аналізу журналів. Це дає змогу зробити підсумки IT-середовища організації та налагодити процес прийняття. Таке впровадження системи SIEM допомагає виявити, чи залишається організація відкритою для зловмисних атак та переконатися, що використання системи SIEM чітко перекриває поставлені цілі.

На початкових етапах впровадження системи SIEM потрібно готуватися до найгіршого сценарію. Підготовка до найгіршого сценарію означає, що організація готова вирішувати найсуворіші атаки, оскільки краще бути занадто захищеним від кібератак, ніж недостатньо.

Проведення оцінки можливих рішень розгортання SIEM слід обробляти за встановленою процедурою. З цією метою SANS Institute розробив окремий Посібник оцінювача до NextGen SIEM (англ. Evaluator Guide to NextGen SIEM) [15].

Базуючи на цьому, підприємство має змогу представити приблизну структурну будову рішення для порівняння з топологією ITC, що існує на підприємстві, з метою оцінки змін, які необхідно провести. Візуалізація типової довідкової архітектури SIEM наведена на рисунку 2.2.

Рішення SIEM, розширене інструментами вразливості та управління ризиками, також мінімізує ризики невідомих вразливостей, виявляючи прогалини в безпеці як в програмному, так і в апаратному забезпеченні.

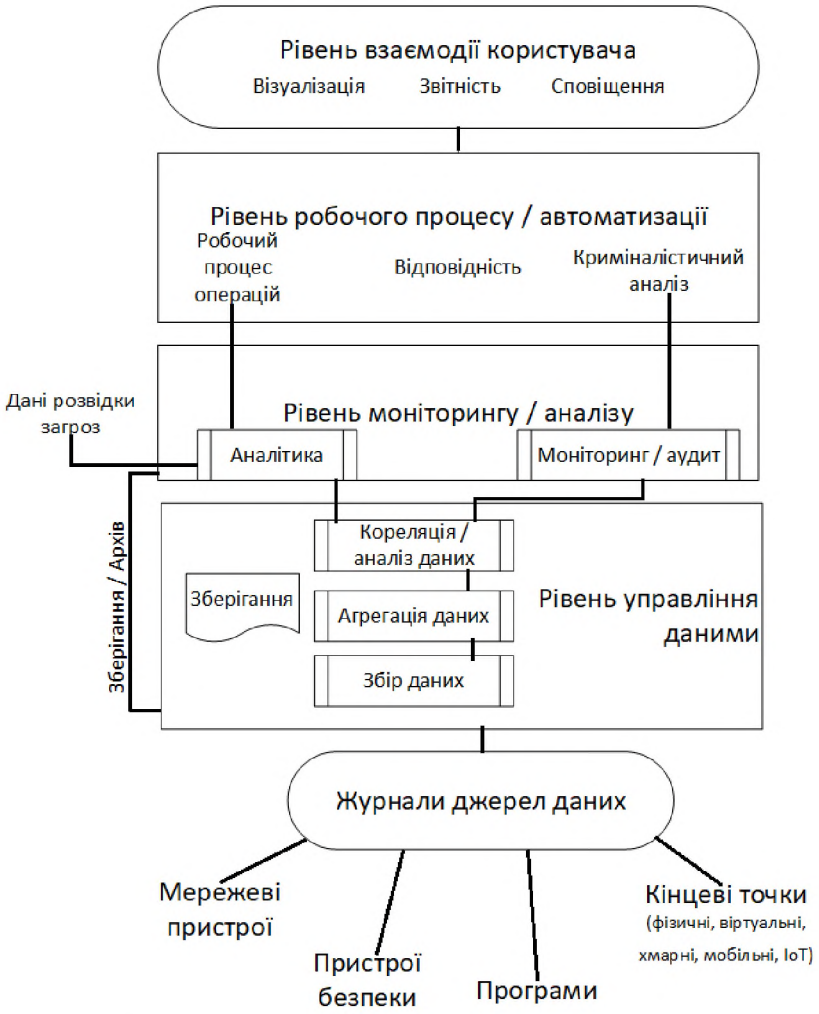

Рисунок 2.2 - Структура типової SIEM

Придбання та розгортання SIEM - проект, що стосується всього бізнесу. Оцінка та закупівлі повинні управлятись як самостійний проект із залученням спеціального керівника проекту та команди, призначених ресурсів, бюджету та графіку.

Беручи до уваги, що топологія кожного підприємства є здебільшого унікальною, не існує єдиних загально визначених вимог для впровадження SIEM системи. Оскільки існує безліч різних варіантів побудови системи у інфраструктурі підприємства, як було зазначено у розділі 1.3, організаціями необхідно зосередитись саме на вимогах до впроваджуваної системи.

Таким чином, за умови використання розробленої методології вибору рішення системи SIEM для впровадження на підприємстві, забезпечується можливість перекриття управління ризиками як підтримка кіберстійкого стану

організації у відповідь на атаки – оптимально можливе рішення у сучасному світі постійно еволюціонуючих кіберзагроз.

2.3 Реалізація запропонованого підходу

2.3.1 Рекомендації для впровадження системи

Розглянемо процес впровадження SIEM з аналітикою, що є ядром функціонування системи, на типовому підприємстві при наступних вимогах об'єкта:

1. Захист від загроз:

- *Моніторинг / аудит:* моніторинг багатьох хостів; підтримка різнорідних форматів; попередньо налаштовані шаблони аномалій; визначення відхилень у режимі реального часу;
- *Аналітика:* застосування шаблонів; окремий аналізатор; поєднання аналітики з інформацію про загрози від різних постачальників; застосування машинного навчання;
- *Полювання на загрози / розслідування*;
- *Відповідь на інцидент:* відповідь на попередньо визначені сценарії; розширена відповідь з використанням ШІ;
- *Аналіз інцидентів/ «форензіка» (Forensic analysis).*

2. Відновлюваність:

- *Наявність надмірнісності.*

3. Адаптованість:

- *Інформація про загрози:* власне вирішення довідки про загрози; підтримка основних сумісних із STIX / TAXII каналів та каналів з відкритим кодом; використання внутрішніх медіакарт.

4. Довговічність:

- *Можливість оновлення.*

5. Експлуатаційні вимоги:

- *Збір даних:* стандартна інфраструктура централізованого управління хостом; журнали даних мережевих пристроїв; журнали даних приладів безпеки;
- *Агрегація даних:* на основі заздалегідь визначених правил; зведене індексування, при структуруванні ризиків; багатозадачність; використання ШІ;
- *Кореляція та аналіз даних:* попередньо налаштовані алгоритми/ шаблони; розширена кореляція; історична кореляція; окремий механізм кореляції;
- *Повна автоматизація*;
- *Попередження*: на основі попередньо визначених правил; виявлення аномалій зі ШІ;
- *Візуалізація*: стандартна інформаційна панель; можливість створення власної інформаційної панелі; багато-панельність.

6. Технічні вимоги:

- *Зберігання:* окрема база даних; додаткові метадані, збагачені контекстом безпеки; можливість уніфікації формату;
- *Утримання:* безстроково (в залежності від стандартів відповідності); підтримка різнорідних форматів.

7. Вимоги бізнесу*:*

- *Зберігання:* необмежений період зберігання; можливість хмарного вирішення;
- *Відповідність:* основні звіти про відповідність, необхідні для IT-галузі; власні спеціальні звіти;
- *Звітність*: попередньо визначені шаблони; можливість створення власних.

Аналізуючи визначені критерії до впровадження та враховуючи результати порівняння систем аналітики [таблиця 2.1], можемо зробити висновок, що максимально задовольняє вимогам функцій кіберстійкості QRadar від компанії IBM, що є максимально повнофункціональною системою.

На прикладі QRadar розглянемо обрану архітектуру SIEM та процес функціонування системи більш детально.

Архітектура IBM QRadar [28] підтримує розгортання різних розмірів та топологій, починаючи від одного хост-розгортання, де всі програмні компоненти працюють в одній системі, до декількох хостів, включаючи різноманітні пристрої - колектори подій, потоків, вузли даних, процесори подій та інші. Перший варіант розгортання полягає в одному вирішенні багатофункціонального пристрою для середньої компанії, подальші приклади описують варіанти розгортання в міру розширення компанії.

Вимоги до розгортання QRadar залежать від здатності обраного розгортання як обробляти, так і зберігати всі дані, що будуть проаналізовані у мережі.

На рисунку 2.3 показані компоненти QRadar, які використовуються для збору, обробки та зберігання даних про події та потоки.

Рисунок 2.3 - Складові подій та потоків QRadar

Головними складовими сучасної SIEM є:

1. Події безпеки:

- системи виявлення вторгнень (англ. Intrusion Detection Systems);
- антивірус, антивірусні програми (англ. Endpoint Security);
- запобігання втраті даних (англ. Data Loss Prevention) ;
- концентратори VPN;
- веб-фільтри;
- медонки (англ. Honeypots) ;
- брандмауери (англ. Firewalls).

2. Журнали мережі:

- маршрутизатори;
- комутатори;
- DNS-сервери (англ. Domain Name System);
- точки бездротового доступу (англ. Wireless Access Points) ;
- широкообласна мережа (англ. WAN - Wide Area Network) ;
- потоки передачі даних;
- приватні хмарні мережі (англ. VPC - Virtual private cloud).

3. Програми та пристрої:

- сервери додатків;
- бази даних;
- інтранет-програми;
- веб-додатки;
- додатки SaaS (англ. Software as a service - Програмне забезпечення як послуга);
- хмарні сервери;
- ноутбуки або настільні комп'ютери для кінцевих користувачів;
- мобільні пристрої.

4. IT-інфраструктура:

- конфігурації;
- локація;
- власники активів;

- карти мережі;
- звіти про вразливості;
- інвентаризація програмного забезпечення.

QRadar збирає, обробляє, агрегує та зберігає мережеві дані в режимі реального часу для управління мережевою безпекою, надаючи інформацію та моніторинг у режимі реального часу з можливістю забезпечення попередження порушення та відповіді на мережеві загрози, з метою забезпечення кіберстійкого стану організації.

QRadar SIEM має модульну архітектуру, яка забезпечує видимість IT-інфраструктури в режимі реального часу, підтримує можливість додавання інтегрованих модулів до платформи, таких як QRadar Risk Manager, QRadar Vulnerability Manager (англ. Менеджер вразливостей) та QRadar Incident Forensics (англ. Криміналістика інцидентів), з метою розширення функціональності.

Функціонування платформи безпеки QRadar складається з трьох рівнів і застосовується до будь-якої структури розгортання QRadar, незалежно від розміру та складності. На рисунку 2.4 показано рівні, що складають архітектуру операцій QRadar [27].

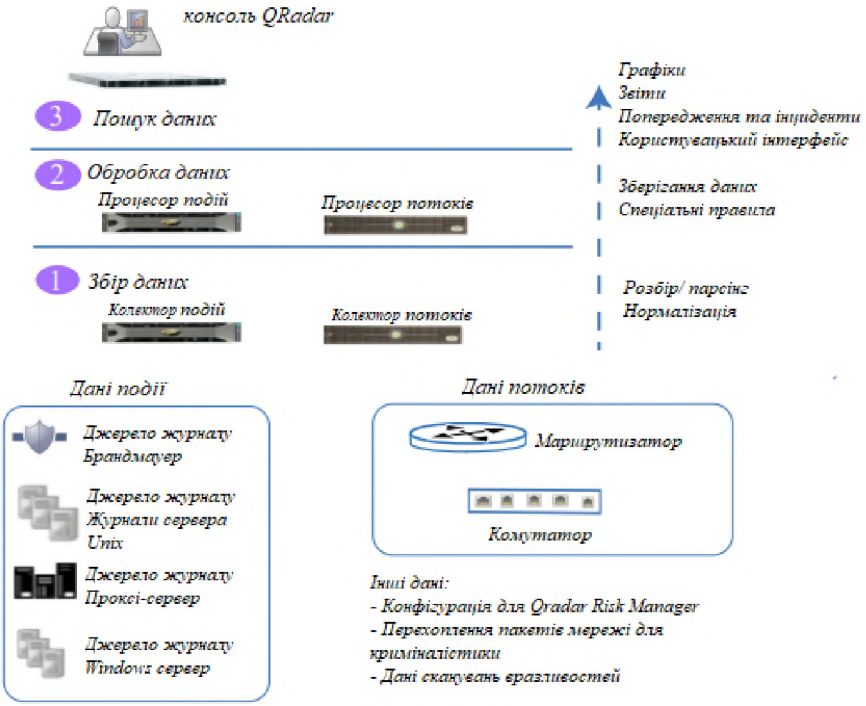

Рисунок 2.4 - Архітектура операцій QRadar

Збір даних - перший рівень, де дані, такі як події чи потоки, збираються з мережі. Рішення «all-in-one» (англ. «все в одному») можна використовувати для збору даних безпосередньо з мережі, тоді як колектори, такі як QRadar Event Collectors (англ. Колектори подій) або QRadar QFlow Collectors (англ. Колектори потоків), служать для збору даних про події або потоки. Дані аналізуються та нормалізуються до того, як вони будуть передані на рівень обробки, задля представлення у структурованому та придатному для використання форматі.

Функціональність орієнтована на збір даних про події та потоки. Дані подій представляють події, що відбуваються в певний момент часу в середовищі користувача, такі як входи до систем, електронна пошта, підключення до VPN (англ. Virtual Private Network - Віртуальна приватна мережа), відмова брандмауера, проксі-з'єднання. Дані потоку - інформація про мережеву активність або інформація про сеанси між двома хостами в мережі.

Другий рівень операцій - рівень обробки даних - місце, де дані про події та потоки проходять через механізм спеціальних правил (англ. CRE - Custom Rules Engine), який генерує порушення та попередження, після чого дані записуються на зберігання.

Дані про події та потоки можуть оброблятися універсальним пристроєм без необхідності додавання процесорів подій або потоків. Якщо об’єм обробки багатофункціонального пристрою перевищений, необхідно додати процесори подій/потоів або будь-який інший пристрій обробки.

Інші функції, такі як QRadar Risk Manager (QRM), QRadar Vulnerability Manager (QVM) або QRadar Incident Forensics, збирають різні типи даних і надають більше функцій. QRadar Risk Manager збирає конфігурацію мережевої інфраструктури та надає схему топології мережі. QRadar Vulnerability Manager забезпечує сканування мережі, обробки даних про вразливості або управління даними про вразливості, які збираються з інших сканерів, таких як Nessus та Rapid7. QRadar Incident Forensics надає можливість для проведення поглиблених криміналістичних розслідувань та відтворення повних мережевих сесій.

На третьому, верхньому, рівні, дані, які збирає та обробляє QRadar, доступні користувачам для пошуку, аналізу, звітності, попереджень або розслідування інцидентів. Користувачі можуть шукати та керувати завданнями адміністратора безпеки для мережі за допомогою інтерфейсу користувача на консолі QRadar.

У системі «все в одному» всі дані збираються, обробляються та зберігаються на приладі багатофункціонального пристрою. У розподілених середовищах, консоль QRadar не виконує обробку або зберігання подій та потоків, а використовується переважно як користувальницький інтерфейс для пошуку, звітів, попереджень та розслідувань.

З метою гарантування кіберстійкості систем підприємства, на сьогоднішній день існують додаткові можливості - інструментування безпеки, автоматизація та реагування (SOAR).

Завдяки інтеграції платформи IBM Resilient SOAR [33] з QRadar розширюються можливості системи управління ризиками, охоплюючи ширший діапазон виявлення, розслідування та виправлення загроз.

Технологічна інтеграція між двома рішеннями дозволяє швидко та ефективно синхронізувати інциденти з QRadar на Resilient, автоматизовано збагатити метадані та керувати повним процесом розслідування.

Поєднання Resilient SOAR з розгортанням QRadar розблоковує додаткові функції:

- поєднання інтелекту та розуміння з автоматизацією та інтеграцією;
- швидше реагування на атаки;
- удосконалення процесів до та після інцидентів.

QRadar надає аналітикам всебічну видимість, максимізуючи інформацію про загрози та ризики. Завдяки Resilient зростає можливість отримувати відомості про загрози та швидко діяти, за допомогою налаштовуваних робочих процесів та динамічних посібників (англ. playbook).

Коли QRadar виявляє загрозу на початку, Resilient може вдосконалити процес реагування. Завдяки керованому реагуванню, існує можливість використання перевірених планів реагування на інциденти, сповнених етапів від

розслідування інцидентів до виправлення. Впровадження підтримки MITRE (англ. Massachusetts Institute of Technology Research & Engineering - Массачусетський інститут технологічних досліджень та інженерії) ATT&CK (англ. adversarial tactics, techniques, and common knowledge - тактики, прийоми та загальновідомі знання супротивників) [44] у програмі QRadar Advisor разом з Watson (штучний інтелект, розроблений IBM) також дозволяє Resilient збагачувати інформацію про інцидент та потенційно здійснювати процес реагування на основі аналізів, отриманих з тактик, технік та процедур (англ. TTP - Tactics, Techniques and Procedures) MITRE.

Стратегія управління ризиками організації може допомогти розробити конкретні підходи для покращення розвідки про загрози та активного захисту від передових кіберсупротивників, що може бути впроваджено завдяки динамічним посібникам Resilient.

Разом QRadar та Resilient забезпечують наскрізне рішення щодо управління загрозами, яке може прискорити та посилити процес реагування на інциденти, поєднуючи точне виявлення загрози, управління, інструментування та автоматизацію, а також штучний та людський інтелект.

Сучасні системи забезпечення інформаційної безпеки є продуктом масштабних зусиль. Принципи проектування забезпечують загальну структуру, що дозволяє тим, хто бере участь у розробці, експлуатації та підтримці системи, зрозуміти принципи побудови задля подальшого функціонування - розвитку архітектури, дизайну та реалізації. Зі збільшенням занепокоєння щодо кіберстійкості, зростає необхідність включати принципи проектування кіберстійкості до набору вимог проектування і самої системи забезпечення даного стану організації, з метою відображення кіберстійкості у відповідному плані захисту програми або плані безпеки.

Розглядаючи обрану архітектуру одного із відомих рішень систем аналітики, було розглянуто принципи стратегічного проектування кіберстійкості, специфічні для врахування передових кіберзагроз, підходи до зменшення ризиків, узгоджені з інженерною стійкістю та виживаністю, що відповідають обмеженням.

Можливість балансування автоматизації, інструментування та управління ризиками Resilient та управління ризиками з виявленням та кореляцією QRadar, допомагає визначити пріоритет на критичних інцидентах, зменшити навантаження на розслідування інцидентів, пришвидшивши процес операцій з безпеки, що забезпечує гарантування кіберстійкого стану організації.

2.3.2 Встановлення критеріїв угоди про рівень обслуговування

Аналізуючи ринок постачальників послуг з кібербезпеки та актуальні рішення систем SIEM, визначаємо, що головним документом є угода про рівень обслуговування (SLA) [34]. SLA визначає кредити на послуги, які будуть надані, якщо постачальник послуг не відповідає цільовим рівням обслуговування.

SLA функціонує орієнтуючись на наступні визначення:

«Максимально доступні хвилини» - загальна кількість хвилин протягом розрахункового місяця, протягом яких захищений вузол було розгорнуто та налаштовано для моніторингу безпеки.

«Час простою» - загальна кількість накопичених хвилин протягом розрахункового місяця, протягом яких інформація моніторингу безпеки для захищеного вузла недоступна.

«Щомісячний відсоток безвідмовної роботи» для захищеного вузла в даному розрахунковому місяці обчислюється як максимально доступні хвилини за вирахуванням простоїв, поділених на максимально доступні хвилини.

Щомісячний час безвідмовної роботи = (Максимально доступні хвилини - Час простою) / Максимально доступні хвилини

Дані норми визначають рівень якості послуг, що надаються постачальником, у разі порушення, постачальник сплачує пенальті.

Визначаючи можливі складові надання сервісу SIEM системи, підприємство повинно встановити часові цілі для наступних характеристик:

- доступність сервісу;
- доступність порталу провайдера;

- повідомлення про пріоритет високого ступеня загрози (повинно бути звітовано у періоді від 15 хвилин до 1 години), канал зв'язку може включати електронну пошту та телефон;
- повідомлення про інцидент середнього ступеня важкості (має бути звітовано у середньому обсязі до 6-12 годин);
- повідомлення про інцидент малого пріоритету (на протязі 24 годин від моменту детекції);
- повідомлення про рівень працездатності системи.

В свою чергу, визначаючи рівень технологічних вимог до базового рівня SIEM системи, головними характеристиками є:

- події в секунду (англ. EPS - Events per Second);
- правопорушення/інциденти на місяць (англ. OPM - Offenses per Month);
- сповіщення/тривоги на місяць (англ. APM - Alerts per Month);
- базові журнали вхідних даних (англ. Log Source Baseline) та їх типи;
- кількість унікальних випадків використання (у доповнення до певних правил, повинна існувати можливість визначення унікальних випадків, у яких підприємство є зацікавленим у звітуванні з відповідним пріоритетом).

Постачальники, як правило, пишуть SLA, тому керівництво підприємства та юридичний персонал зобов'язані забезпечити найкраще задоволення прав та потреб підприємства. Сфери, які слід ретельно розглянути:

1. Положення щодо делегованого та / або спільного контролю повинні бути детально описані в SLA. Це особливо важливо, якщо постачальнику доручено контролювати та діяти у випадку інцидентів, які потім будуть оброблені аналітиками обох сторін.

2. Вимоги щодо наявності, обробки, зберігання та розпорядження конфіденційною інформацією, повинні бути конкретно зазначені, включаючи географічне розташування журналів та даних безпеки (відповідність).

3. Будь-які вимоги щодо шифрування даних, що перебувають у стані спокою та / або в русі, повинні бути детально окреслені, зокрема, хто зберігає та / або контролює ключові матеріали.

4. Повинні бути прописані детальні вимоги щодо реагування на аварії, безперервність бізнесу та процедури, операції з відновлення після аварій.

5. Домовленості сторонніх аудиторів повинні бути чітко визначеними. Це особливо важливо, якщо правоохоронні органи вимагають доступу до даних, зібраних постачальником.

6. Процедури сповіщення, якщо постачальник SIEM отримує юридичний наказ про надання доступу до даних, які можуть містити дані організації.

7. Вимога забезпечення, щоб дані, зібрані постачальником послуг, збиралися та зберігались у судово-надійному порядку, що відповідає юридичним вимогам конкретної країни та регуляторним правилам.

8. Вимоги щодо доступності, включаючи канали зв'язку між постачальником SEIM та організацією та час сповіщень інцидентів.

9. Конфіденційність та безпека даних.

10. Можливість аудиту постачальника SIEM та їх об'єктів. Це може бути особливо важливим, якщо підприємству потрібен аудит SSAE 16 (англ. Statement on Standards for Attestation Engagements № 16 - Заява про стандарти з питань атестації № 16) або SAS 70 (англ. Statement on Auditing Standards № 70 - Заява про стандарти аудиту № 70), аудит PCI або інший аудит, задля демонстрування здатності дотримуватися вимог регулювання.

11. Гарантії ефективності та гарантії, якщо постачальник SIEM поводиться недбало.

Регулярний запит на зміну SLA також може мати місце. Повинен прийматися на протязі 24 годин після запиту, впровадження відбувається під час вікна технічного обслуговування.

Визначаючи рівень аутсорсингу, важливим є встановлення рівнів підтримки аналітиків. У наступній таблиці детально описуються рівні підтримки актуальної системи на сьогодні.

Таблиця 2.4 - Рівні підтримки SIEM системи

Підтримка рівня	Опис
Підтримка рівня 1	Усі випадки підтримки починаються з рівня 1, де створюється початковий квиток. Проблема виявлена та чітко задокументована, розпочато основне усунення несправностей.
Підтримка рівня 2	Усі випадки підтримки, які неможливо вирішити за допомогою підтримки рівня 1, перекваліфікуються до рівня 2, де більш досвідчені спеціалісти можуть надавати більш складну підтримку.
Підтримка рівня 3	Усі випадки підтримки, які не можуть бути вирішені підтримкою рівня 2, перекваліфікуються до рівня 3, де підтримку надають найбільш кваліфіковані та досвідчені інженери, які мають можливість співпрацювати зі додатковими джерелами та системами для вирішення найскладніших питань.

Зрештою, контракти та юридичний відділ організації нестимуть відповідальність за критичне вивчення та затвердження умов будь-яких SLA для захисту підприємства. Вище керівництво зобов'язане забезпечити, щоб усі потенційні проблеми були розглянуті та зрозумілі заздалегідь. Підписант повинен ретельно розуміти мінуси та найгірші випадки систем SIEM, щоб забезпечити включення відповідних положень до SLA. В ідеалі, провайдери повинні включати пункти про відшкодування збитків, щоб, у разі помилок, які є дорогими для клієнтів, постачальник SIEM повинен був забезпечити грошову компенсацію для покриття заподіяної шкоди.

Висновки до Розділу 2

Першочерговим завданням для організації, що вирішує використовувати кібербезпеку як послугу, є вивчення передумов, кваліфікації, повноважень та репутації постачальника перед укладанням угоди про обслуговування, що містить детальну інформацію про послуги, надані права доступу та положення щодо безпеки доступу до мережі.

Порівнюючи можливі рішення аутсорсингу, визначається, що оптимальним є Управління інформаційною безпекою та подіями (SIEM). Цей підхід поєднує дані про мережевий трафік / події з різних джерел і співвідносить їх з метою виділення елементів (аномалій), які потребують подальшого дослідження. Завдяки можливості розгортання рішень SIEM як внутрішньо, так і використання аутсорсингу з цією ціллю, Управління інформаційною безпекою та подіями стає ключовим рішенням серед інших інтелектуальних систем аналітики посеред підприємств будь-якого розміру та сфери діяльності задля забезпечення кіберстійкості. Гарантується видимість у багаторівневому захисті для своєчасного виявлення загроз, разом з можливістю управління ризиками на всіх рівнях. Задля зменшення зростаючої вразливості до кіберзагроз, світогляд змінюється до забезпечення кіберстійкого стану, що і задовольняється єдиною централізованою системою безпеки - впровадженням рішення Управління інформаційною безпекою та подіями.

Встановлення рішення SIEM - один із найефективніших інструментів при управлінні ризиками: запобігання інцидентів із безпеки, виявлення загроз в мінімальні проміжки часу, допомога організації дотримуватися вимог та регламенту - реалізація кіберстійкого стану. Дотримуючись викладених вище практик та обравши правильного постачальника, організація можете забезпечити безперебійну реалізацію рішення SIEM.

РОЗДІЛ 3 ЕКОНОМІЧНИЙ РОЗДІЛ

3.1 Вступ

Метою даного розділу є аналіз економічної ефективності впровадження інтелектуальної системи аналітики з метою забезпечення кіберстійкості підприємства. Для розрахунку економічної ефективності методу необхідно брати до уваги такі аспекти:

- потенціальні фінансові втрати від реалізації кіберзагроз;
- комплексні витрати при застосуванні різних, взаємно-непов'язаних методів виявлення атак у ІТС, що використовуються на підприємствах;
- капітальні та експлуатаційні витрати для зниження ризику за допомогою засобів захисту;
- показник різниці між ресурсними витратами при впровадженні поодиноких методів захисту, що застосовуються, та підходу, що досліджувався;
- аналіз доцільності та ефективності впровадження досліджуваного методу.

Враховуючи різнорідну природу методів здійснення атак, необхідно проаналізувати ефективність системи у контексті здатності до використання при сценаріях атак, що раніше не реєструвалися.

При впровадженні досліджуваного методу на практиці необхідно враховувати такі ризики:

- неправильний підбір коефіцієнтів різних показників, від точності яких залежить ефективність виявлення конкретної атаки та аномалій в цілому;
- відказ системи моніторингу діяльності та аналізу рішень, що приймаються;
- висока вартість реалізації системи, через що впровадження системи може затягуватися чи бути унеможливлене;
- рівень універсальності методу.

Для зменшення цих ризиків необхідно обговорювати можливість забезпечення надмірності - наявності відмовостійкого рішення - другої централізованої консолі, що є повним бекапом основної, і, вразі відмови, одразу може бути активована (пасивно-активне комунікаційне рішення).

Суттєво зменшити ризики дозволить також методика навчання персоналу, що аналізуватиме та проводитиме моніторинг ефективності системи виявлення на постійній основі, включаючи як аналітичні, так і технічні характеристики.

Якщо окремі вимоги не можуть бути виконані через нестачу ресурсів, то постійному контролю повинні піддаватися проблеми та недоліки, що вже існують і відомі. Вирішення цих проблем може переглядатися та модифікуватися задля оптимізації витрат та поступове зменшення ризиків.

При відсутності належного контролю за станом відомих проблем та аналізу можливої вразливості у системі можуть з'являтися серйозні проблеми різних аспектів: інформаційна безпека, швидкість роботи системи, стан технічного обладнання, показник корисної дії системи.

З цією метою ефективним є рішення передачі ризику третій стороні – компанії з аутсорсингу послуг кібербезпеки, що зможе забезпечити усі належні питання – від технічного обслуговування (при повній передачі системи SIEM) до послуг моніторингу (часткова передача обов'язків). Можливі рішення наведені у розділі 1.3 (таблиця 1.4).

3.2 Розрахунок капітальних витрат

До фіксованих витрат, що повинні бути здійснені в рамках реалізації інтелектуальної системи кіберзахисту, необхідно включити:

- вартість створення документації проекту реалізації інтелектуальної системи;
- витрати на залучення зовнішніх консультантів;
- вартість апаратного та ліцензійного програмного забезпечення, необхідного для реалізації;

- вартість створення програмного забезпечення без урахування витрат на підтримку та обслуговування;
- витрати на впровадження методів інтеграції нового методу із середовищем, що вже функціонує.

3.2.1 Визначення витрат на створення програмного продукту

Для розрахунку загальної вартості реалізації забезпечення кіберстійкості через впровадження інтелектуальної системи необхідно враховувати такі показники:

- трудомісткість розробки та опрацювання реалізованого методу;
- витрати при застосуванні системи аналітики.

Трудомісткість розробки методу впровадження інтелектуальної системи аналітики можна розрахувати за формулою (3.1):

$$t = t_{тз} + t_{в} + t_{а} + t_{пр} + t_{опр} + t_{д}, \text{ годин} \qquad (3.1)$$

де $t_{тз}$ - час складання технічного завдання на розробку;

$t_{в}$ - тривалість опрацювання технічного завдання;

$t_{а}$ – тривалість розробки проекту інтелектуальної системи аналітики;

$t_{пр}$ - тривалість процесу імплементації;

$t_{опр}$ - час опрацювання реалізованого методу на ПК;

$t_{д}$ - час розробки експлуатаційної документації для даного рішення системи.

Враховуючи варіативність часу виконання роботи та вибір підходу до проектування через різну кваліфікацію розробників, у розрахунку економічної ефективності досліджуваного методу буде використовуватися кваліфікація та рівень навичок спеціаліста середньої ланки. Досвід роботи такого спеціаліста, зазвичай, складає від двох років, та включає в себе взаємодію як із об’єктом дослідження, так і зі спорідненими сферами.

Умовну кількість операторів системи виявлення можна визначити за формулою (3.2):

$$Q = q \times c \times (1 + p), \text{ штук,} \quad (3.2)$$

де q – очікувана кількість операторів;

c – коефіцієнт складності системи аналітики;

p – коефіцієнт корекції системи у процесі опрацювання.

Коефіцієнт складності системи аналітики, що розробляється, відносно типового завдання складатиме:

$$c = 1{,}8.$$

Можлива корекція алгоритму не є багато вірогідною через сталість схеми побудови системи, а також через кінцеву кількість компонентів.

$$p = 0{,}07.$$

Очікувана кількість операторів логіки аналітики складає:

$$q = 50.$$

Враховуючи параметри, що приведені вище, умовна кількість операторів логіки аналітики системи, що розробляється, складатиме:

$$Q = 50 \times 1{,}8 \times (1 + 0{,}07) = 96 \text{ (штук).}$$

Приймаючи середню кваліфікацію спеціаліста та специфіку роботи, складові показника трудомісткості розробки та опрацювання реалізованого методу будуть такі:

- Час складання технічного завдання на розробку програмних рішень:

$$t\text{тз} = 18 \text{ години;}$$

- Тривалість опрацювання технічного завдання визначається за формулою (3.3):

$$t\text{в} = \frac{Q \times B}{(75 \ldots 85) \times k}, \text{ годин,} \quad (3.3)$$

де В – коефіцієнт збільшення тривалості роботи над розробкою через недостатнього опису завдання;

k – коефіцієнт, що залежить від стажу розробника.

Приймаючи відповідні значення для даних коефіцієнтів, маємо такі результати:

$$B = 1{,}4;$$

$$k = 1{,}0;$$

$$t\text{в} = \frac{96 \times 1{,}4}{75} = 1{,}8 \text{ (годин)}.$$

Тривалість розробки проекту (алгоритму), за яким працюватиме система, розраховується за формулою (3.4):

$$ta = \frac{Q}{(20 \ldots 25) \times k}, \text{ годин.} \qquad (3.4)$$

Тривалість розробки алгоритму складатиме:

$$ta = \frac{96}{20} = 4{,}8 \text{ (годин)}.$$

Тривалість процесу імплементації рішення системи розраховується за формулою (3.4) і складатиме:

$$t\text{пр} = \frac{96}{20} = 4{,}8 \text{ (годин)}.$$

Час опрацювання реалізованого методу на ПК можна розрахувати за наступною формулою (3.5):

$$t\text{опр} = \frac{1{,}5 \times Q}{(4 \ldots 5) \times k}, \text{ годин.} \qquad (3.5)$$

Час опрацювання реалізованого методу на ПК:

$$t\text{опр} = \frac{1{,}5 \times 96}{4} = 36 \text{ (годин)}.$$

Час розробки експлуатаційної документації для даного рішення системи можна розрахувати за формулою (3.6):

$$t_{\text{д}} = \frac{Q}{(15 \dots 20) \times k} + \frac{Q}{(15 \dots 20)} \times 0{,}75, \text{годин.} \qquad (3.6)$$

Час розробки експлуатаційної документації складатиме:

$$t_{\text{д}} = \frac{96}{16} + \frac{96}{16} \times 0{,}75 = 10{,}5 \text{ (годин)}.$$

Загальна трудомісткість розробки методу впровадження інтелектуальної системи аналітики, метою якої є забезпечення кіберстійкого стану організації складатиме:

$$t = 18 + 1{,}8 + 4{,}8 + 4{,}8 + 36 + 10{,}5 = 76 \text{ (годин)}.$$

3.2.2 Розрахунок витрат на створення методу впровадження інтелектуальної системи аналітики

Для розрахунку загальних витрат на створення методу впровадження системи необхідно визначити необхідні витрати на заробітну плату виконавця роботи та витрати машинного часу.

Витрати на заробітну плату виконавця роботи можна розрахувати за формулою (3.7):

$$\text{Ззп} = t \times \text{Зпр}, \quad \text{грн}, \qquad (3.7)$$

де t – загальна тривалість створення методу впровадження інтелектуальної системи аналітики у годинах;

Зпр – середньогодинна заробітна платня розробника.

За результатами вивчення ринку послуг реалізації та впровадження систем аналітики середньогодинна заробітна платня розробника складатиме:

Зпр = 565 грн/год.

Витрати на заробітну плату виконавця складатимуть:

$$Ззп = 76 \times 565 = 43\,000 \text{ (грн)}.$$

Для розрахунку вартості машинного часу для налагодження реалізованого методу впровадження системи аналітики використовується формула (3.8):

$$Змч = (tопр + tд) \times Смч, \quad \text{грн}, \qquad (3.8)$$

де tопр - час опрацювання реалізованого методу на ПК, у годинах ;

tд - час розробки експлуатаційної документації для даного рішення системи можна розрахувати за формулою, у годинах;

Смч – вартість однієї години машинного часу, грн/година.

Вартість однієї години машинного часу визначається за формулою (3.9):

$$Смч = P \times tнал \times Ce + \frac{Фзал \times На}{Fp} + \frac{Клпз \times Напз}{Fp}, \text{грн}, \qquad (3.9)$$

де P - встановлена потужність ПК, кВт;

Ce - тариф на електричну енергію, грн/кВт·година;

Фзал - залишкова вартість ПК на поточний рік, грн.;

На - річна норма амортизації на ПК, частки одиниці;

Напз – річна норма амортизації на ліцензійне програмне забезпечення, частки одиниці;

*К*лпз - вартість ліцензійного програмного забезпечення, грн.;

Fp – річний фонд робочого часу.

Вартість машинного часу визначається враховуючи комплект стандартного персонального комп'ютера. Первісна вартість ПК визначається виходячи з фактичного терміну його експлуатації як різниця між первісною вартістю та зносом за час використання. Вартість стандартного монітору та системного блоку виробника Lenovo становить 10000 грн. При нормі амортизації у п'ять років, споживання даного комплекту складає 0,5 кВт/год.

Річна норма амортизації розраховується за формулою 3.10 [14]:

$$H_A = 1 - \sqrt[n]{\frac{Ф_{ЛКВ}}{Ф_{ПЕРВ}}}, \text{ грн/год} \qquad (3.10)$$

При вартості електроенергії 1,68 грн., маємо показник вартості машинного часу:

$$\text{Смч} = 16{,}3 \text{ грн.}$$

Тоді згідно з формулою (3.9) вартість години машинного часу становить:

$$C_{МЧ} = 0{,}5 \cdot 1 \cdot 1{,}68 + \frac{10000 \cdot (1 - \sqrt[5]{\frac{2000}{10000}}) \cdot}{1920} + \frac{27000 \cdot (1 - \sqrt[3]{\frac{0}{27000}})}{1920} = 16{,}3 \text{ (грн).}$$

Вартість машинного часу для налагодження методу впровадження системи аналітики складатиме:

$$\text{Змч} = (36 + 10{,}5) \times 16{,}3 = 758 \text{ (грн).}$$

Визначити остаточні капітальні витрати на проектування та впровадження методу виявлення атак можна за формулою (3.11):

$$К = К_{пр} + К_{зпз} + К_{пз} + К_{аз} + К_{навч} + К_{н}, \qquad (3.11)$$

де $К_{пр}$ – вартість розробки проекту інформаційної безпеки та залучення для цього зовнішніх консультантів, тис. грн;

$К_{зпз}$ – вартість закупівель ліцензійного основного й додаткового програмного забезпечення (ПЗ), тис. грн;

$К_{пз}$ – вартість створення основного й додаткового програмного забезпечення, тис. грн;

$К_{аз}$ – вартість закупівлі апаратного забезпечення та допоміжних матеріалів, тис. грн;

$К_{навч}$ – витрати на навчання технічних фахівців і обслуговуючого персоналу, тис. грн;

$К_{н}$ – витрати на встановлення обладнання та налагодження системи інформаційної безпеки, тис. грн.

Вартість ліцензії на програмні SIEM-системи коливається від

1 тис. до 200 тис. дол. США в рік або за курсом НБУ станом на 13.11.20 (28 грн/ дол. США), від 28 тис. до 5,6 млн. грн. Додатково ці системи потребують від двох тижнів до кількох місяців на налаштування, що вимагає спеціальних навичок від адміністратора системи.

Розрахуємо найменші можливі капітальні витрати на впровадження інтелектуальної системи аналітики.

$К_{зпз}$ = 2,5 тис. дол. США = 70 000 (тис. грн.) (за курсом НБУ станом на 13.11.20 28 грн/ дол. США).

$К_{пз}$= 0, оскільки ПЗ супроводжується до його налагодження в системі.

Для функціонування системи аналітики необхідно придбати сервер, на якому буде відбуватися аналіз даних, що дозволить швидку обробку та збереження великих масивів даних. Даним вимогам відповідає сервер ARTLINE Business T25 v07 (T25v07), ціна якого 24 350 грн. Доставка коштує 60 грн.

$К_{аз}$ =24 410 (грн.)

Управління системою потребує спеціальних навичок. Розробники програмних засобів захисту вимагають проходження курсів, без яких захищеність системи не визнається [21].

Дані курси проводять віддалено і коштують приблизно 300 дол. США або 8 400 грн. Для їх проходження спеціаліст має витрати 30-40 годин тобто $К_{навч} = В_{навч} + К_{г} \cdot З_{пра}$ [19], [20] де

де $К_{Г}$ – кількість годин навчання;

$З_{пра}$ = 300 грн/ год – середньогодинна заробітна платня аналітика системи за результатами вивчення ринку послуг систем аналітики.

Тоді $К_{навч}$ = 8 400 + 30·300 = 17 400 грн,

Умовний час встановлення агенту на ПК 0,5 год. Налаштування системи триває від двох тижнів до кількох місяців, що вимагає щоденної уваги спеціаліста. Тоді вартість налаштування [11]:

$$К_{н} = (n_K \cdot t_K + n_H \cdot t_H) \cdot З_{пра} = (35 \cdot 0{,}5 + 14 \cdot 1) \cdot 300 = 9\,450 \text{ (грн)},$$

де n_K – кількість ПК в ІТС;

t_K – час, що витрачається на встановлення агенту;

n_H – кількість днів, відведена на налаштування;

t_H – час, необхідний для налаштування в день;

$З_{пра}$ = 300 грн/ год – середньогодинна заробітна платня аналітика системи за результатами вивчення ринку послуг систем аналітики.

Таким чином, капітальні витрати відповідно до формули (3.11) складатимуть:

$$К = 43\ 000 + 70\ 000 + 24\ 410 + 17\ 400 + 9\ 450 = 164\ 260 \text{ (грн.)}$$

3.3 Розрахунок експлуатаційних витрат

До експлуатаційних витрат необхідно включити:

- вартість систематичного відновлення системи;
- витрати на керування системою.

Річні експлуатаційні витрати можна розрахувати за формулою (3.12):

$$С = С_в + С_к, \qquad (3.12)$$

де $С_в$ - вартість систематичного відновлення системи;

$С_к$ - витрати на керування системою.

До витрат на керування системою інформаційної безпеки входять:

- витрати на амортизацію;
- витрати на навчання користувачів системи, технічного та адміністративного персоналу;
- витрати на заробітну платню персоналу;
- витрати на адміністрування системи та її підтримку.

Користуючись статистичними даними таблиці 3.1 [12], маємо відповідні показники експлуатаційних витрат підприємства, враховуючи величину розрахованих капітальних витрат.

Таблиця 3.1 - Вагові частки статей витрат у сукупній вартості

Фіксовані (капітальні) вкладення	*21%*
Поточні витрати, у т.ч.	*79%*
Керування системою	12%
Технічна підтримка й відновлення	21%
Активність користувача	46%

Капітальні витрати становлять 164 260 грн, що становить 21% витрат у сукупній вартості, тоді:

$$C = \frac{164\,260 \cdot 79}{21} = 617\,931 \text{ (грн)}$$

3.4 Оцінка можливого збитку від реалізації атаки на ІТС

Для розрахунку вартості збитку, що понесе типова компанія, при реалізації атаки будь-якого масштабу (забезпечується стан кіберстійкості – відповіді та відновлення від інциденту будь-якого ступеня серйозності – від порушення конфіденційності/ витоку даних до шифрування даних програмами-вимагачами/ реалізації атак «відказ в обслуговуванні»), необхідно враховувати наступні дані:

- $t_п$ – час простою вузла корпоративної мережі, у годинах;
- $t_в$ – час, необхідний для відновлення системи, у годинах;
- $t_{ві}$ – час відновлення інформації, у годинах;
- $З_0$ – заробітна платня обслуговуючого персоналу;
- $З_с$ – заробітна платня співробітників атакованого вузла;
- $Ч_0$ – чисельність обслуговуючого персоналу;
- $Ч_с$ – чисельність співробітників атакованого вузла;
- О – обсяг продажів атакованого вузла, у грн.;
- П – вартість доопрацювання, модифікації програмного забезпечення чи апаратного устаткування;
- І – число атакованих вузлів;

- N – середнє число атак на рік.

Втрати від простою атакованого вузла можна визначити за формулою (3.13):

$$U = \text{Пп} + \text{Пв} + V, \quad (3.13)$$

де $П_п$ – оплачувані втрати робочого часу при простоях системи, у грн.;

$П_в$ – вартість відновлення системи (переустановлення, зміна налаштувань), у грн.;

V – втрати від зниження обсягу продажів за час простою системи, у грн.

Для розрахунку витрат на оплату робочого часу при простоях системи використовується формула (3.14):

$$\text{Пп} = \frac{\sum \text{Зс}}{F} \times t\text{п}, \quad (3.14)$$

де F – місячний фонд робочого часу, що становить 176 год.

При кількості працівників атакованого вузла, що становить 5 осіб, та середній заробітній платні у 25 000 грн, маємо число витрат на оплату робочого часу при простоях системи складатимуть:

$$\text{Пп} = \frac{125\,000 \times 7}{176} = 4\,971 \text{ (грн)}.$$

Для розрахунку вартості відновлення системи використовується формула (3.15):

$$\text{Пв} = \text{Пви} + \text{Ппв} + \text{Пзч}, \quad (3.15)$$

де $П_{ВИ}$ – витрати на повторне уведення інформації у систему, у грн.;

$П_{ПВ}$ – витрати на відновлення вузла системи, у грн.;

$П_{зч}$ – вартість доопрацювання устаткування або зміни частини системи.

Витрати на повторне уведення інформації у систему розраховуються за формулою (3.16):

$$\text{Пви} = \frac{\sum \text{Зс}}{F} \times t\text{ви}, \qquad (3.16)$$

Таким чином, маємо наступний показник витрат на відновлення інформації у системі:

$$\text{Пви} = \frac{125\,000 \times 10}{176} = 7\,102 \text{ (грн)}.$$

Витрати на відновлення вузла системи визначаються за формулою (3.17):

$$\text{Ппв} = \frac{\sum \text{Зо}}{F} \times t\text{в}, \qquad (3.17)$$

$$\text{Ппв} = \frac{125\,000 \times 8}{176} = 5\,682 \text{ (грн)}.$$

Вартість відновлення системи становить:

$$П_в = 7\,102 + 5\,682 + 10\,000 = 22\,784 \text{ (грн.)}.$$

Для розрахунку втрат від зниження обсягу продажів під час простою використовується формула (3.18):

$$V = \frac{\text{О}}{F\text{г}} \times (t\text{п} + t\text{в} + t\text{ви}), \qquad (3.18)$$

Де $F_г$ - річний фонд робочого часу роботи організації, $F_г = 2080$ год.

$$V = \frac{500\,000}{2080} \times (7 + 8 + 10) = 6\,010 \text{ (грн)}$$

Число упущеної вигоди внаслідок здійснення атаки становить:

$$U = 4\,971 + 22\,784 + 6\,010 = 33\,765 \text{ (грн)}.$$

Показник загального збитку від реалізації атаки становить (3.19):

$$B = \sum_I \sum_N U \qquad (3.19)$$

$$B = 15 \times 15 \times 33\,765 = 7\,597\,125 \text{ (грн)}.$$

Загальний ефект від впровадження системи виявлення атак розраховується за формулою (3.20):

$$E = B \times R - C, \qquad (3.20)$$

де R – очікувана ймовірність атаки на вузол, у частках одиниці;

C – щорічні експлуатаційні витрати.

$$\text{E} = 7\,597\,125 \times 0{,}5 - 617\,931 = 3\,180\,631{,}5 \text{ (грн)}.$$

3.5 Аналіз показників економічної ефективності системи виявлення атак

Для визначення показнику економічної ефективності реалізованої системи аналітики необхідно спиратися на наступні параметри:

- TCO - сукупна вартість володіння;
- ROSI - коефіцієнт повернення інвестицій;

Коефіцієнт повернення інвестицій визначається за наступною формулою:

$$ROSI = \frac{E}{K}, \quad \text{частки одиниці} \qquad (3.21)$$

де E – загальний ефект від впровадження системи виявлення атак;

K – розмір капітальних інвестицій.

$$ROSI = \frac{3\,180\,631{,}5}{164\,260} = 19{,}4 \text{ частка одиниць}$$

Економічно проект можна визначити як ефективний, а його впровадження є доцільним, якщо виконується наступна умова (3.22):

$$ROSI > \frac{Nдеп - Nінф}{100}, \qquad (3.22)$$

де $N_{деп}$ – річна депозитна ставка або прибутковість альтернативного варіанту вкладення коштів, у %;

$N_{інф}$ – річний рівень інфляції, у %.

Приймаючи значення рівня інфляції поточного року рівним 5% та середнє значення депозитної ставки рівною 12%, маємо відповідний результат нерівності:

$$ROSI = 0{,}194; \quad ROSI > 0{,}07$$

Термін окупності капітальних інвестицій T_0 розраховується за формулою (3.23):

$$To = \frac{1}{ROSI}, \quad років \qquad (3.23)$$

Таким чином, термін окупності капітальних інвестицій T_0 складає = 5 років.

Висновки до розділу 3

Кібербезпека передбачає безліч різних технічних та інформаційних рішень, необхідних для захисту та стійкості, яких неможливо досягти в повному обсязі без правильного підходу. Як зазначається, кіберстійкість спрямована на динамічний захист організації з метою своєчасних відповідей на інциденти та підтримки кібер-рівноваги, що забезпечується управлінням ризиками.

Управління ризиками підприємства будь-якого масштабу потребує централізованої системи, що зможе забезпечити видимість факторів впливу та можливих загроз на усіх рівнях структури функціонування підприємства. У даному розділі було розраховано економічну ефективність впровадження інтелектуальної системи аналітики з метою забезпечення кіберстійкості підприємства.

Було розраховано коефіцієнт повернення інвестицій $ROSI = 0{,}194$, який, задовольняє умові економічно ефективного проекту:

$$ROSI > \frac{N\text{деп} - N\text{інф}}{100}$$

$$ROSI > 0{,}07$$

Також, визначений термін окупності капітальних інвестицій T_0 склав 5 років, беручи до уваги, що система є рішенням на необмежено довгий проміжок часу, впровадження інтелектуальної системи аналітики у ІТС підприємства, є доцільним та необхідним.

Розрахунки необхідних витрат на початкову реалізацію та підтримку системи, а також показники окупності системи, при використанні у довгостроковій перспективі, задовольняють вимогам та підкреслюють важливість запобігання ризиків, пов'язаних із функціонуванням інформаційних систем типового підприємства.

ВИСНОВКИ

Теоретичне значення отриманих результатів - визначено основні вимоги до інтелектуальних систем аналітики для забезпечення кіберстійкості та розроблено алгоритм вибору функціональної SIEM.

За результатами аналізу було встановлено, що впровадження системи дозволить замовнику вирішити наступні задачі:

- управління доступом;
- виявлення спроб несанкціонованого доступу та використання;
- реагування на несанкціонований доступ;
- забезпечення збільшення часу безвідмовної роботи систем;
- мінімізація часу відновлення систем;
- зменшення вразливостей та вживання заходів для мінімізації ризиків;
- контроль та керування процесом управління кіберризиками.

В ході виконання роботи було отримано наступні теоретичні та практичні результати:

- проаналізовано статистичні тенденції потенційних загроз інформаційній безпеці;
- розглянуто аспекти стратегії управління ризикам, пов'язаними із забезпеченням кіберстійкості;
- проаналізовано підходи до реалізації інтелектуальних систем аналітики та типові рішення з аутсорсингу послуг з кібербезпеки;
- проведено порівняння характеристик відомих рішень SIEM, аналіз їх функцій та сформовано критерії для вибору інтелектуальної системи аналітики для гарантування кіберстійкості;
- сформульовано алгоритм вибору функціональної SIEM;

- розглянуто процес вибору SIEM на підприємстві та запропоновано рекомендації для впровадження системи;
- показано можливість використання запропонованого підходу для управління ризиками за збалансованих витрат та комплексного багатофункціонального рішення SIEM;
- розраховано потенційні втрати від реалізації можливих атак та вартість впровадження інтелектуальної системи аналітики на основі обраного методу.

ПЕРЕЛІК ПОСИЛАНЬ

1. Базельський комітет з банківського нагляду. Кіберстійкість: спектр практик - https://www.bis.org/bcbs/publ/d454.pdf - Загол. з екрану.
2. Відкритий факторний аналіз інформаційного ризику. Стандарт відкритого групового аналізу ризиків - https://www2.opengroup.org/ogsys/catalog/C13G - Загол. з екрану.
3. Відкритий факторний аналіз інформаційного ризику. Таксономія відкритих груп ризиків - https://www2.opengroup.org/ogsys/catalog/C13K - Загол. з екрану.
4. ДСТУ ISO/IEC 27005:2015 Методи захисту. Управління ризиками інформаційної безпеки.
5. Європейський інститут програмного забезпечення. Модель управління стійкістю. Кібербезпека та стійкість бізнесу - https://esicenter.bg/sites/default/files/2019-05/2019-02%20ESICEE-RMM%20Overview%20%20v%202%202%20FMI%20-%20DIGEST.pdf - Загол. з екрану.
6. Звіт з кіберзагроз Sonicwall 2020 - https://www.sonicwall.com/resources/2020-cyber-threat-report-pdf/ - Загол. з екрану.

7. Звіт про безпеку програмного забезпечення Check Point 2020 - https://www.ntsc.org/assets/pdfs/cyber-security-report-2020.pdf - Загол. з екрану.
8. Звіт про безпеку Fireeye Mandiant 2020 - https://content.fireeye.com/m-trends/rpt-m-trends-2020 - Загол. з екрану.
9. Індекс розвідки загрози X-Force, вироблений IBM X-Force Incident Response and Intelligence Services (IRIS) 2020 - https://www.kommersant.ru/docs/2018/IBMXForceThreatIntelIndex2020.pdf - Загол. з екрану.
10. Комітет спонсорських організацій (COSO) Комісії Тредвей (2017) Внутрішній контроль - інтегрована структура - https://www.coso.org/Documents/990025P-Executive-Summary-final-may20.pdf - Загол. з екрану.
11. Лекції.Орг - інформаційний ресурс для студентів і школярів, , офіційний сайт - https://lektsii.org/15-1904.html- Загол. з екрану.
12. Методичні вказівки до виконання економічної частини дипломного проекту зі спеціальності 125 Кібербезпека / Упорядники: І.В. Шереметьєва, Д.П. Пілова, Н.М. Романюк. – Дніпро: Національний технічний університет «Дніпровська політехніка», 2017. – 17с.
13. Міжнародна електротехнічна комісія (IEC) (2019) Управління ризиками - Методи оцінки ризиків. IEC 31010: 2019 - https://www.iso.org/standard/72140.html - Загол. з екрану.
14. Міністерство фінансів України, офіційний сайт - http://index.minfin.com.ua/index/infl/ - Загол. з екрану.
15. Посібник оцінювача до NextGen SIEM SANS Institute - https://www.sans.org/media/vendor/evaluator-039-s-guide-nextgen-siem-38720.pdf - Загол. з екрану.
16. Постанова КМУ Про затвердження Методики розрахунку орієнтовної середньої вартості підготовки одного кваліфікованого робітника, фахівця, аспіранта, докторанта від 20 травня 2013 р. № 346 -

https://zakon.rada.gov.ua/laws/show/346-2013-%D0%BF#Text - Загол. з екрану.

17. Природа ефективної оборони: Перехід від кібербезпеки до кіберстійкості - - https://www.accenture.com/_acnmedia/Accenture/Conversion-Assets/DotCom/Documents/Local/en/Accenture-Shifting-from-Cybersecurity-to-Cyber-Resilience-POV.pdf - Загол. з екрану.
18. Публікація NIST Framework з кібербезпеки
19. Розрахунок витрат з навчання персоналу. Сучасний менеджмент, офіційний сайт - http://www.fellowmanage.ru/xins-77-1.html - Загол. з екрану.
20. Савченко В.А. Управління розвитком персоналу, К.: КНЕУ, 2002. -351 с. Навчальний посібник - https://library.if.ua/book/104/7044.html - Загол. з екрану.
21. Сертифікація спеціалістів з управління: офіційний сайт компанії «CISCO» – http://www.cisco.com/c/en/us/training-events/training-certifications/certifications/ specialist/security/ - Загол. з екрану.
22. Спеціальна публікація NIST 800-34 Rev. 1 Посібник з планування на випадок надзвичайних ситуацій для Федеральних інформаційних систем.
23. Стандарти та гайди з кіберстійкості Initio - https://www.initio.eu/blog/2019/3/7/cyber-resilience-standards-and-guidelines - Загол. з екрану.
24. Стандарт ISO 22301: 2019 Безпека та кіберстійкість - Системи управління безперервністю бізнесу – Вимоги.
25. Таксономія ризиків The Open Group - https://publications.opengroup.org/c13k - Загол. з екрану.
26. Хмарні служби безпеки. Основні види та напрямки розвитку -
    a. https://dsimg.ubm-us.net//MDRoverMSSPSIEM_2017.pdf - Загол. з екрану.

27. Центр знань IBM. Огляд архітектури QRadar- https://www.ibm.com/support/knowledgecenter/SS42VS_7.4/com.ibm.qradar.doc/c_qradar_deployment_guide_arch.html - Загол. з екрану.
28. Центр знань IBM. Огляд розгортання QRadar - https://www.ibm.com/support/knowledgecenter/SS42VS_7.3.2/com.ibm.qradar.doc/c_qradar_deployment_guide_overview.html - Загол. з екрану.
29. AT&T Cybersecurity AlienVault Unified Security Management, офіційний сайт - https://cybersecurity.att.com/who-we-are/press-releases/alienvault-unified-security-management-platform-for-government-receives-niap-certification - Загол. з екрану.
30. COSO - Комітет спонсорських організацій Комісії Тредвей - [https://www.coso.org/ - Загол. з екрану.
31. ENISA Ландшафт загроз 2020 - https://www.enisa.europa.eu/topics/threat-risk-management/threats-and-trends?fbclid=IwAR26a-lQRJaK3Xk-dTZ0qWIFXW-Lxaljh6wkYeIy1rQ32momjFJOZPL2yoI - Загол. з екрану.
32. IBM QRadar, офіційний сайт - https://www.ibm.com/security/security-intelligence/qradar - Загол. з екрану.
33. IBM Resilient SOAR, офіційний сайт - https://www.ibm.com/products/resilient-soar-platform - Загол. з екрану.
34. Leadmark. Практичний посібник з управління ризиками аутсорсингу - https://www.leadmark.nl/wp-content/uploads/2017/04/Guidance-on-Managing-Outsourcing-Risk.pdf - Загол. з екрану.
35. LogRhythm NextGen SIEM Platform, офіційний сайт - https://logrhythm.com/products/nextgen-siem-platform/ - Загол. з екрану.
36. ManageEngine EventLog Analyzer, офіційний сайт - https://www.manageengine.com/products/eventlog/ - Загол. з екрану.
37. McAfee Звіт про загрози COVID-19 - https://www.mcafee.com/enterprise/en-us/assets/reports/rp-quarterly-threats-july-2020.pdf - Загол. з екрану.
38. McAfee Enterprise Security Manager, офіційний сайт - https://docs.mcafee.com/bundle/enterprise-security-manager-10.2.0-product-

guide-unmanaged/page/GUID-88473528-B9BD-4799-B3A7-BC7A8C22B55D.html - Загол. з екрану.

39. NISTIR 8286. Інтеграція кібербезпеки та управління ризиками підприємств - https://nvlpubs.nist.gov/nistpubs/ir/2020/NIST.IR.8286.pdf - Загол. з екрану.
40. OSSEC, офіційний сайт -https://www.ossec.net/ossec-2-8-released/ - Загол. з екрану.
41. RSA NetWitness, офіційний сайт - https://community.rsa.com/community/products/netwitness/1065- Загол. з екрану.
42. SolarWinds Security Event Manager, офіційний сайт - https://www.solarwinds.com/security-event-manager - Загол. з екрану.
43. Splunk Enterprise Security, офіційний сайт - https://splunkbase.splunk.com/app/263/ - Загол. з екрану.
44. The MITRE Corporation (2019) ATT&CK - https://attack.mitre.org - Загол. з екрану.

ДОДАТОК А. Відомість матеріалів дипломної роботи

№	Формат	Найменування	Кількість листів	Примітки
Документація				
1	А4	Реферат	2	
2	А4	Список умовних скорочень	3	
3	А4	Зміст	2	
4	А4	Вступ	2	
5	А4	Процес управління ризиками кібербезпеки з використанням інтелектуальних систем аналітики	38	
6	А4	Мінімізація ризиків, пов’язаних із забезпеченням кіберстійкості	36	
7	А4	Економічний розділ	16	
8	А4	Висновки	2	
9	А4	Перелік посилань	5	
10	А4	Додаток А	1	
11	А4	Додаток Б	1	
12	А4	Додаток В	1	
13	А4	Додаток Г	1	

ДОДАТОК Б. Перелік матеріалів на оптичному носії

1 Пояснювальна_записка.docx

2 Презентація.pptx

ДОДАТОК В. Відгук керівника економічного розділу

Керівник розділу _____

(підпис) (ініціали, прізвище)

ДОДАТОК Г. Відгук керівника кваліфікаційної роботи

В І Д Г У К
на кваліфікаційну роботу студентки групи 125м-19-1
Гулої Жанни Володимирівни
на тему: «Ризико-орієнтований підхід до забезпечення кіберстійкості з використанням інтелектуальних систем аналітики»

Пояснювальна записка ст. Гулої Жанни Володимирівни складається зі вступу, трьох розділів і висновків, викладених на 108 сторінках. Кваліфікаційна робота присвячена актуальній темі забезпечення кіберстійкості як можливості мінімізації ризиків підприємства з використанням інтелектуальних систем аналітики.

Тема кваліфікаційної роботи безпосередньо пов'язана з об'єктом діяльності магістра спеціальності 125 «Кібербезпека». Для досягнення мети у дипломній роботі вирішуються наступні задачі: аналіз підходів до реалізації інтелектуальних систем аналітики; дослідження процесу впровадження SIEM на підприємстві та процесу функціонування системи; аналіз отриманих результатів порівняння відомих рішень SIEM. Ст. Гула Ж.В. виявила основні переваги аутсорсингу послуг з кібербезпеки, проаналізувала можливі аутсорсингові рішення та порівняла відомі рішення SIEM систем за визначеними критеріями забезпечення кіберстійкості.

Практичне значення роботи полягає у визначені основних вимог до інтелектуальних систем аналітики задля забезпечення кіберстійкості та розробці алгоритму вибору функціональної SIEM. Автором також було запропоновано критерії угоди про рівень обслуговування, що застосовується при аутсорсингу.

Кваліфікаційна робота ст. Гулої Ж.В. виконана відповідно до вимог до дипломних робіт, зроблена на належному рівні і може бути допущена до захисту, заслуговує оцінку – «відмінно».

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

Керівник кваліфікаційної роботи

Керівник спец. розділу