МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
ДЕРЖАВНИЙ УНІВЕРСИТЕТ
ІНФОРМАЦІЙНО-КОМУНІКАЦІЙНИХ ТЕХНОЛОГІЙ
НАВЧАЛЬНО-НАУКОВИЙ ІНСТИТУТ ЗАХИСТУ ІНФОРМАЦІЇ
КАФЕДРА УПРАВЛІННЯ ІНФОРМАЦІЙНОЮ ТА КІБЕРНЕТИЧНОЮ БЕЗПЕКОЮ

КВАЛІФІКАЦІЙНА РОБОТА

на тему: «КІБЕРБЕЗПЕКА ТА КІБЕРСТІЙКІСТЬ БІЗНЕСУ: ПОРІВНЯЛЬНА ХАРАКТЕРИСТИКА ПІДХОДІВ ТА МЕТОДІВ»

на здобуття освітнього ступеня магістра
зі спеціальності 125 Кібербезпека
освітньо-професійної програми Управління інформаційною безпекою

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

Антон ГУНДЕР
(підпис) *Ім'я, ПРІЗВИЩЕ здобувача*

Виконав: Здобувач вищої освіти гр. УБДМ 61
Антон ГУНДЕР

Керівник:
к. держ. упр., доц. Тетяна МУЖАНОВА

Рецензент:
_____

Київ 2024

ДЕРЖАВНИЙ УНІВЕРСИТЕТ
ІНФОРМАЦІЙНО-КОМУНІКАЦІЙНИХ ТЕХНОЛОГІЙ

Навчально-науковий інститут захисту інформації

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

ЗАТВЕРДЖУЮ
Завідувач кафедри УІКБ
_____ Світлана ЛЕГОМІНОВА
"____" _____ 2024 р.

ЗАВДАННЯ
НА КВАЛІФІКАЦІЙНУ РОБОТУ

здобувачу Гундеру Антону Миколайовичу
(прізвище, ім'я, по батькові здобувача)

1. Тема кваліфікаційної роботи: "КІБЕРБЕЗПЕКА ТА КІБЕРСТІЙКІСТЬ БІЗНЕСУ: ПОРІВНЯЛЬНА ХАРАКТЕРИСТИКА ПІДХОДІВ ТА МЕТОДІВ"

керівник кваліфікаційної роботи Тетяна Мужанова, к.держ.упр., доцент
(Ім'я, ПРІЗВИЩЕ, науковий ступінь, вчене звання)
затверджені наказом Державного університету інформаційно-комунікаційних технологій від "19" жовтня 2023 р. №145

2. Строк подання кваліфікаційної роботи "18" грудня 2023 р
3. Вихідні дані до кваліфікаційної роботи: кібербезпека, кіберстійкість .
4. Перелік питань, які потрібно розробити:
   1. Встановити сутність і відмінності концепцій кібербезпеки та кіберстійкості.
   2. Дослідити методи й підходи до забезпечення кібербезпеки підприємства.
   3. З'ясувати засади розробки, впровадження й оцінювання ефективності стратегії кіберстійкості бізнесу.
5. Перелік ілюстративного матеріалу: *презентація*
6. Дата видачі завдання "02" жовтня 2023 р.

:

КАЛЕНДАРНИЙ ПЛАН

№ з/п	Назва етапів кваліфікаційної роботи	Строк виконання етапів роботи	Примітка
1.	Визначення об’єкту, предмету, мети та завдань дослідження.	10.10.2023	
2.	Збір та аналіз літератури.	23.10.2023	
3.	Вивчення сутності й відмінностей концепцій кібербезпеки та кіберстійкості.	27.10.2023	
4.	Дослідження методів і підходів до забезпечення кібербезпеки підприємства.	10.11.2023	
5.	З’ясування засад розробки, впровадження й оцінювання ефективності стратегії кіберстійкості бізнесу.	15.11.2023	
6.	Формулювання висновків на основі отриманих результатів дослідження.	22.11.2023	
7.	Оформлення роботи.	04.12.2023	
8.	Оформлення презентації.	14.12.2023	
9.	Отримання рецензії на роботу.	18.12.2023	
10.	Захист в ДЕК.	.01.2024	

Здобувач вищої освіти _____ Антон ГУНДЕР
(підпис) *(Ім’я, ПРІЗВИЩЕ)*

Керівник
кваліфікаційної роботи _____ Тетяна МУЖАНОВА
(підпис) *(Ім’я, ПРІЗВИЩЕ)*

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

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

Направляється здобувач Гундер А.М. до захисту кваліфікаційної роботи
(прізвище та ініціали)
за спеціальністю 125 Кібербезпека
(код, найменування спеціальності)
Освітньо-професійної програми Управління інформаційною безпекою
(назва)
на тему: "КІБЕРБЕЗПЕКА ТА КІБЕРСТІЙКІСТЬ БІЗНЕСУ: ПОРІВНЯЛЬНА ХАРАКТЕРИСТИКА ПІДХОДІВ ТА МЕТОДІВ"
Кваліфікаційна робота і рецензія додаються.

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

Висновок керівника кваліфікаційної роботи

Здобувач **ГУНДЕР Антон** у кваліфікаційній роботі відповідно до обраної теми встановив сутність і відмінності концепцій кібербезпеки та кіберстійкості; дослідив методи й підходи до забезпечення кібербезпеки підприємства; з'ясував засади розробки, впровадження й оцінювання ефективності стратегії кіберстійкості бізнесу.

ГУНДЕР Антон показав розуміння проблеми дослідження та бачення основних теоретичних та практичних напрямів її вирішення, довів володіння методами наукового дослідження, проявив себе як організований, відповідальний виконавець.

Результати дослідження апробовані на міській науково-практичній конференції "Кременчуцький Форум Кібербезпеки 2023: Ініціативи та Розвиток", що доводить практичну значимість отриманих результатів.

Вищевикладене дозволяє оцінити кваліфікаційну роботу здобувача **ГУНДЕРА Антона** на позитивну оцінку та присвоїти йому кваліфікацію "Магістр з кібербезпеки" за освітньо-професійною програмою "Управління інформаційною безпекою".

Керівник кваліфікаційної роботи _____ Тетяна Мужанова
(підпис) *(Ім'я, ПРІЗВИЩЕ)*

"___" _____ 2024 року

Висновок кафедри про кваліфікаційну роботу

Кваліфікаційна робота розглянута. Гундер А.М. допускається до захисту даної роботи в Державній екзаменаційній комісії.

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

ВІДГУК РЕЦЕНЗЕНТА
на кваліфікаційну магістерську роботу

Здобувача вищої освіти Гундера Антона Миколайовича
На тему: КІБЕРБЕЗПЕКА ТА КІБЕРСТІЙКІСТЬ БІЗНЕСУ: ПОРІВНЯЛЬНА ХАРАКТЕРИСТИКА ПІДХОДІВ ТА МЕТОДІВ

Актуальність: У сучасному світі, де більшість бізнес-процесів та особистих взаємодій відбувається в цифровому просторі, питання кібербезпеки й кіберстійкості набувають ключового значення.

Причинами такого стану речей є, перш за все, пріоритетність завдання захисту цифрових даних внаслідок їх важливості для повсякденного ведення бізнесу; збільшення кількості і складності кіберзагроз; постійне вдосконалення методів зловмисного впливу, які використовують кіберзлочинці, а також необхідність адаптації стратегій захисту до постійного розвитку інформаційно-комунікаційних технологій.

З огляду на це дослідження підходів і методів забезпечення кібербезпеки та кіберстійкості бізнесу є актуальним науковим завданням.

Позитивні сторони. У кваліфікаційній роботі встановлено сутність та відмінності концепцій кібербезпеки та кіберстійкості; досліджено методи та підходи до забезпечення кібербезпеки підприємства; з'ясовано засади розробки, впровадження й оцінювання ефективності стратегії кіберстійкості бізнесу.

Робота оформлена відповідно до вимог, а її структура забезпечує досягнення поставленої мети. Основні положення проілюстровані рисунками. Кваліфікаційна робота підтвердила володіння здобувачем методами наукового дослідження та грунтовне розуміння сутності й відмінностей сучасних концепцій кібербезпеки та кіберстійкості, а також підходів до їх забезпечення.

Недоліки

1. Доцільно було б ширше розглянути розвиток ландшафту кіберзагроз як чинника виникнення концепції кіберстійкості.

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

Висновок: Кваліфікаційна робота виконана на достатньому науково-методичному рівні, заслуговує позитивної оцінки і рекомендується до захисту, а здобувач Гундер Антон Миколайович заслуговує присвоєння кваліфікації "Магістр кібербезпеки за освітньо-професійною програмою "Управління інформаційною безпекою".

Рецензент:

_____ _____
підпис

РЕФЕРАТ

Текстова частина кваліфікаційної роботи на здобуття освітнього ступеня магістра: 83 стор., 14 рис., 61 джерело.

Метою роботи є порівняння підходів і методів забезпечення кібербезпеки та кіберстійкості бізнесу.

Об'єктом дослідження є концепції забезпечення кібербезпеки та кіберстійкості бізнесу.

Предметом дослідження – сукупність підходів і методів забезпечення кібербезпеки та кіберстійкості бізнесу.

Методи дослідження. Для вирішення завдань дослідження використовувалися методи аналізу та синтезу, уточнення понять, узагальнення й порівняння, класифікації. Важливим є також використання статистичних даних, що дозволяє оцінювати ефективність різних підходів на практиці.

Короткий зміст роботи. У роботі встановлено сутність та відмінності концепцій кібербезпеки та кіберстійкості; досліджено методи й підходи до забезпечення кібербезпеки підприємства; з'ясовано засади розробки, впровадження й оцінювання ефективності стратегії кіберстійкості бізнесу.

Галузь застосування. Результати дослідження можуть бути використані у ході розробки і впровадження стратегій кібербезпеки та кіберстійкості на підприємствах різних галузях з метою зміцнення корпоративної кібербезпеки, поліпшення реакції на інциденти та створення більш стійкої цифрової інфраструктури.

КЛЮЧОВІ СЛОВА: КІБЕРБЕЗПЕКА, КІБЕРСТІЙКІСТЬ, МЕТОДИ ТА ПІДХОДИ ДО ЗАБЕЗПЕЧЕННЯ КІБЕРБЕЗПЕКИ, СТРАТЕГІЇ КІБЕРСТІЙКОСТІ БІЗНЕСУ.

ABSTRACT

The text part of the qualification work for obtaining the master's degree: 83 pages, 14 figures, 61 sources.

Purpose of research is to compare approaches and methods of ensuring cyber security and cyber resilience of business.

Object of research is the concepts of ensuring cyber security and cyber resilience of business.

Subject of research is a set of approaches and methods for ensuring cyber security and cyber resilience of business.

Research methods. Methods of analysis and synthesis, clarification of concepts, generalization and comparison, and classification were used to solve research problems. It is also important to use statistical data, which allows you to evaluate the effectiveness of different approaches in practice.

Brief content of research. The work establishes the essence and differences of the concepts of cyber security and cyber resilience; methods and approaches to ensuring the cyber security of the enterprise were investigated; the principles of development, implementation and evaluation of the effectiveness of the business cyber resilience strategy are clarified.

Field of research. The results of the study can be used in the development and implementation of cyber security and cyber resilience strategies at enterprises in various industries in order to strengthen corporate cyber security, improve response to incidents and create a more sustainable digital infrastructure.

KEY WORDS: CYBER SECURITY, CYBER RESILIENCE, METHODS AND APPROACHES TO PROVIDING CYBER SECURITY, BUSINESS CYBER RESILIENCE STRATEGIES.

ЗМІСТ

ПЕРЕЛІК УМОВНИХ ПОЗНАЧЕНЬ І СКОРОЧЕНЬ 8
ВСТУП 9
РОЗДІЛ 1 СУТНІСТЬ І ВІДМІННОСТІ КОНЦЕПЦІЙ КІБЕРБЕЗПЕКИ ТА КІБЕРСТІЙКОСТІ 11
1.1 Поняття та ключові риси кібербезпеки та кіберстійкості 11
1.2 Загрози та виклики в кіберпросторі 17
1.3 Огляд основних теоретичних моделей кібербезпеки 20
Висновки до розділу 1 28
РОЗДІЛ 2 МЕТОДИ Й ПІДХОДИ ДО ЗАБЕЗПЕЧЕННЯ КІБЕРБЕЗПЕКИ ПІДПРИЄМСТВА 30
2.1 Превентивні методи кібербезпеки 30
2.2 Детективні методи кібербезпеки 40
2.3 Реагування та відновлення після інцидентів 45
Висновки до розділу 2 53
РОЗДІЛ 3 СТРАТЕГІЇ КІБЕРСТІЙКОСТІ БІЗНЕСУ: ЗАСАДИ РОЗРОБКИ, ВПРОВАДЖЕННЯ Й ОЦІНЮВАННЯ ЕФЕКТИВНОСТІ 55
3.1 Розробка та імплементація стратегій кіберстійкості 55
3.2 Оцінка ефективності стратегій кіберстійкості 63
3.3 Роль нормативно-правової бази у забезпеченні кіберстійкості на прикладі CRA 69
Висновки до розділу 3 73
ВИСНОВКИ 75
ПЕРЕЛІК ПОСИЛАНЬ 77

ПЕРЕЛІК УМОВНИХ ПОЗНАЧЕНЬ І СКОРОЧЕНЬ

CRA	Cyber Resilience Act
GDPR	General Data Protection Regulation
IDS	Intrusion Detection System
IPS	Intrusion Prevention System
ISO	International Organization for Standardization
NIST	National Institute of Standards and Technology
SIEM	Security Information and Event Management
SOAR	Security Orchestration, Automation and Response

ВСТУП

Актуальність теми. У сучасному світі, де більшість бізнес-процесів та особистих взаємодій відбувається в цифровому просторі, питання кібербезпеки й кіберстійкості набувають ключового значення. Зростання ролі захисту кіберсередовища викликане низкою факторів. Перш за все, зростання обсягу цифрових даних та їх важливість для повсякденного ведення бізнесу робить захист цих даних пріоритетним завданням. Поряд з цим, збільшується кількість і складність кіберзагроз: від простих вірусів до складних нападів на інфраструктуру, а кіберзлочинці постійно вдосконалюють методи зловмисного впливу. Нагальність теми підсилюється постійним розвитком інформаційно-комунікаційних технологій, що вимагає адаптації стратегій захисту.

З огляду на це дослідження підходів і методів забезпечення кібербезпеки та кіберстійкості бізнесу є актуальним науковим завданням.

Метою роботи є вивчення й порівняння підходів і методів забезпечення кібербезпеки та кіберстійкості бізнесу.

Об'єктом дослідження є концепції забезпечення кібербезпеки та кіберстійкості бізнесу.

Предмет дослідження - сукупність підходів і методів забезпечення кібербезпеки та кіберстійкості бізнесу.

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

1. Встановити сутність і відмінності концепцій кібербезпеки та кіберстійкості.
2. Дослідити методи й підходи до забезпечення кібербезпеки підприємства.
3. З'ясувати засади розробки, впровадження й оцінювання ефективності стратегії кіберстійкості бізнесу.

Методи дослідження. Для вирішення завдань дослідження використовувалися методи аналізу та синтезу, уточнення понять, узагальнення й порівняння, класифікації. Важливим є також використання статистичних даних,

що дозволяє оцінювати ефективність різних підходів на практиці.

Наукова новизна одержаних результатів. У роботі проведене порівняння концепцій кібербезпеки й кіберстійкості, а також підходів і методів їх забезпечення, проаналізовано засади розробки, впровадження й оцінювання ефективності стратегій кіберстійкості бізнесу, в результаті впровадження яких буде забезпечено зміцнення корпоративної кібербезпеки, поліпшення реакції на інциденти та створення більш стійкої цифрової інфраструктури.

Практичне значення одержаних результатів. Результати дослідження будуть корисними для керівників компаній, фахівців з кіберзахисту, розробників політик і стандартів кібербезпеки, які зможуть використати отримані напрацювання для підвищення ефективності існуючих систем забезпечення кібербезпеки та розробки нових стратегій захисту цифрових активів.

Апробація результатів. Результати дослідження апробовані на Всеукраїнській науково-практичній конференції “Кременчуцький Форум Кібербезпеки 2023: Ініціативи та Розвиток ”.

РОЗДІЛ 1
СУТНІСТЬ І ВІДМІННОСТІ КОНЦЕПЦІЙ КІБЕРБЕЗПЕКИ ТА КІБЕРСТІЙКОСТІ

1.1 Поняття та ключові риси кібербезпеки та кіберстійкості

Кібербезпека та кіберстійкість є ключовими компонентами для забезпечення безпеки бізнесу. Вони допомагають захистити дані, системи та мережі від кібератак, а також забезпечити відновлення після кібератак.

Ранній етап розвитку кібербезпеки почався з моменту створення перших комп'ютерних мереж. Наприклад, у 1988 році черв'як Морріса, перший відомий черв'як, що розповсюджувався через Інтернет, заразив тисячі комп'ютерів, що призвело до значних фінансових втрат. Це стало поворотом в усвідомленні необхідності захисту комп'ютерних систем.

З розвитком Інтернету та електронної комерції кіберзагрози стали більш складними та різноманітними. З'явилися віруси, трояни, шпигунське програмне забезпечення, а згодом - DDoS-атаки та шкідливе ПЗ. Одним з відомих прикладів є атака "WannaCry" у 2017 році, яка заразила комп'ютери у більш ніж 150 країнах, використовуючи слабкості у Windows або ж дуже актуальним прикладом є атака на інфраструктуру Київстар у 2023, що стала однією з наймасштабніших у світі, де все ще невідомі деталі як саме реалізувалась така атака.

Кожній організації дуже важлива довіра клієнтів та партнерів, яка може дуже вмить знизитись, якщо важливі та конфіденційні дані, доручені їй або створені внутрішньо, стануть об'єктом злому та компрометації. Дедалі більша частина процесів підприємства, наприклад, внаслідок роботизації виробництва та розподілу, залежить від цифрових процесів. Захист від кіберзлочинності, цифрового вторгнення, шахрайства ззовні або зсередини є найважливішим фактором для стабільності та виживання бізнесу в епоху цифрової

трансформації. Побудова всебічної програми кіберстійкості є ключем до безпеки підприємства.

Кібербезпека - це практична діяльність, спрямована на захист комп'ютерних систем і мереж від кібератак. Вона включає в себе весь комплекс заходів - від керування паролями до інструментів комп'ютерної безпеки на основі технологій машинного навчання [1].

Кібербезпека насамперед зосереджена на запобіганні й захисті комп’ютерних систем, мереж і даних від цифрових атак, несанкціонованого доступу й інших загроз. Охоплює широкий спектр методів, технологій і процесів, призначених для захисту цілісності, конфіденційності та доступності даних.

Заходи кібербезпеки спрямовані на запобігання загрозам шляхом захисту систем від несанкціонованого доступу або атак включають розгортання брандмауерів, антивірусного програмного забезпечення, систем виявлення вторгнень (IDS) і систем запобігання вторгненням (IPS).

Значною частиною кібербезпеки є виявлення потенційних ризиків, оцінка їхньої ймовірності та впливу, а також вжиття заходів для їх пом’якшення. Оцінка ризиків і сканування вразливостей є звичайними методами кібербезпеки.

Кібербезпека передбачає дотримання політик, стандартів і правових вимог. Щоб захистити конфіденційну інформацію, організаціям часто потрібно дотримуватися таких нормативних актів, як GDPR, HIPAA або PCI-DSS.

Підходи до забезпечення кібербезпеки бізнесу значною мірою залежать від технологічних рішень. Вони зосереджені на впровадженні апаратних і програмних продуктів, які захищають від відомих вразливостей і загроз.

Хоча технології відіграють вирішальну роль, навчання користувачів і персоналу компанії безпечній поведінці в Інтернеті та “кібергігієні” також є фундаментальною частиною стратегії кібербезпеки.

Кібербезпека включає розробку плану реагування на інциденти, у якому описано, які кроки необхідно вжити у разі порушення цілісності, доступності або конфіденційності інформаційних активів [2].

Кібербезпека може бути розділена на п'ять основних типів:

1. Кібербезпека у сфері критичної інфраструктури: Цей тип кібербезпеки захищає від кіберзагроз основні системи, необхідні для підтримання життєдіяльності суспільства, наприклад, електромережі та лікарні.

2. Безпека мережі: Цей тип кібербезпеки включає усунення вразливостей, що впливають на операційні системи та мережеву архітектуру - сервери і хости, маршрутизатори і точки бездротового доступу, а також мережеві протоколи.

3. Хмарна безпека: Цей тип кібербезпеки пов'язаний із захистом даних, застосунків та інфраструктури у хмарі.

4. Безпека IoT: Цей тип кібербезпеки захищає інтелектуальні пристрої, підключені до IoT. Вони підключаються до мережі без додаткового втручання людини. Наприклад, це можуть бути інтелектуальні пожежні сигналізації, освітлення, термостати й інші пристрої.

5. Безпека програм: Цей тип кібербезпеки пов'язаний з усуненням вразливостей, що виникають внаслідок небезпечних процесів розробки під час проєктування, кодування та публікації ПЗ або веб-сайту [3].

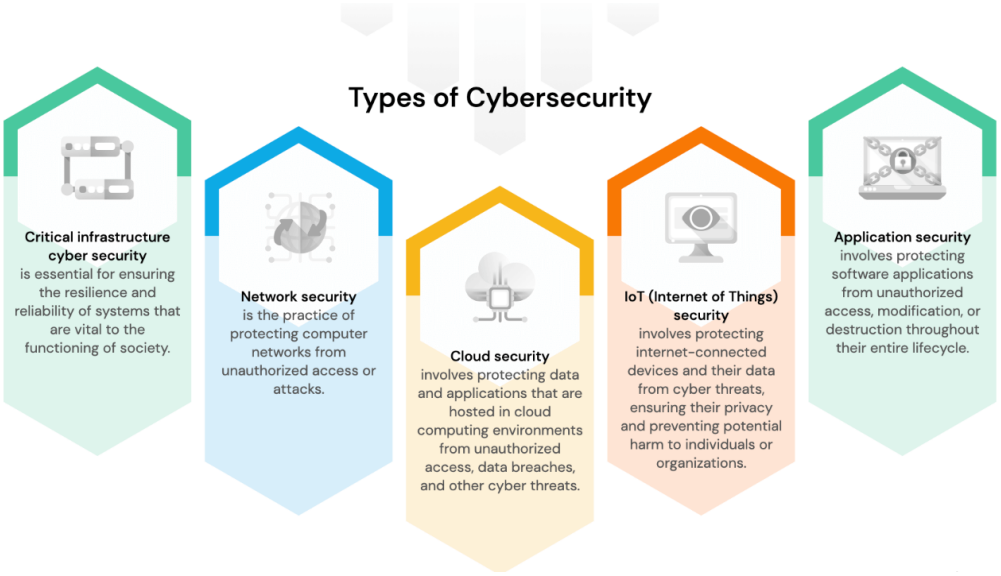

Рис. 1.1. Основні види кібербезпеки

Систему кібербезпеки можна розділити на підрозділи, де внутрішня координація кожного підрозділу має критично важливе значення для всієї системи кібербезпеки. Такі підрозділи забезпечують відновлення в аварійних ситуаціях і планування безперервності життєдіяльності бізнесу; покращення репутації компанії та підвищення рівня довіри з боку розробників, партнерів,

клієнтів, зацікавлених сторін та співробітників [4].

Кібербезпека важлива для забезпечення надійного захисту від атак, спрямованих на отримання доступу, зміну, видалення, знищення або вимагання конфіденційних даних компаній, організацій або окремих користувачів. Також кібербезпека здатна запобігати атакам, які спрямовані на відключення або порушення роботи систем та пристроїв [5].

Термін "кіберстійкість" є відносно свіжим, але стає все більш популярним і актуальним у галузі інформаційної та кібербезпеки. Він включає в себе ряд завдань і процесів, які відносяться до інформаційних технологій і захисту бренду. Кіберстійкість має ширший підхід, який охоплює здатність організації продовжувати ефективну роботу перед обличчям кіберзагроз і швидко відновлюватися після будь-яких збоїв або пошкоджень. Концепція кіберстійкості визнає, що, незважаючи на найкращі заходи безпеки, порушення можуть і будуть відбуватися.

Кіберстійкість дозволяє підготуватися до атаки, забезпечує ефективну діяльність і протидію під час атаки, а також знижує можливі наслідки атаки на компанію. Кіберстійкість полягає в забезпеченні того, що бізнес процеси можуть і мають продовжуватися під час і після кіберінциденту.

Поняття кіберстійкості передбачає адаптацію до нових загроз і мінливого середовища. Це означає не лише захист від відомих загроз, але й можливість реагувати на нові та непередбачені виклики.

Компанія, що заявляє про свою кіберстійкість, має надійні плани реагування на інциденти та відновлення після них. Це включає відновлення нормальної роботи систем і даних після атаки.

Організації розробляють і регулярно оновлюють план відмовостійкості, який включає стратегії зменшення впливу атак і забезпечення швидкого відновлення.

Елементи кіберстійкості в компанії розділяють на кілька основних категорій: управління, права доступу, сегментування, забезпечення цілісності та конфіденційності даних, активне реагування на інциденти, відновлення і

координація, скоординований захист компанії:

1. Управління кіберстійкістю повністю базується на процесі управління ризиками в компанії в прив’язці до загальної стратегії розвитку бізнесу. Ця категорія включає в себе управління кіберризиками, аудит кіберзахищеності компанії і розробку стратегії кібербезпеки в компанії.

2. Права доступу, або управління правами доступу для забезпечення кіберстійкості, здійснюється відповідно до принципу їх мінімізації. Це означає, що користувачам необхідно надавати мінімально можливий рівень доступу для виконання їх обов’язків і завдань.

3. Сегментування має на увазі не тільки вже звичний термін сегментування мережі, а й сегментування IT архітектури і кібербезпеки для забезпечення багаторівневого захисту даних та інформаційних систем.

4. Активне реагування на інциденти і кібератаки включає в себе впровадження автоматизованих засобів виявлення та реагування, а також розробку і впровадження процесів управління реагуванням на кібератаки в компанії.

5. Скоординований захист включає в себе елементи всіх категорій і об’єднує їх в єдину стратегію забезпечення кібербезпеки і стійкості. Ця категорія часто виділяють в окрему послугу – «захист бренду», що по суті своїй одне і те ж.

6. Забезпечення цілісності та конфіденційності має на меті зниження збитків для інформаційних систем і даних в разі інциденту або атаки

7. Моніторинг включає постійну оцінку всіх процесів і діяльності компанії з точки зору кібербезпеки і кіберстійкості.

8. Відновлення кіберстійкості базується на стандартних процесах відновлення після збоїв (DRP) і планування безперервності ведення бізнесу (BCP).

Кібербезпека та кіберстійкість повинні бути включені в стратегію бізнесу з самого початку і бути пріоритетними. Це включає в себе визначення ризиків, розробку та впровадження політик та процедур кібербезпеки, навчання персоналу, регулярне тестування та оновлення систем кібербезпеки

Кібербезпека та кіберстійкість — два терміни, які часто обговорюються в контексті захисту цифрових активів організації, але вони стосуються різних концепцій і підходів у сфері інформаційних технологій і безпеки.

Відмінності концепцій кібербезпеки та кіберстійкості показано на рис. 1.2.

Cyber Security	Cyber Resilience
Primarily focuses on prevention	Concentrates on adaptability and recovery
Utilises tools like firewalls, antivirus, and encryption	Uses strategies like incident response plans and backup systems
Aims to prevent breaches and unauthorised access	Aims to ensure continuity even after a breach
Addresses threats externally	Addresses threats both externally and internally, considering organisational resilience

Рис. 1.2. Різниця між кібербезпекою та кіберстійкістю

По суті, кібербезпека зосереджена на створенні бар'єрів, щоб не допустити зловмисників і захистити системи та дані від злому, використовує такі засоби як міжмережеві екрани, антивіруси, криптографію, спрямовує зусилля на запобігання порушенням безпеки і неавторизованому доступу, протидіє загрозам ззовні.

Натомість, кіберстійкість припускає, що системи можуть бути зламані, і підкреслює здатність працювати під час атаки та швидко відновлюватися після неї, концентрується на адаптивності і відновленні після порушень безпеки, використовує стратегії реагування на інциденти і системи резервного копіювання, спрямовує зусилля на забезпечення безперервності бізнесу навіть після інциденту, протидіє загрозам як зовнішньо, так і внутрішньо, забезпечуючи організаційну стійкість.

І кібербезпека, і кіберстійкість мають вирішальне значення для сучасних організацій. Ефективна стратегія поєднує потужні заходи кібербезпеки для

запобігання та виявлення атак із надійним плануванням кібервідмовостійкості, щоб гарантувати, що бізнес зможе протистояти інцидентам і швидко відновлюватися після них. Мета полягає не тільки в тому, щоб запобігти кожній можливій атаці, але й у тому, щоб організація могла вижити після атаки з недоторканими основними функціями.

1.2 Загрози та виклики в кіберпросторі

Вивчення кіберпростору як середовища, де розгортаються динамічні процеси взаємодії між бізнес-структурами та потенційними кіберзагрозами, відкриває перед нами картину складної багатовекторної взаємодії. Сьогоднішній цифровий ландшафт охоплює не лише традиційні комп'ютерні системи, але й розширену екосистему з мобільних пристроїв, інтернету речей, хмарних платформ, що створює нові можливості для зростання та інновацій у бізнесі.

Однак, з цими можливостями приходять і нові виклики, які потребують ретельного аналізу та розуміння. На перший погляд, важко осягнути всю глибину та широту потенційних загроз, що існують в кіберпросторі. Від простих шкідливих програм, що знищують дані кінцевого користувача, до складних цілеспрямованих атак на корпоративні мережі – цей спектр є дивовижно різноманітним. Розуміння цих загроз вимагає не тільки технічних знань, але й глибокого вникнення в специфіку бізнес-процесів, що є предметом захисту.

Кіберзлочинність, яка охоплює діяльність від окремих хакерів до організованих злочинних угруповань і навіть державних структур, є головною загрозою в сучасному кіберпросторі. Такі атаки можуть призвести не лише до втрати даних, але й до фінансових втрат, порушення роботи підприємств, а у випадку з критично важливою інфраструктурою – до серйозних соціальних наслідків.

Кібератаки є суттєвим викликом для сучасних компаній, оскільки вони не

лише створюють безпосередні загрози безпеці інформації, але й можуть призводити до комплексних і масштабних проблем, які стосуються всієї діяльності організації. Традиційними продовж останніх років є такі загрози кіберезпеці: шкідливе ПЗ, DoS-атаки, фішинг, програми-вимагачі, атаки нульового дня, методи соціальної інженерії, ботнети тощо. Водночас, відповідно до прогнозів Європейського Агентства з кібербезпеки ENISA у період до 2030 року людство зіткнеться з такими загрозами й викликами кібербезпеці [6] (Рис. 1.3):

Рис. 1.3. Актуальні загрози кібербезпеці на період до 2030 року

- Компрометація ланцюга поставок внаслідок залежності від ПЗ.
- Просунуті, масштабні дезінформаційні кампанії.
- Зростання авторитарного цифрового стеження, що має наслідком втрату приватності.
- Зростання ролі людських помилок і використання застарілих систем в кіберфізичних екосистемах.
- Цілеспрямовані атаки, посилені даними смарт-пристроїв.
- Відсутність аналізу й належного управління космічною інфраструктурою та об’єктами.

- Зростання кількості розширених гібридних загроз.
- Дефіцит навичок у галузі кіберезпеки.
- Транскордонні постачальники послуг ІКТ як єдина точка невдач.
- Зловживання штучним інтелектом.

Значні фінансові втрати, які компанії зазнають в результаті кібератак, часто є лише верхівкою айсберга. Прямі збитки, такі як крадіжка фінансової інформації або вимагання викупу за дешифрування даних після атаки програм-вимагачів, чітко вказують на необхідність посилення кібербезпеки. Однак, поза цими безпосередніми втратами, існує цілий ряд складних проблем, що вимагають глибшого розуміння та системного підходу.

Вплив на репутацію компанії є одним з найбільш значущих довгострокових наслідків кіберінцидентів. Якщо інформація про кібератаку стає відома публіці, це може негативно позначитися на довірі клієнтів та партнерів, а також привести до втрати ринкової вартості. Відновлення репутації вимагає часу та ресурсів, і часто стає довгостроковим завданням для компанії.

Порушення діяльності компанії через кібератаки також є серйозним викликом. Зупинка виробничих процесів, збої у системах управління та втрата критично важливих даних можуть мати негативні наслідки для бізнесу, які виходять далеко за рамки безпосередніх втрат від самої атаки.

Юридичні наслідки та відповідальність перед регулюючими органами стають все більш актуальними в контексті зростаючих вимог до захисту даних. Компанії, що зазнали кібератак, можуть зіштовхнутись із судовими позовами, штрафами та вимогою до вжиття додаткових заходів безпеки, що вимагає додаткових витрат та ресурсів.

Втрата інтелектуальної власності через кібератаки може надовго підірвати конкурентоспроможність компанії, особливо якщо в руки конкурентів потрапляють важливі торгові секрети, стратегії або інноваційні розробки.

1.3 Огляд основних теоретичних моделей кібербезпеки

Структура або ж модель кібербезпеки – це набір політик, практик і процедур, які впроваджуються для створення ефективної безпеки. Ці рамки надають організаціям вказівки щодо захисту своїх активів від кіберзагроз шляхом виявлення, оцінки та керування ризиками, які можуть призвести до витоку даних, збоїв у системі чи інших збоїв [7].

Інфраструктури кібербезпеки допомагають організаціям розробляти та підтримувати ефективну стратегію безпеки, яка відповідає конкретним потребам середовища. Завдяки оцінці поточних практик безпеки та виявленню прогалин у захисті ці інфраструктури допомагають командам із кібербезпеки впроваджувати належні заходи захисту для захисту критично важливих активів.

Нижче перелічені найактуальніші міжнародні фреймворки для досягнення відповідності вимог безпеки:

1. Концепція NIST

Національний інститут стандартів і технологій (NIST) є урядовою агенцією, яка відповідає за вдосконалення технологій і стандартів безпеки в Сполучених Штатах. Структура кібербезпеки NIST надає організаціям рекомендації щодо виявлення, захисту, виявлення, реагування на кібератаки та відновлення після них. Структуру було створено в 2014 році як керівництво для федеральних агентств, але принципи застосовуються майже до будь-якої організації, яка прагне створити безпечне цифрове середовище.

Тепер у своїй другій версії структура NIST є комплексним набором найкращих практик для організацій, які прагнуть покращити свою безпеку. Він містить докладні вказівки щодо управління ризиками, управління активами, контролю ідентифікації та доступу, планування реагування на інциденти, управління ланцюгом поставок тощо [8].

На рисунку 1.4 зображено ключові функції концепції NIST

- Ідентифікація передбачає розробку розуміння організацією, як

управляти кіберризиками для систем, активів, даних і можливостей.

- Захист визначає заходи безпеки для забезпечення виконання критично важливих сервісів.
- Виявлення описує дії для ідентифікації настання події.
- Реагування включає дії, що необхідно здійснити у відповідь на виявлений інцидент кібербезпеки.
- Відновлення визначає діяльність для підтримки планів стійкості та відновлення функціональних можливостей або сервісів, що були порушені внаслідок інциденту кібербезпеки [9].

Рис. 1.4. Принципи концепції NIST

2. ISO 27001 та 27002

ISO 27001 та ISO 27002 є двома найпоширенішими стандартами для управління інформаційною безпекою сьогодні. Ці стандарти забезпечують комплексну основу для організацій, які прагнуть захистити свої дані за допомогою надійних політик і найкращих практик.

Ці стандарти, розроблені Міжнародною організацією зі стандартизації (ISO), викладають принципи та методи, які гарантують, що організації вживають відповідних заходів для захисту своїх даних. Від управління активами та контролю доступу до реагування на інциденти та безперервності бізнесу, ці стандарти містять вказівки, які допоможуть компаніям захистити свої мережі.

ISO 27001 — це міжнародний стандарт, який забезпечує системний підхід до оцінки ризиків, вибору засобів контролю та впровадження. Він містить вимоги щодо створення системи управління інформаційною безпекою (СУІБ).

ISO 27002 — це кодекс практики, який описує більш конкретні та детальні засоби контролю безпеки. При спільному застосуванні ці два стандарти надають організаціям комплексний підхід до управління інформаційною безпекою.[10]

Рис. 1.5. Переваги стандартів ISO 27000

На рис. 1.5 зображено ключові переваги та наголошення стандартизації ISO серії 27000, серед яких:

- Зниження вразливостей безпеки.
- Оптимізація витрат.
- Вдосконалений менеджмент безпекою.
- Постійне вдосконалення стану безпеки.
- Зростання довіри зацікавлених клієнтів [10].

3. CIS Controls

Центр управління безпекою в Інтернеті (CIS) надає передові методи для організацій, які прагнуть захистити свої мережі від кіберзагроз. Ця структура включає 20 засобів контролю, що охоплюють багато областей безпеки,

наприклад контроль доступу, управління активами та реагування на інциденти.

Елементи управління CIS поділяються на три категорії: базові, фундаментальні та організаційні (Рис. 1.6).

Рис. 1.6. Засоби управління CIS

Базові засоби (1-6): ключові засоби управління, які слід запровадити в кожній організації для забезпечення необхідної готовності до кіберзахисту.

Фундаментальні (7-16): найкращі технічні методи, які забезпечують безперечні переваги безпеки та є раціональним кроком для будь-якої організації.

Організаційні (17-20): ці засоби контролю відрізняються від попередніх, оскільки незважаючи на значну кількість технічних елементів, більше зосереджені на людях і процесах, залучених до кібербезпеки [11].

4. SOC 2

Структура контролю організації обслуговування (SOC) — це стандарт аудиту, який використовується сторонніми аудиторами для оцінки безпеки, доступності, цілісності обробки, конфіденційності та конфіденційності систем і служб компанії. SOC2 є одним із найпоширеніших стандартів у цій структурі, спеціально розроблений для постачальників хмарних послуг.

Стандарт SOC вимагає від організацій надавати детальну документацію щодо своїх внутрішніх процесів і процедур, пов’язаних із безпекою, доступністю, цілісністю обробки, конфіденційністю та конфіденційністю. Документи, сумісні з SOC, повинні включати такі політики, як заходи контролю доступу, протоколи шифрування даних, плани реагування на інциденти тощо.

Організації також повинні надати докази ефективності своїх засобів контролю, як-от журнали аудиту або результати тестів на проникнення, щоб переконатися, що їхні заходи безпеки функціонують належним чином і можуть захистити їхні дані від кіберзагроз [12].

5. PCI-DSS

Рада основних платіжних процесів розробила стандарт безпеки даних платіжних карток (PCI-DSS) для захисту даних платіжних карток клієнтів. Цей стандарт містить комплексний набір вимог, розроблених для того, щоб допомогти організаціям захистити свої системи та запобігти несанкціонованому доступу до інформації про клієнтів [13].

Структура PCI-DSS включає 12 вимог, яким організації повинні відповідати для захисту даних клієнтів. Ці вимоги охоплюють контроль доступу, безпеку мережі та зберігання даних, характерні для галузі обробки платежів. Він також включає заходи щодо захисту даних платіжних карток клієнтів, включаючи технології шифрування та токенізації (Рис. 1.7) [14].

Серед вимог фреймворк PCI DSS виділяє:

- Створення та підтримання захищеної мережі.
- Захист збережених даних платіжних карт.
- Розробка та підтримання заходів безпеки.
- Захист переданих даних платіжних карт у відкритих мережах.
- Регулярне оновлення та управління системи захисту від вірусів.
- Розробка та підтримання захищених систем і додатків.
- Обмеження доступу до даних платіжних карток.
- Ведення ідентифікації користувачів.
- Обмеження фізичного доступу до даних карт.

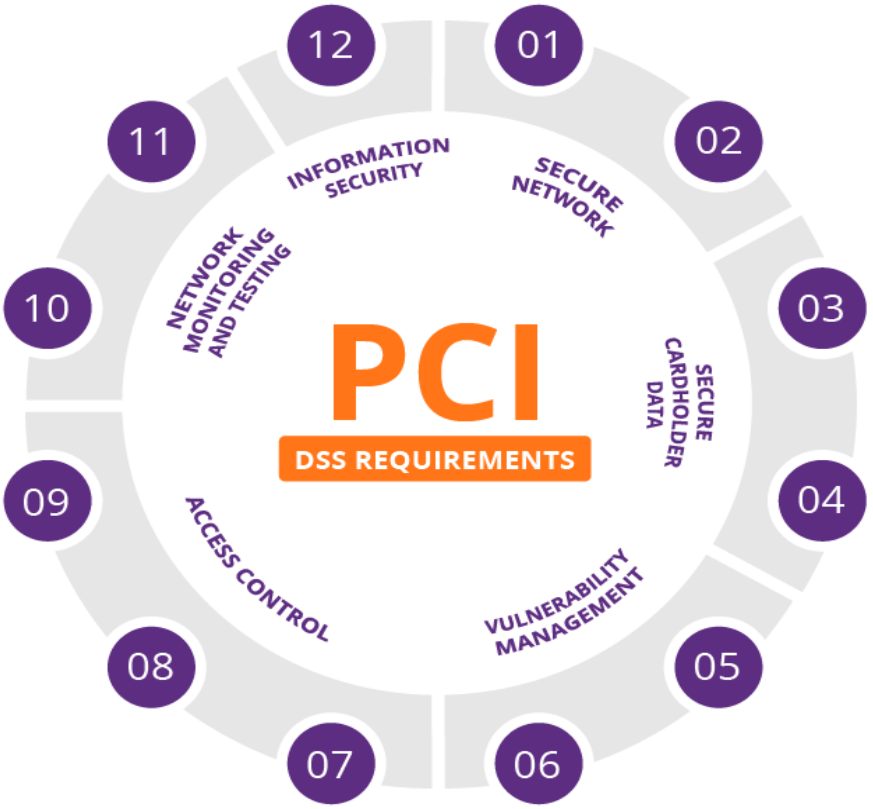

Рис 1.7. Вимоги PCI-DSS

- Відстеження та моніторинг доступу до мережевих ресурсів і даних платіжних карток.
- Регулярне тестування систем безпеки.
- Політика безпеки для всіх працівників.

6. COBIT

Цілі управління інформаційними та пов'язаними технологіями (COBIT), розроблені Асоціацією аудиту та контролю інформаційних систем (ISACA), є комплексною структурою, розробленою для того, щоб допомогти організаціям ефективніше керувати своїми IT-ресурсами. Ця структура пропонує найкращі практики управління, управління ризиками та безпеки.

Структура COBIT розділена на п'ять категорій: планування й організація, придбання та впровадження, надання і підтримка, моніторинг і оцінка, керування й оцінка (Рис. 1.8). Кожна категорія містить певні процеси та дії, які допомагають організаціям ефективно керувати своїми IT-ресурсами.

COBIT також містить докладні вказівки з безпеки та захисту даних, що охоплюють контроль доступу, автентифікацію користувачів, шифрування,

журнал аудиту та області реагування на інциденти. Ці вказівки надають організаціям повний набір заходів, які можна використовувати для захисту їхніх систем від кіберзагроз [15].

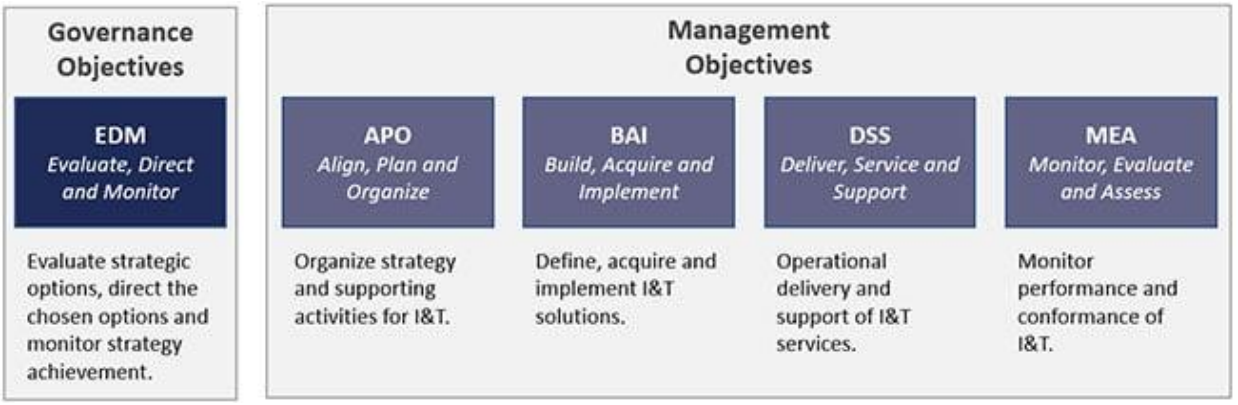

Рис. 1.8. Категорії заходів COBIT.

7. HITRUST модель безпеки

Загальна структура безпеки (CSF) Альянсу довіри до інформації про охорону здоров'я (HITRUST) - це комплексна структура безпеки, розроблена для галузі охорони здоров'я. Цей стандарт включає найкращі методи захисту безпеки даних пацієнтів, охоплюючи такі сфери, як контроль доступу, ідентифікація й управління доступом, шифрування, ведення журналів аудиту та реагування на інциденти.

HITRUST CSF включає детальне управління кібербезпекою, управління ризиками та вимоги дотримання, допомагаючи організаціям відповідати відповідним нормативним вимогам, одночасно захищаючи свої системи від потенційних кіберзагроз [16].

8. CCM

Cloud Control Matrix (CCM) від Cloud Security Alliance (CSA) - це комплексна структура безпеки для хмарних систем і програм, яка охоплює контроль доступу, автентифікацію користувачів, шифрування, ведення журналів аудиту та реагування на інциденти.

Подібно до HITRUST, CCM також містить докладні вказівки щодо управління безпекою та управління ризиками та спрямований на допомогу організаціям у відповідності до відповідних нормативних стандартів [17].

9. CMMS 2.0

CMMC 2.0 (Cybersecurity Maturity Model Certification) - це остання версія інфраструктури Міністерства оборони США (DOD), оголошена в 2021 році і розроблена для захисту інформації про національну безпеку шляхом створення набору узгоджених стандартів кібербезпеки для будь-якої організації, яка працює з DOD.

У CMMC 2.0. є три окремі рівні залежно від конфіденційності даних, які обробляє організація. Кожен рівень має збільшену кількість необхідних практик, а також інтенсивність оцінювання. На базовому рівні 1 існує 17 практик із щорічною самооцінкою. На рівні 3 потрібно понад 110 практик разом із трирічним оцінюванням під керівництвом уряду [18].

Також варто згадати моделі кібербезпеки для потреб відповідності вимогам певних країн і регіонів:

10. Essential 8

Essential 8 - це базова структура кібербезпеки, якої рекомендовано дотримуватися всім організаціям Азіатсько-Тихоокеанського регіону, подібна до NIST Framework у США. Створена ACSC (Австралійським центром кібербезпеки) у 2017 році, Essential 8 є набором мінімальних найкращих практик для уникнення компрометації систем. На відміну від багатьох інших підходів, він спеціально зосереджений на мережах на базі Microsoft Windows.

Головною метою є : запобігання кібератак, пом’якшення впливу кібератак та відновлення даних та доступності систем [19].

Essential 8 виділяє такі методи пом’якшення загроз як:

- контроль і виправлення додатків;
- зміцнення додатків користувача;
- обмеження адміністративних привілеїв;
- виправлення операційних систем;
- багатофакторна аутентифікація;
- регулярне резервне копіювання.

11. Cyber essentials

Cyber Essentials - це основна структура для Великобританії, створена NCSC (Національним центром кібербезпеки) у 2014 році. Структура побудована навколо п’яти основних технічних засобів управління, призначених для захисту від найпоширеніших кібератак: брандмауери й маршрутизатори, безпечна конфігурація, управління доступом, захист від шкідливих програм, управління виправленнями/оновлення програмного забезпечення.

Окрім надання базового набору стандартів для захисту організацій, дотримання Cyber Essentials вимагається для деяких державних контрактів Великобританії. Доступні два рівні сертифікації: базова самооцінка, а також сертифікація Cyber Essentials Plus, яка вимагає технічної перевірки від третьої сторони [20].

Загалом ці найпоширеніші моделі кібербезпеки охоплюють різні підходи до вирішення проблем кібербезпеки. Перш ніж вибрати одну з них, важливо оцінити потреби й можливості конкретної організації та визначити, яка структура їм найкраще відповідає. Вибір оптимального підходу допоможе організації налагодити ефективне управління безпекою, надасть детальні вказівки і процедури захисту від відповідних загроз цифровим активам бізнесу.

Висновки до розділу 1

У розділі 1 досліджено поняття кібербезпеки та кіберстійкості, важливість яких постійно зростає у сучасному цифровому світі.

Встановлено відмінності між концепціями кібербезпеки та кіберстійкості бізнесу, зокрема зазначено, що метою кібербезпеки є постійний захист цифрових мереж і систем бізнесу, щоб запобігти зловмисникам в реалізації кібератак. Натомість метою кіберстійкості є готовність до реалізованих кібератак, забезпечення можливості попри це далі вести бізнес та швидко відновлюватися.

Кібербезпека використовує такі засоби як міжмережеві екрани, антивіруси, криптографію, спрямовує зусилля на запобігання порушенням безпеки і неавторизованому доступу, протидіє загрозам ззовні. Кіберстійкість впроваджує стратегії реагування на інциденти і системи резервного копіювання, спрямовує зусилля на забезпечення безперервності бізнесу навіть після інциденту, протидіє загрозам як зовнішньо, так і внутрішньо, забезпечуючи організаційну стійкість.

З’ясовано, що традиційними продовж останніх років є такі загрози кіберезпеці як шкідливе ПЗ, DoS-атаки, фішинг, програми-вимагачі, атаки нульового дня, методи соціальної інженерії, ботнети тощо. Водночас, новими загрозами й викликами кібербезпеці стануть компрометація ланцюга поставок, масштабні дезінформаційні кампанії, тотальне цифрове стеження, зростання кількості розширених гібридних загроз, зловживання штучним інтелектом тощо.

У рамках дослідження розглянуто ключові теоретичні моделі кібербезпеки (ISO 27000, COBIT, NIST, CIS та інші), які дозволять підприємствам формувати ефективні стратегії захисту. Підкреслено, що інтеграція цих концепцій у бізнес-стратегії є критично важливою для створення стійкої та безпечної цифрової екосистеми, а комплексний підхід до управління кіберризиками, який охоплює технічні, адміністративні й репутаційні заходи, є необхідністю для сучасного бізнесу, щоб ефективно реагувати на динамічні загрози у кіберпросторі.

РОЗДІЛ 2
МЕТОДИ Й ПІДХОДИ ДО ЗАБЕЗПЕЧЕННЯ КІБЕРБЕЗПЕКИ ПІДПРИЄМСТВА

2.1 Превентивні методи кібербезпеки

Превентивні методи кібербезпеки - це підходи та заходи, спрямовані на запобігання кібератакам або іншим інцидентам кібербезпеки, перш ніж вони стануться. Вони включають широкий спектр технічних і адміністративних засобів, таких як шифрування даних, фаєрволи, антивірусне програмне забезпечення, політики безпеки та навчання персоналу. Ці методи мають на меті зменшити вразливість систем і мереж до потенційних загроз і забезпечити, щоб організація була краще підготовлена до виявлення, протистояння і мінімізації наслідків небажаних подій.

Gartner, один із ключових лідерів громадської думки в галузі кібербезпеки, зазначає, що у 2023 році світ витратив на безпеку та управління ризиками на 11,3% більше порівняно з 2022 роком. Організації витрачають більше на кібербезпеку, щоб керувати ризиками розширення поверхні атак, що значною мірою спричинено такими факторами [21]:

- Збільшення дистанційної роботи.

Тенденція віддаленої роботи продовжується, створюючи відсутність видимості та контролю над співробітниками. Віддалені середовища важче захистити, оскільки вони розташовані поза периметром організації. Гібридні робочі середовища також є джерелом ризику, оскільки вони розширюють зону потенційних атак. Коли працівникам кібербезпеки доводиться захищати як внутрішні, так і віддалені середовища, це збільшує ймовірність людської помилки та, зрештою, порушення.

- Перехід на хмарні технології

Gartner прогнозує, що до 2025 року більше половини корпоративних витрат в IT буде сфокусовано у хмарні. Захист хмарної інфраструктури може бути складним через збільшення кількості векторів атак, складність хмарних середовищ і розподіл обов'язків щодо безпеки між клієнтом і провайдером хмарних послуг.

- Взаємодія ланцюжків поставок

Ланцюжок поставок продовжує залишатися загальною точкою збою кібербезпеки. Зі збільшенням кількості третіх сторін, з якими бізнес інтегрується і взаємодіє, зростає ймовірність доступу хакерів до інфраструктури.

- Конвергенція IT/OT-IoT

Заходи безпеки та протоколи для пристроїв Інтернету речей (IoT) і операційних технологій (OT) все ще розробляються, наражаючи IT-системи на ризики кібербезпеки. Кіберзловмисники можуть використовувати пристрої IoT і OT як точки входу в системи організації.

У сучасних реаліях і, враховуючи нинішні технологічні тренди, захищаючи IT інфраструктуру організації, рекомендується зосередитися на таких напрямах кібербезпеки:

- Розвиток безпеки хмарного середовища організації:

Швидкі темпи міграції компаній у хмарні середовища в останні роки не залишили шансів для кібербезпеки, щоб надолужити такі темпи. Погано захищені віддалені робочі середовища, з яких часто можна отримати доступ до хмарних служб, та інші хмарні вразливості спонукають до швидкого розвитку індустрії хмарної безпеки. Gartner прогнозує значне зростання сектору хмарної безпеки у найближчих роках.

- Використання моделі нульової довіри для технології VPN:

Віртуальні приватні мережі можуть створити проблеми з масштабованістю, є схильними до кібератак і вразливими в сучасних гібридних середовищах. Тому підхід нульової довіри для цієї технології є безпечним і масштабованим. У США адміністрація Байдена вимагала від державних організацій відповідати принципам нульової довіри до кінця 2024 фінансового

року [22].

- Фокусування на безпеці інфраструктури ланцюгів поставок:

Очікується, що найближчими роками спеціалісти з кібербезпеки шукатимуть нові способи захисту ланцюгів поставок і розроблятимуть існуючі методи управління ризиками ланцюжків поставок у сфері кібербезпеки. Здебільшого це відповідь на випадки шпигунства, державні кібератаки та геополітичні збурення, які впливають на глобальний ланцюг поставок. Наприклад, у лютому 2022 року Росія націлилася на технології, задіяні в роботі критично важливої української інфраструктури [23]. За прогнозами Gartner, до 2025 року 45% організацій зазнають атак на ланцюжки поставок програмного забезпечення, що втричі більше, ніж у 2021 році.

- Посилення вимог відповідності стандартам кібербезпеки:

Уряди в усьому світі посилюють свої зусилля щодо захисту персональних даних своїх громадян. Gartner прогнозує, що сучасні правила конфіденційності стосуватимуться персональних даних 65% населення світу, порівняно з 10% у 2020 році. У 2023 році п’ять штатів США запровадили нові закони про конфіденційність даних. Після оновлення законів про кібербезпеку, стандартів і правил бізнес-компанії мають зосередити більше уваги на дотриманні вимог і захисті корпоративних даних.

- Розвиток інструментів виявлення загроз і реагування на них:

Єдиний спосіб, завдяки якому організація може ефективно впоратися з атаками, - це максимально оперативно виявити підозрілу активність користувачів у корпоративній інфраструктурі та негайно відреагувати на неї. Рішення для виявлення загроз і реагування створені саме для цього. Gartner зазначає, що попит на хмарні засоби виявлення й реагування зросте найближчим часом.

Нижче перелічені найактуальніші методи превентивного захисту від кіберзагроз:

1. Створення надійних політик кібербезпеки.

Політика кібербезпеки служить офіційним посібником із впровадження

всіх заходів компанії з метою підвищення ефективності кіберзахисту. Політика допомагає фахівцям із безпеки та співробітникам бути на одній «хвилі» й описує основні практики інформаційної безпеки для всієї компанії.

Доцільно розглянути можливість впровадження ієрархічної політики кібербезпеки, яка складається з єдиної централізованої політики та додаткових політик, унікально розроблених для різних підрозділів організації. Ієрархічна політика кібербезпеки враховує унікальні потреби кожного підрозділу, допомагаючи підвищити загальну ефективність політики кібербезпеки й уникнути порушення окремих робочих процесів. Аналогічним чином організація може розробити політики безпеки з урахуванням різних сфер кіберзахисту організації, наприклад, політики управління активами, мережевої та операційної безпеки, контролю доступу, безпечного використання електронної пошти і браузера, безпеки персоналом тощо.

2. Захист корпоративного периметра безпеки і мережі IoT

Сучасні периметри організацій простягаються далеко за брандмауери та DMZ, оскільки віддалена робота, хмарні середовища та пристрої IoT значно розширюють зону атаки. Очікується, що ринок IoT зросте приблизно до 567 мільярдів доларів у 2027 році з приблизно 384 мільярдів доларів у 2021 році.

Камери безпеки, дверні дзвінки, розумні дверні замки, системи опалення й офісне обладнання - багато з них підключені до Інтернету і можуть бути використані як потенційні вектори атак. Наприклад, зламаний принтер може дозволити зловмисникам переглядати всі роздруковані або відскановані документи.

Варто подумати про захист периметра компанії, щоб захистити свої прикордонні маршрутизатори і створити екрановані підмережі. Щоб підвищити безпеку бази даних підприємства, доцільно відокремити конфіденційні дані від корпоративної мережі й обмежити доступ до таких даних. Організація може поєднати звичайні засоби захисту, такі як брандмауери та VPN, із моделлю нульової довіри, щоб захистити свої активи і системи. Відповідно до концепції нульової довіри обов’язковою є постійна перевірка користувачів і пристроїв

організації, щоб запобігти несанкціонованому доступу.

3. Використання підходів безпеки, орієнтованих на людей

Технологічно-центричного підходу до кібербезпеки недостатньо для забезпечення повного захисту, оскільки хакери часто використовують людей як точки входу.

Згідно зі звітом Verizon про розслідування витоку даних за 2022 рік, 82% зломів пов'язані з людським фактором. Підхід, орієнтований на людей, може допомогти організації зменшити ризики, пов'язані з людьми. У безпеці, орієнтованій на людей, важливим периметром є самі працівники. Навчання та контроль за персоналом – це головне, що потрібно враховувати для безпечного середовища, орієнтованого на людей.

На рис 2.1 показані вимоги щодо забезпечення безпеки даних з урахуванням людського фактора.

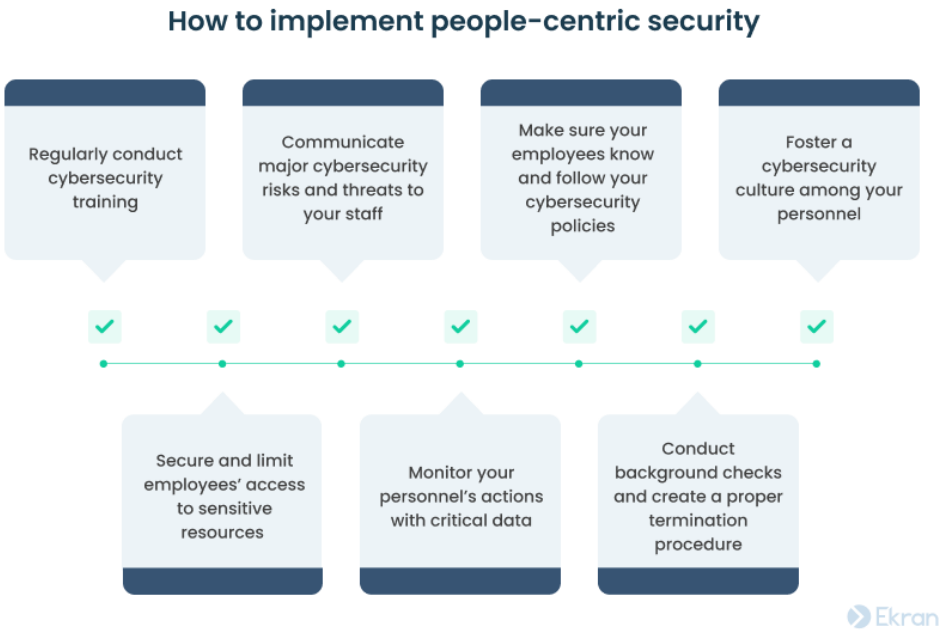

Рис. 2.1. Вимоги до стратегії безпеки, орієнтованої на людей

До основних вимог стратегії безпеки, орієнтованої на людей, відносять: проведення регулярного навчання з кібербезпеки для працівників, інформування персоналу про основні ризики та загрози кібербезпеки, запевнення менеджменту в тому, що співробітники знають і дотримуються політик кібербезпеки компанії, сприяння культурі кібербезпеки серед персоналу, забезпечення безпечного

доступу для працівників до чутливих ресурсів, моніторинг дій персоналу, що працює з критично важливими даними, та перевірка бекграунду працівників. Ці кроки підкреслюють важливість не лише технічних заходів, але й ключову роль персоналу у забезпеченні кібербезпеки шляхом навчання й залучення працівників до практик безпеки [24].

4. Контроль доступу до чутливих даних:

Надання співробітникам багатьох привілеїв за замовчуванням дозволяє їм отримувати доступ до конфіденційних даних, навіть якщо їм це не потрібно. Такий підхід підвищує ризик інсайдерських загроз і дозволяє хакерам отримати доступ до конфіденційних даних, щойно вони скомпрометують обліковий запис співробітника.

Застосування моделі мінімальних дозволів (також називається принципом найменших привілеїв) є набагато кращим рішенням, яке передачає призначення кожному користувачеві найменших можливих прав доступу та підвищення привілеїв лише за необхідності. Якщо доступ до конфіденційних даних не потрібен, відповідні привілеї відкликають.

На додаток до принципу найменших привілеїв і моделі нульової довіри, своєчасний підхід до управління доступом забезпечує ще більшу деталізацію контролю привілеїв користувачів, надаючи персоналу доступу за запитом на певний час і з поважної причини.

Варто звернути особливу увагу на віддалений доступ до корпоративної інфраструктури. Захист співробітників, які працюють дистанційно, вимагає поєднання таких заходів як покращення видимості їхніх дій і належне налаштування мереж організації.

5. Жорсткий менеджмент паролів:

Облікові дані співробітників надають кіберзлочинцям прямий доступ до конфіденційних даних і цінної бізнес-інформації, що належить або обробляється компанією. Атаки типу брутфорс, соціальна інженерія та інші методи можуть бути використані для компрометації облікових даних співробітників без відома організації.

Організації часто використовують спеціалізовані інструменти управління паролями, щоб запобігти таким атакам. Такі рішення можуть надати контроль над обліковими даними персоналу, зменшуючи ризик компрометації облікових записів. Варто віддати перевагу засобам управління паролями, які забезпечують автентифікацію без пароля, одноразові паролі й можливості шифрування паролів.

Якщо організація схильна довіряти своїм співробітникам і готова дати їм право самостійно управляти своїми паролями, необхідно встановити такі вимоги щодо політики паролів кібербезпеки:

- використання окремого пароля для кожного облікового запису;
- створення окремих облікових записів для особистого й комерційного використання;
- створення складних паролів зі спеціальними символами, цифрами та великими літерами;
- використання мнемотехніки та інших тактик для запам’ятовування довгих паролів;
- використання менеджерів і генераторів паролів;
- заборона повідомлення облікових даних іншим співробітникам;
- регулярна зміна паролів, принаймні раз на три місяці.

6. Відстеження активності привілейованих та сторонніх користувачів:

Привілейовані користувачі та треті сторони, які мають доступ до інфраструктури компанії, володіють усіма засобами, щоб викрасти конфіденційні дані й залишитися непоміченими. Навіть якщо ці користувачі не діють зловмисно, вони можуть ненавмисно спричинити порушення кібербезпеки.

Найефективнішим способом захистити конфіденційні дані компанії є відстеження діяльності привілейованих і сторонніх користувачів у корпоративному IT-середовищі. Моніторинг активності користувачів (UAM) допомагає підвищити видимість, виявити зловмисну активність і зібрати докази для судових розслідувань. Рішення UAM надає корисну інформацію про те, чим займаються працівники організації і користувачі. Інструменти UAM відстежують дії користувачів у формі скріншотів і надають відомості про відвідані веб-сайти,

натиснуті клавіші та відкриті програми [25].

7. Управління ризиками ланцюгів поставок:

Постачальники, партнери, субпідрядники, провайдери послуг та інші треті сторони, які мають доступ до ресурсів організації, можуть бути вразливими до атак на ланцюг поставок. Відповідно до 8-го щорічного звіту про стан ланцюга поставок [26], з 2019 по 2022 рік кількість атак на ланцюги поставок програмного забезпечення зросла на дивовижні 742%, що графічно зображено на рис 2.2.

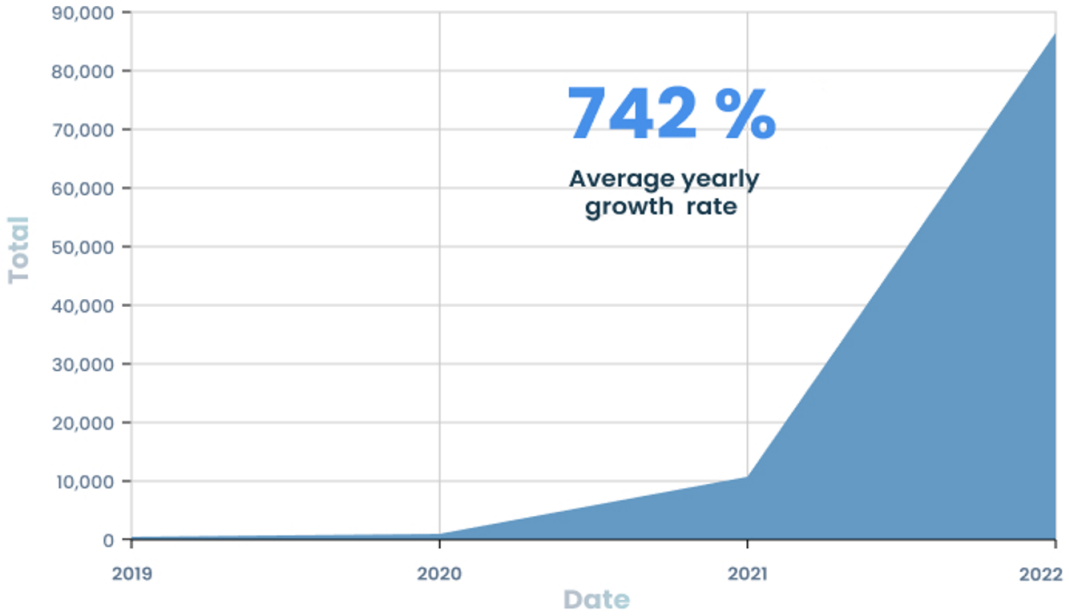

Рис. 2.2. Графік динаміки атак на ланцюги поставок у 2019-2022 рр.

Під час атаки на ланцюжок постачання кіберзлочинці проникають або зривають роботу одного з постачальників і використовують це для ескалації атаки далі по ланцюгу постачання, що може вплинути на організацію-кінцевого споживача продуктів чи послуг. Так, під час злому Solarwinds кіберзлочинцям вдалося отримати доступ до мереж і даних тисяч організацій, вставивши зловмисний код в оновлення програмного забезпечення Solarwinds [27].

Щоб усунути ризики в ланцюзі поставок, компанія має мислити ширше управління ризиками третіх сторін і розробити комплексну стратегію управління ризиками в кібернетичному ланцюжку поставок (C-SCRM). C-SCRM сприятиме безперервності бізнесу й покращить видимість ланцюга постачання. Спеціальна публікація NIST SP 800-161r1 [28] і NIST Key Practices in Cyber SCRM [29] можуть допомогти організації створити власну програму C-SCRM.

8. Удосконалення захисту й управління даними:

Управління бізнес-даними має вирішальне значення для конфіденційності та безпеки організації. Для ефективного управління даними доцільно почати з документування процесів управління інформацією у відповідній політиці, зокрема сформувати перелік даних, які збираються, обробляються та зберігаються в організації; встановити посадових осіб, які мають до них доступ; визначити місця зберігання й термін використання/видалення даних; окреслити заходи щодо захисту даних.

Зазвичай, при розробці заходів захисту даних організації орієнтуються на дотримання ключових принципів інформаційної безпеки або ж так званої тріади CIA: цілісності, доступності й конфіденційності. Видання Gartner виділяє чотири ключові методи для їх забезпечення: криптошифрування, маскування, видалення даних, що вже не використовуються або неактивні, а також резервне копіювання критично важливих даних для подальшого відновлення в разі інциденту [30].

9. Використання біометричного захисту:

Біометрія забезпечує швидку автентифікацію персоналу, безпечне управління доступом і точну ідентифікацію. Біометрія - це надійний спосіб перевірити особистість працівників і користувачів перед наданням доступу до цінних активів. Біометричні технології забезпечують більш надійну автентифікацію, ніж паролі, тому їх часто використовують для багатофакторної автентифікації (MFA). Однак автентифікація - не єдина сфера використання біометрії. Служби безпеки застосовують різні біометричні методи для виявлення зламаних привілейованих облікових записів у режимі реального часу [30].

Поведінкова біометрія особливо корисна для контролю безпечної активності користувачів, оскільки дозволяє аналізувати унікальні способи взаємодії користувачів із пристроями введення. Співробітники служби безпеки у разі виявлення аномальної поведінки отримують сповіщення і можуть негайно відреагувати.

Системи аналітики поведінки користувачів і об’єктів (UEBA), які аналізують діяльність користувачів, використовують такі поведінкові

біометричні фактори:

- динаміку використання клавіш, що відстежує швидкість набору тексту та схильність до типових людських помилок у певних словах для створення профілів поведінки користувача;
- динаміку миші, що відстежує час між натисканнями і швидкість, ритм і стиль переміщення курсора [32].

10. Використання мультифакторної автентифікації (MFA):

Багатофакторна автентифікація допомагає захистити конфіденційні дані, додаючи додатковий рівень безпеки. Якщо MFA активовано, зловмисники не можуть увійти, навіть якщо вони мають пароль користувача, оскільки для входу необхідно володіти інформацією про інші фактори автентифікації, такі як номер мобільного телефону, відбиток пальця, голос або маркер безпеки.

Незважаючи на те, що MFA вважається базовим засобом перевірки, вона є одним із найкращих методів захисту й відповідає більшості вимог кібербезпеки, зокрема Загальному регламенту захисту даних (GDPR), стандарту безпеки даних індустрії платіжних карток (PCI DSS) і програмі безпеки клієнтів SWIFT (CSP). Такі технічні гіганти, як Google і Twitter, рекомендують своїм користувачам прийняти MFA. Додатковою перевагою MFA є можливість розрізняти користувачів спільних облікових записів, покращуючи можливості контролю доступу [33].

11. Регулярне проведення аудитів кібербезпеки:

Регулярне проведення аудитів допомагає оцінити стан кібербезпеки організації та, за потреби, скорегувати його. Під час перевірок виявляють вразливості кібербезпеки, прогалини у дотриманні вимог нормативної відповідності, підозрілу активність співробітників, привілейованих користувачів і сторонніх партнерів. Якість аудиту залежить від повноти даних з різних джерел: журналів аудиту, записів сеансів і метаданих.

Детальні журнали безпеки рішень UAM надають інформацію про дії як кінцевих, так і привілейованих користувачів, включаючи метадані активності, знімки екрана та інші корисні дані. На основі цієї інформації проводять аналіз

першопричин подій безпеки та виявляють слабкі місця корпоративної системи кібербезпеки. Якщо організація приймає рішення про розгортання рішення UAM, варто звернути увагу на продукти, які пропонують звітування про певні типи дій, інциденти, користувачів тощо, оскільки саме звіти дозволяють значно прискорити і спростити проведення аудитів [34].

12. Спрощення технологічної інфраструктури бізнесу:

Розгортання й обслуговування великої кількості інструментів є дорогим і трудомістким. Крім того, програмне забезпечення, яке потребує ресурсів, може уповільнити робочі процеси організації. Для оптимізації і спрощення інфраструктури безпеки організація повинна мати одне або кілька комплексних рішень з усіма необхідними функціями [35].

2.2 Детективні методи кібербезпеки

Детективні засоби управління є ключовим компонентом програми кібербезпеки, що забезпечує видимість зловмисної діяльності, порушень і атак на IT-середовище організації. Ці засоби охоплюють реєстрацію подій і пов’язаний моніторинг і сповіщення, які сприяють ефективному управлінню IT. Під час аудиту програми кібербезпеки аудитори повинні визначити й оцінити ці критичні засоби управління.

Детективні методи допомагають виявити атаки, яким не вдалося запобігти з використанням превентивних заходів, та є важливою частиною комплексної стратегії кібербезпеки. Якщо спеціальні засоби виявлення кібербезпеки належним чином спроектовані й ефективно функціонують, то вони можуть зупинити кіберзагрози. Ці елементи управління зазвичай виконуються або контролюються центром операційної безпеки (SOC), який відповідає за моніторинг кібербезпеки [36].

Система управління інформацією про безпеку та подіями (SIEM) є

центральною програмною платформою, яка інтегрує журнали подій, зібрані з кількох джерел, із джерелами даних про загрози (наприклад, канали в реальному часі) та контекстну інформацію про активи й користувачів [37]. Типовим прикладом SIEM системи є IBM QRadar (Рис. 2.3).

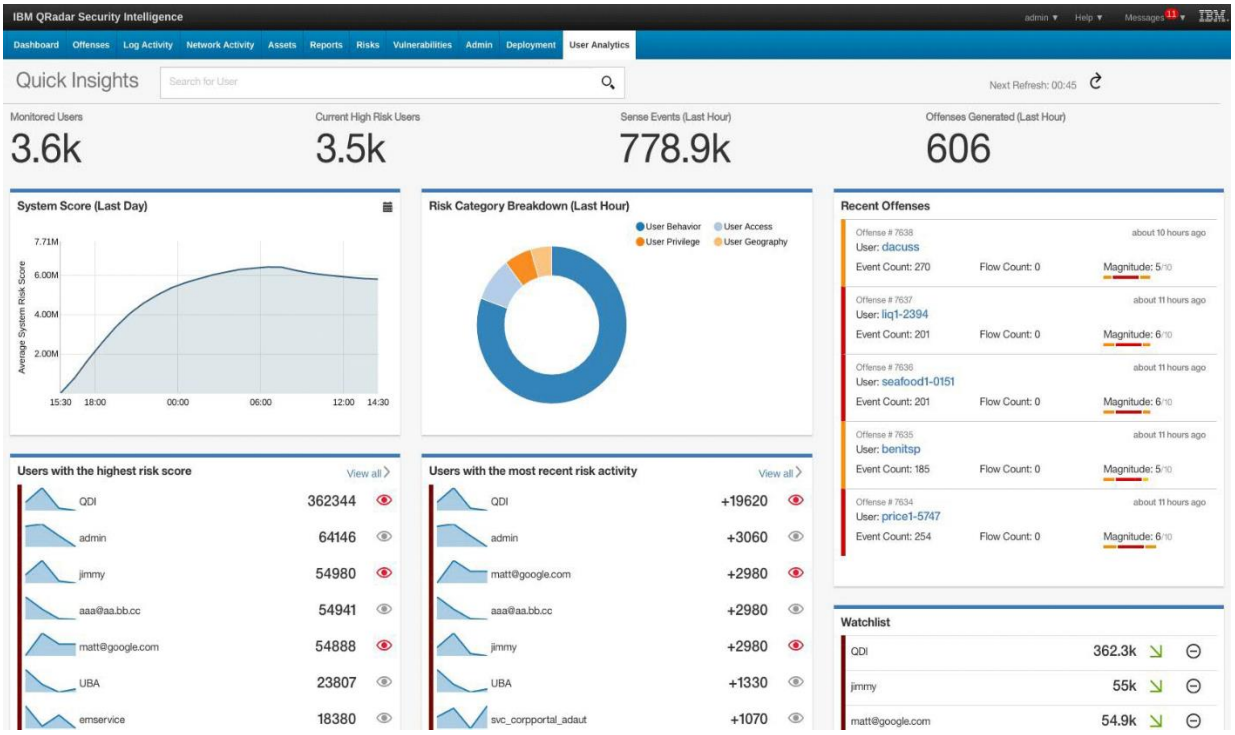

Рис. 2.3. SIEM система IBM QRadar

Існують альтернативи підходу SIEM, включаючи системи виявлення вторгнень (IDS) і системи запобігання вторгненням (IPS), які збирають і аналізують дані безпеки. Також є можливість повністю передати функцію моніторингу безпеки сторонньому постачальнику.

SIEM агрегує, нормалізує (стандартизує формат) і корелює дані про події, щоб ідентифікувати та пріоритезувати загрози, відфільтровувати помилкові спрацьовування й надавати оперативну інформацію про загрози. Унікальний контекст організації (активи, користувачі, ризики) має бути інтегрований в операції SIEM. SIEM є основним інструментом для аналізу безпеки, реагування на інциденти, криміналістики та дотримання нормативних вимог (звітування). Критичні можливості для управління інформацією про безпеку й управління подіями в загальній SIEM включають моніторинг у реальному часі, розвідку загроз, моніторинг даних і користувачів, моніторинг програм, аналітику, управління журналами та звітування [38].

Конкретні випадки використання можуть включати виявлення підозрілої поведінки (наприклад, скомпрометовані привілейовані облікові записи користувачів, доступ до конфіденційних даних), виявлення порушень політики (наприклад, зміна конфігурації сервера), виявлення розширених постійних загроз (APT) і шахрайства (наприклад, зміна обсягів торгівлі або грошових переказів). Аудитори мають оцінити структуру й ефективність функціональності SIEM.

Управління журналом подій є критично важливим компонентом функціональності SIEM. Журнали подій мають бути агреговані з більшості або всіх розгорнутих технологій в організації, включаючи пристрої безпеки (брандмауери, IDS/IPS, веб-проксі), мережеві пристрої (маршрутизатори, комутатори), системи (наприклад, мейнфрейми, сервери середнього класу, розподілені сервери), програми, бази даних, пристрої зберігання даних, настільні комп’ютери кінцевих точок і мобільні пристрої. Дані журналів подій також агрегуються з різних технологічних функцій, таких як управління продуктивністю і змінами.

Налаштування вихідних систем для надсилання даних журналів до центральної системи SIEM може потребувати значних зусиль. У великих організаціях обсяг даних журналів подій може бути величезним, а вимоги до зберігання можуть бути високими і різноманітними [39].

Для управління журналами зазвичай використовують окремий модуль, сервер або компонент (наприклад, HP Arcsight Log Aggregator, IBM Security QRadar Log Manager). Аудитори завжди очікують максимального рівня охоплення журналів SIEM з IT-середовища організації для більш ефективних результатів.

Для успішного функціонування SIEM системи й розвідки загроз необхідно мати належним чином налаштовані джерела інформації про загрози. Gartner визначає розвідку загроз як знання, що ґрунтуються на доказах, включаючи контекст, механізми, індикатори, наслідки й дієві поради, існуючої або нової загрози або небезпеки для активів, які можуть бути використані для прийняття рішень щодо відповіді суб’єкта на цю загрозу чи небезпеку.

Існує широкий спектр постачальників аналізу загроз, які можуть надавати

тактичні або оперативні канали інформації про репутацію Інтернет-протоколу (IP) (наприклад, підозрювані джерела зловмисного ПЗ за IP або уніфікованим покажчиком ресурсу [URL]); профілі шкідливих програм; індикатори шаблонів компромісу, командування та управління (C&C); ексфільтраційні підходи.

Нижче представлений короткий огляд джерел розвідки загроз, класифікованих за наявними службами, доступними для прийому в систему SIEM:

- Постачальники SIEM, які пропонують канали аналізу загроз як частину єдиного рішення, наприклад, IBM QRadar SIEM у поєднанні зі службою IBM X-Force Threat Intelligence.
- Комерційна агрегована й упакована інформація про загрози з багатьох джерел: структурованих і неструктурованих, наприклад, канал CyberSquared ThreatConnect6 (у партнерстві з Cisco Sourcefire) і AlienVault Open Threat Exchange (OTX), який вважається найбільшим у світі краудсорсинговим сховищем даних про загрози.
- Безкоштовні канали розвідки загроз (наприклад, Google Safe Browsing API, Zeus Tracker Blocklist), які пропонуються через спільноту інформаційної безпеки переважно у форматі файлу кристалографічної інформації (CIF), включаючи чорні списки IP-адрес і URL-адрес, підозрюваних у зловмисній діяльності.
- Оригінальна інформація про загрози, що пропонується у вигляді каналів загроз, правил, чорних списків і синтаксичних аналізаторів (наприклад, RSA FirstWatch,8 який пропонує інформацію про передові та нові загрози на стратегічному і тактичному рівнях).

Існують відмінності в інформації про загрози, яка може бути необробленими, невідфільтрованими, неперевіреними даними з різними рівнями достовірності й інтелекту, які оброблені, відсортовані, дистильовані, точні та своєчасні й отримані з надійних джерел. Таким чином, явна перевага надається аналізу загроз.

Інтелектуальні дані про загрози стають більш корисними, коли аналітики безпеки застосовують контекстуальні знання й наукові методи до аналізу загроз.

Контекстуальне знання означає глибше значення подій минулого, теперішнього та майбутнього. Крім того, ці знання включають контекстуальний зв'язок між тактиками, техніками і процедурами (TTP) та операційним середовищем (наприклад, інфраструктурою). Конкретні розвідувальні дані, збагачені контекстом і корисними даними, є важливими для оцінювання серйозності і пріоритетності загроз [40].

Ще одним ключем для ефективної роботи з інцидентами є правильна оцінка серйозності і пріоритетизації вхідних інцидентів. Внутрішньою проблемою моніторингу активності, пов'язаної з безпекою, є потенційний потік подій і сповіщень, які можуть створюватися та передаватися в систему SIEM. За оцінками FireEye, типове розгортання системи кібербезпеки генерує п'ять сповіщень за секунду [41]. Лише небагато організацій мають ресурси для дослідження такого обсягу діяльності.

Ключовим показником інструментів моніторингу кібербезпеки (наприклад, SIEM) є не кількість сповіщень, а здатність виявляти реальні загрози, фільтрувати значущі сповіщення та збагачувати ці сповіщення контекстом, який полегшує дії. Ця фільтрація, перевірка й кореляція вхідних подій і сповіщень є ключовим процесом у загальних можливостях розшуку. Щоб зосередити ресурси (наприклад, час аналітика безпеки) на найбільш значних загрозах, організація має керувати потоком подій безпеки шляхом:

- зменшення кількості сповіщень від пристроїв, наприклад зміни частоти сповіщень з кожної секунди на кожну хвилину, групування сповіщень з однаковими IP адресами, джерелами та призначеннями, видалення непотрібних індикаторів та помилкових спрацьовувань;
- пріоритезація найбільш важливих сповіщень на основі бізнес-ризиків;
- встановлення пріоритетів за активами, впливом на бізнес-функції і типом діяльності (наприклад, маяки, порушення політики).

2.3 Реагування та відновлення після інцидентів

Реагування на інциденти

Реагування на інциденти та відновлення в контексті кібербезпеки – це критично важливі елементи захисту інформаційних систем від загроз та атак. У сучасному світі, де організації постійно зіштовхуються з різноманітними та складними кіберзагрозами, ефективне реагування на інциденти і здатність до швидкого відновлення є ключовими для забезпечення безперервності бізнесу та захисту чутливих даних.

Цей процес включає не тільки технічні аспекти, такі як ідентифікація та усунення загроз, але й організаційні заходи, зокрема планування, підготовку персоналу й розробку політик відновлення. Ключовим моментом є створення чіткого й ефективного плану реагування на інциденти, що дозволить швидко ідентифікувати, аналізувати та реагувати на кіберзагрози, мінімізуючи потенційну шкоду та відновлюючи нормальну роботу систем [42].

Дослідження свідчать про те, що критичні інциденти безпеки практично неминучі завдяки злочинній винахідливості з боку порушника та помилкам з боку користувача. Реактивна, неорганізована відповідь на атаку дає перевагу зловмисникам і наражає бізнес на більший ризик. У гіршому випадку, фінансова, операційна й репутаційна шкода від інциденту може змусити організацію припинити діяльність. З іншого боку, злагоджена, добре перевірена стратегія реагування на інциденти, яка відповідає кращим практикам кібербезпеки, обмежує негативні наслідки і створює передумови для швидшого відновлення бізнесу.

Основу ефективної обробки подій безпеки є план реагування на інциденти - стандартний набір документів організації, у якому детально описано:

- які загрози, експлойти та ситуації кваліфікуються як інциденти безпеки, що викликають покарання, і що робити, коли вони трапляються.
- хто відповідає за обробку інциденту, які завдання виконує і як інші можуть з ними зв’язатися у разі інциденту безпеки;

- коли, за яких обставин і як члени команди мають виконувати встановлені завдання з реагування на інциденти безпеки [43].

План реагування на інциденти діє як детальна, авторитетна карта, яка спрямовує респондентів від початкового виявлення, оцінки й сортування інциденту до його стримування та вирішення.

Успішне реагування на інцидент вимагає завчасного складання, перевірки й тестування планів до того, як виникне критична ситуація. Загалом, план реагування на інцидент має включати такі компоненти:

- Огляд плану.
- Перелік ролей і обов'язків.
- Список інцидентів, які вимагають вжиття заходів.
- Поточний стан мережевої інфраструктури та засобів контролю безпеки.
- Процедури виявлення, розслідування та стримування.
- Ерадикаційні процедури (викорінення першопричин інцидентів).
- Відновлювальні процедури.
- Процес повідомлення про порушення.
- Список подальших завдань після інциденту.
- Список контактів.
- Тестування плану реагування на інцидент.
- Поточні перегляди.

Найгіршим часом для виявлення неточностей у плані реагування на інциденти – це реальна критична ситуація безпеки. Експерти радять організаціям проводити регулярні симуляції з різноманітними векторами атак, такими як програми-вимагачі, фішинг, зловмисні інсайдери й атаки типу брутфорс.

Багато підприємств проводять навчання реагування на інциденти, щоб перевірити свої плани. Настільна вправа, заснована на обговоренні, передбачає обговорення особливостей нападу й реакції команди. Оперативні настільні вправи включають практичні завдання з відтворенням відповідних процесів, щоб побачити, як вони розгортаються. Такі шаблони можуть допомогти спланувати

ефективне моделювання.

Після змодельованих і реальних інцидентів безпеки групи реагування повинні вивчити те, що сталося, і переглянути отримані уроки. Варто звернути увагу на будь-які прогалини в безпеці, які виникли, визначити відповідні додаткові засоби, шляхи вдосконалення процесів і, відповідно, оновлення плану реагування на інциденти. Варто пам'ятати, що план реагування на інциденти – це не рішення «встановити й забути». Він має постійно розвиватися, щоб відображати зміни в ландшафті загроз, IT-інфраструктурі й бізнес-середовищі. Експерти рекомендують принаймні щорічно проводити офіційну комплексну повторну оцінку та перегляд корпоративного плану реагування на інциденти [44].

Для того, щоб полегшити процес розробки плану реагування на інциденти, доцільно звернутися до вже розроблених підходів до реагування на інциденти від відомих міжнародних експертних організацій, таких як NIST, ISO та ISACA незважаючи на те, що кожна із зазначених організацій пропонує свою концепцію відповіді на інциденти, вони відрізняються незначно і визначають схожі етапи реагування (Рис. 2.4):

Рис. 2.4. Етапи реагування на інциденти кібербезпеки

- Підготовка/планування. Створення групи реагування на інциденти та відповідних політик, процеси та посібники; розгортання інструментів та служб для підтримки реагування на інциденти.
- Виявлення/ідентифікація. Використання IT-моніторингу для виявлення,

оцінки, перевірки та сортування інцидентів безпеки.

- Стримування. Вживання заходів, щоб зупинити погіршення інциденту й відновити контроль над IT-ресурсами.
- Ерадикація. Усунення загрозливої діяльності, включаючи зловмисне програмне забезпечення і шкідливі облікові записи користувачів; визначити будь-які вразливості, якими скористалися зловмисники.
- Відновлення. Повернення до нормальної роботи і усунення/пом’якшення відповідних вразливостей.
- Врахування помилок на основі попереднього досвіду. Аналіз інциденту для визначення сутності, часу і методів реалізації події, визначення елементів управління безпекою, політик і процедур, які функціонували неоптимально, і вибір шляхів їх покращення, на основі чого здійснюється оновлення плану реагування на інциденти [45].

За кожною успішною програмою реагування на інциденти стоїть скоординована, ефективна й ефективна команда реагування на інциденти. Зрештою, політики безпеки, процеси та інструменти мало що значать без кваліфікованих фахівців, які їх підтримують і втілюють у життя. Ця міжфункціональна група складається з людей з різних підрозділів організації, які відповідають за виконання етапів і процесів, пов’язаних із реагуванням на інциденти. Нижче наведено найпоширеніші типи груп реагування на інциденти:

- Група реагування на інциденти комп’ютерної безпеки (CSIRT).
- Група реагування на комп'ютерні інциденти (CIRT).
- Група реагування на комп’ютерні надзвичайні події (CERT).

Ці абревіатури часто використовуються як синоніми на місцях, і команди нерідко мають однакові цілі й обов’язки. Важливим зауваженням є те, що назва CERT є зареєстрованою торговою маркою Університету Карнегі-Меллона, тому компанії повинні подати заявку на дозвіл на її використання [46].

Інший термін, який часто використовують для позначення групи реагування на інциденти, – це центр операційної безпеки (SOC). SOC охоплює людей, інструменти і процеси, які управляють програмою безпеки організації. Хоча групи

SOC можуть відповідати за реагування на інциденти, це не є їх єдиним завданням в організації. Інші обов'язки команд SOC включають виявлення й управління активами, ведення журналів діяльності і дотримання нормативних вимог.

Головними цілями групи реагування на інциденти є виявлення й реагування на події безпеки та мінімізація їх впливу на бізнес. Таким чином, обов'язки команди в основному узгоджуються з етапами, окресленими в структурі та плані реагування на інциденти. Командні завдання охоплюють [47]:

- Підтримка готовності до інцидентів безпеки та їх запобігання.
- Розробка плану реагування на інцидент.
- Тестування, оновлення й управління планом реагування на інцидент перед використанням.
- Виконання настільних вправ реагування на інциденти.
- Розробка показників для аналізу програмних ініціатив.
- Визначення і класифікація подій безпеки.
- Усунення загроз, виявлення основних причин і видалення уражених систем з робочих середовищ.
- Відновлення після інцидентів і відновлення уражених систем.
- Проведення подальших заходів, включаючи документування, аналіз інцидентів і визначення способів запобігання подібним подіям і покращення майбутніх заходів реагування.
- Регулярний перегляд та оновлення плану реагування на інциденти [47].

Для більш структурованого й автоматизованого управління і реагування на інциденти використовують такий інструмент як SOAR (Security, Orchestration, Automation and Response). SOAR є одним із найновіших інструментів для реагування на інциденти. Його можливості схожі на можливості SIEM, що створює певну плутанину. Оркестрація безпеки, автоматизація й реагування – це набір технологій, які в поєднанні допомагають групам безпеки збирати, аналізувати, виявляти події безпеки та реагувати на події безпеки з невеликою або взагалі без участі людини.

Нижче наведено основні функції кожного компонента SOAR:

- Оркестрація безпеки. Ця функція з’єднує та інтегрує внутрішні й зовнішні інструменти за допомогою вбудованих або спеціальних інтеграцій та API, збирає та консолідує дані, агреговані різними інструментами, щоб ініціювати функції реагування на основі визначених параметрів і процесів аналізу інцидентів.

- Автоматизація безпеки. Ця функція використовує дані, зібрані під час оркестровки безпеки, для запуску робочих процесів і завдань на основі визначених порогових значень і дій, викладених у посібниках реагування на інциденти. Платформи SOAR можуть автоматично виправляти вразливості з меншим ризиком і виконувати завдання низького рівня, які раніше виконували аналітики, наприклад сканування вразливостей. Загрози високого ризику також можуть автоматично передаватися аналітикам безпеки для подальшого розслідування.

- Реагування. За допомогою єдиного представлення ця функція дозволяє фахівцям із безпеки, мережевим і системним аналітикам отримувати доступ до інформації про загрози та обмінюватися нею, співпрацювати й виконувати заходи реагування на інциденти [48].

Операції систем SIEM подібні до платформ SOAR, але їм не вистачає ключової функції: автоматизованої реакції. SIEM просто сповіщають команди про можливі інциденти; вони не запускають автоматичні дії. SIEM і SOAR мають подібний середній час виявлення, але SOAR перевершує середній час відповіді завдяки своїм автоматизованим можливостям.

Платформи SOAR доповнюють аналітиків такими можливостями:

- Координація розвідки загроз.
- Ведення справ.
- Управління вразливостями.
- Автоматизоване збагачення для ремедіації.
- Пошук загроз.
- Автоматизація реагування на інциденти.

У цих випадках використання платформ SOAR може допомогти підвищити продуктивність; автоматизувати повторювані, нудні й менш важливі завдання; використовувати наявні інструменти безпеки краще й більш контекстно;

покращити інтеграцію сторонніх інструментів. Однак платформи SOAR не позбавлені недоліків. Зокрема, SOAR можуть бути не в змозі легко або взагалі інтегруватися з усіма інструментами безпеки, не відповідають культурі безпеки в організації та можуть не відповідати завищеним очікуванням користувачів.

Відновлення після інцидентів

Превентивні методи кібербезпеки - це підходи та заходи, спрямовані на запобігання кібератакам або іншим інцидентам кібербезпеки, перш ніж вони стануться. Вони включають широкий спектр технічних і адміністративних засобів, таких як шифрування даних, фаєрволи, антивірусне програмне забезпечення, політики безпеки та навчання персоналу. Ці методи мають на меті зменшити вразливість систем і мереж до потенційних загроз і забезпечити, щоб організація була краще підготовлена до виявлення, протистояння і мінімізації наслідків небажаних подій.

Детективні засоби управління є ключовим компонентом програми кібербезпеки, що забезпечує видимість зловмисної діяльності, порушень і атак на IT-середовище організації. Ці засоби охоплюють реєстрацію подій і пов’язаний моніторинг і сповіщення, які сприяють ефективному управлінню IT. Під час аудиту програми кібербезпеки аудитори повинні визначити й оцінити ці критичні засоби управління.

Детективні методи допомагають виявити атаки, яким не вдалося запобігти з використанням превентивних заходів, та є важливою частиною комплексної стратегії кібербезпеки. Якщо спеціальні засоби виявлення кібербезпеки належним чином спроектовані й ефективно функціонують, то вони можуть зупинити кіберзагрози. Ці елементи управління зазвичай виконуються або контролюються центром операційної безпеки (SOC), який відповідає за моніторинг кібербезпеки [36].

Реагування на інциденти та відновлення в контексті кібербезпеки – це критично важливі елементи захисту інформаційних систем від загроз та атак. У сучасному світі, де організації постійно зіштовхуються з різноманітними та

складними кіберзагрозами, ефективне реагування на інциденти і здатність до швидкого відновлення є ключовими для забезпечення безперервності бізнесу та захисту чутливих даних.

Цей процес включає не тільки технічні аспекти, такі як ідентифікація та усунення загроз, але й організаційні заходи, зокрема планування, підготовку персоналу й розробку політик відновлення. Ключовим моментом є створення чіткого й ефективного плану реагування на інциденти, що дозволить швидко ідентифікувати, аналізувати та реагувати на кіберзагрози, мінімізуючи потенційну шкоду та відновлюючи нормальну роботу систем [42].

Процес відновлення після інциденту спрямований на повернення бізнесу до нормальної діяльності після реалізації інциденту, пов’язаного з кібербезпекою. Головна його мета - це мінімізувати збитки, швидко відновити повноцінну роботу й запобігти майбутнім порушенням. Фахівці з кібербезпеки рекомендують організаціям дотримуватися таких практик в разі реалізованої кібератаки на бізнес:

- Дотримання плану реагування на інциденти: грамотно спроектований план реагування зробить процес відновлення менш виснажливим, чітко розподіляючи обов'язки між групами й окремими особами.

- Розпізнання та зупинка атаки: для цього потрібно визнати наявність атаки, а потім спробувати стримати її, щоб зменшити збитки. Це можна зробити, вимкнувши доступ зловмисників, ізолюючи системи, які були скомпрометовані. У разі внутрішнього витоку необхідно скасувати доступи облікового запису користувача, який був використаний зловмисником.

- Ефективна комунікація: важливо переконатися, що про кібератаку повідомляють правильну інформацію. Тому дуже важливо мати офіційні протоколи зв’язку після атаки заздалегідь. Варто переконатися, що внутрішня комунікація між відділами здійснюється через ефективні канали, які забезпечують належний обмін інформацією.

- Оцінка збитків: потрібно оперативно оцінити, що було втрачено або пошкоджено, щоб визначити подальші дії. Для здійснення процесу відновлення необхідно створити спеціальну групу й виконати таку послідовність дій: збір

фактів, які допоможуть розробити ефективні процеси відновлення; документування того, як відбулася атака, як вона вплине на клієнтів, які активи постраждали, хто є жертвами та який це тип атаки.

- Усунення пошкоджень і відновлення активів: відновлення активів, які були скомпрометовані, шляхом заміни або очищення дисків зберігання даних уражених ІТ-активів, а також завантаження будь-яких втрачених даних із джерел резервного копіювання. Активація всіх хмарних реплік мережевого середовища є ще одним варіантом, який допоможе продовжити бізнес-операції у ході розслідування атаки.
- Перегляд етичних зобов'язань бізнесу: необхідно бути відкритим і чесним з працівниками та клієнтами щодо атаки та її причин, навести аргументи на користь того, що компанія переглянула свої плани й посилила усі поточні протоколи кібербезпеки [49].

Висновки до розділу 2

У другому розділі було розглянуто превентивні й детективні методи кібербезпеки. Встановлено, що превентивні методи кібербезпеки охоплюють широкий спектр технічних і адміністративних засобів, таких як шифрування даних, фаєрволи, антивірусне ПЗ, політики безпеки й навчання персоналу, які мають на меті зменшити вразливість систем і мереж до потенційних загроз і забезпечити належну підготовку організації до виявлення, протистояння і мінімізації наслідків небажаних подій.

Детективні засоби управління забезпечують видимість зловмисної діяльності, порушень і атак на ІТ-середовище організації і охоплюють реєстрацію подій, моніторинг і сповіщення, які сприяють ефективному управлінню ІТ. Детективні методи допомагають виявити атаки, яким не вдалося запобігти з використанням превентивних заходів.

У ході дослідження проаналізовані потенційні стратегії бізнесу для реагування на інциденти кібербезпеки та подальше відновлення після таких інцидентів, що дозволяє скласти картину для подальшого аналізу стратегій кіберстійкості бізнесу. Окрема увага приділена розробці гнучких стратегій реагування на інциденти, які враховують специфіку бізнесу та можливі сценарії кібератак. Особлива увага приділяється розумінню різних аспектів кібербезпеки та їх взаємозв'язку, підкреслюючи важливість багаторівневого підходу, який включає як запобігання інцидентам, так і гнучке реагування на них. Цей підхід сприяє не тільки ефективному реагуванню на поточні загрози, але й адаптації до нових викликів у швидкозмінному цифровому світі.

РОЗДІЛ 3
СТРАТЕГІЇ КІБЕРСТІЙКОСТІ БІЗНЕСУ: ЗАСАДИ РОЗРОБКИ, ВПРОВАДЖЕННЯ Й ОЦІНЮВАННЯ ЕФЕКТИВНОСТІ

3.1 Розробка та імплементація стратегій кіберстійкості

Стратегія кіберстійкості - це ретельно розроблена архітектура, яка дає бізнесу можливість захищатися від кібератак, виявляти, реагувати і відновлюватися після них. Стратегія кіберстійкості побудована на ідеї, що незалежно від того, наскільки добре захищена компанія, атака відбудеться.

Стійкість кібербезпеки залежить від багатьох оперативних заходів, таких як безперервність бізнесу, аварійне відновлення, реагування на інциденти і плани кібербезпеки.

Головна мета стійких організацій - зменшити вплив успішної кібератаки та продовжувати ефективну роботу. Досягти цього можна завдяки забезпеченню продуктивного взаємозв’язку між інструментами кібербезпеки, налагодженню їх сумісного функціонування й доповнення один одного.

Організація, яка є кіберстійкою, може адаптуватися до відомих і невідомих криз, небезпек, складних ситуацій і перешкод [50].

Кіберстійкість допоможе бізнесу не лише у сфері безпеки, але й стане почесним плюсом, який визнають клієнти й ділові партнери компанії. Швидка адаптація до безкінечних змін, які тепер є новою нормою, допоможе організації у довгостроковій перспективі забезпечити стабільність і зберегти існування.

Стратегія кіберстійкості допоможе організації:

- Покращити фінансове становище: шляхом зменшення ризиків, організація зменшує фінансові втрати. Слід пам’ятати, що більшість кібератак спрямовані на викрадення грошей жертви. Крім того, чим довше процедури та системи компанії не працюють через інцидент, тим більше грошей вона втрачає.

За даними Cybersecurity Ventures, до 2025 року кіберзлочинність коштуватиме компаніям у всьому світі 10,5 трильйонів доларів на рік.

- Завоювати довіру: відповідність міжнародним стандартам кібербезпеки (наприклад, стандарту з управління інформаційною безпекою ISO/IEC 27001, стандарту безпеки даних індустрії платіжних карток PCI-DSS) забезпечить довіру до організації з боку персоналу, партнерів, клієнтів, постачальників тощо.
- Бути конкурентоспроможними: демонструючи кіберстійкість, компанія демонструє відданість, добре продуманий бізнес-план, цілісне бачення забезпечення стійкості до кіберзагроз. Усе це дасть надає конкурентну перевагу перед компаніями, які не можуть гарантувати таких умов.
- Створити власний бренд: не варто недооцінювати силу бренду й репутацію. Витік даних може заплямувати роки успішної роботи, зробивши організацію ізгоєм серед інших представників бізнесу або навіть позбавивши її можливості відновитися повністю після серйозної хакерської атаки [51].

Сильна стратегія кіберстійкості забезпечує досягнення таких цілей:

- Протидія загрозам – завчасне виявлення та пом’якшення кіберзагроз, перш ніж вони зможуть використати вразливі місця у системі організації.
- Розробка плану реагування на інциденти – формування чіткої послідовності дій швидкого й ефективного виявлення, стримування та управління кіберінцидентами.
- Забезпечення безперервності роботи – впровадження вчасних і ефективних заходів резервного копіювання і відновлення, щоб підтримувати безперервну роботу навіть у разі кібератаки.
- Зміцнення довіри зацікавлених сторін – демонстрація непохитної відданості кібербезпеці та стійкості з боку компанії, щоб вселити довіру і впевненість у клієнтів, партнерів і зацікавлених сторін.
- Відповідність нормативним вимогам. Корпоративна стратегія кібербезпеки має сприяти дотриманню галузевих правил і стандартів, захисту конфіденційних даних зацікавлених сторін і запобігання юридичним і фінансовим наслідкам [52].

Отже для створення кіберстійкого бізнес-середовища організація має дотримуватися таких важливих вимог:

1. Забезпечити постійний нагляд за станом кібербезпеки в організації.

Ландшафт загроз постійно змінюється, і організації прагнуть встигати за ними в умовах обмежених бюджетів і ресурсів, вдаючись до трудомісткого ручного експорту даних до багатьох електронних таблиць і постійно переслідуючи загрози, а не передбачаючи потенційні атаки чи компрометації. Це призводить до нецілеспрямованого прийняття рішень і неадекватного стратегічного планування на кожному рівні організації. Для вирішення цієї невідповідності NIST радить командам розробляти і впроваджувати політику та процедури кібербезпеки.

Тим не менш, командам з кібербезпеки потрібні нові підходи, щоб проактивно розглядати поточні та нові кіберризики й управляти ними. Вони повинні більш повно розуміти, де розставляти пріоритети своїх зусиль, як об’єктивно вимірювати прогрес у часі та коли ефективно повідомляти результати зацікавленим сторонам, щоб пом’якшити атаки та значно зменшити кількість інцидентів, на які їм потрібно швидко реагувати.

Запобігання кібератакам означає не лише впровадження рекомендацій NIST щодо навчання й підвищення обізнаності працівників з кібербезпеки, а також впровадження систем контролю доступу та моніторингу. Це також вимагає повної видимості активів і ризиків, широкого контексту потенційних загроз безпеці та чітких показників для об’єктивного вимірювання кіберризиків.

Організації, які можуть передбачати кібератаки й повідомляти про ці ризики для підтримки прийняття рішень, матимуть найкраще становище для захисту від нових загроз. Сьогодні, коли дані є особливо складними і динамічними, а конфіденційні дані швидко зростають і поширюються, організаціям необхідно знати їх місцезнаходження, класифікацію, спосіб доступу до них та інші фактори, щоб зрозуміти потенційні ризики і потреби в захисті.

Найуспішніші плани кібервідмовостійкості починаються з оцінювання. Командам потрібно не лише переглянути сильні та слабкі сторони, можливості й

загрози в кіберпросторі, але й визначити рішення, необхідні для побудови кіберзахисту й ефективного реагування на кібератаки. Передовий досвід у галузі аналізу загроз у поєднанні з досвідом інтелектуальної безпеки даних і рішень для управління даними, що працюють локально та у хмарі, допомагають організаціям розробляти ефективніші програми кіберготовності [54].

2. Дотримуватися принципу нульової довіри: ніколи не довіряй, завжди перевіряй:

Застаріла модель безпеки, зосереджена на ідеї “довіряти, але перевіряти”, більше не діє в сучасному бізнесі й урядовому середовищі, оскільки периметрів більше не існує. Найкращі практики для цифрового бізнесу вимагають створення архітектури за принципами нульової довіри, та найменших привілеїв, щоб знати, хто і коли має доступ до якої інформації.

Скомпрометована конфіденційна інформація завдає шкоди діловій репутації, може призвести до втрати конкурентних переваг, а також зменшення гнучкості й обізнаності про ситуацію. Ось чому зараз надзвичайно важливо захистити кожну особу і систему на найширшому діапазоні пристроїв і середовищ.

Цифрова ідентифікація - це сукупність інформації про особу, організацію чи електронний пристрій, яка існує в Інтернеті. З такою кількістю підприємств, які переживають цифрову трансформацію, з’явився сплеск ідентифікаційних даних із безпрецедентним доступом до них. Сьогодні кількість ідентифікаторів із привілейованим доступом та управлінням на кількох пристроях значно перевищує кількість користувачів, що покладає на команду безпеки обов’язок краще захистити ширшу поверхню атак.

Крім того, використання багатьох застарілих інструментів для управління безпекою ідентифікаційної інформації особи створює передумови для труднощів і неефективності, якими можуть скористатися хакери. Комплексне управління доступом на основі ролей у поєднанні з правилами «ніколи не довіряти, а завжди перевіряти» краще захищає організацію від програм-вимагачів і внутрішніх загроз.

Оскільки дані зараз є скрізь, організація повинна знайти спосіб комплексної уніфікації управління даними і їх безпекою: від кінцевих точок до хмарних робочих навантажень, від резервного копіювання до виробництва і від ідентифікації до власне даних, щоб зупинити зловмисників. Підхід до запобігання атакам, який орієнтується на першочергові дані, доповнює рекомендації NIST щодо впровадження шифрування та інших заходів безпеки для захисту даних, вимагає видимості й контролю всіх корпоративних і особистих даних. Завдяки повній видимості організація зможе мінімізувати ризики даних у всіх своїх хмарних і локальних системах для безпеки даних, конфіденційності, їх відповідності й управління [55].

3. Мати детальну інформацію про корпоративні дані й архітектуру:

NIST рекомендує регулярно тестувати й оновлювати плани реагування на інциденти, а також проводити регулярні оцінки вразливостей і тестування на проникнення. Це дуже важливо, оскільки швидке виявлення зловмисного ПЗ допомагає компанії набути впевненості й уникнути виплати викупу.

Окрім цих вказівок для виробничих систем, організація може виявити кіберзагрози і сліпі зони у своєму виробничому середовищі, запустивши автоматичне сканування, створивши резервні копії відомих уразливостей. Ці сканування також спрощують оцінку корпоративних ризиків та відповідають суворим вимогам безпеки та відповідності, не впливаючи на виробниче середовище.

Сканування робочих і резервних середовищ забезпечує оцінювання їх стан і можливість відновлення. Завдяки ретельній перевірці резервних копій організація може переконатися, що жодна відома вразливість не буде повторно введена у робоче середовище під час відновлення. Усе це надає глибшу інформацію і комплексне уявлення про всі кіберзагрози у виробничому середовищі, щоб організація могла їх усунути, перш ніж ними скористається зловмисник.

Класифікація даних на основі штучного інтелекту та машинного навчання (Artifical Intelligence/Machine Learning, AI/ML) також прискорює захист,

виявлення й реагування на програми-вимагачі, тримаючи бізнес на крок попереду кіберзлочинців. Організація може постійно знаходити конфіденційні та регламентовані дані, зокрема персональні дані (Personally Identifiable Information, PII), захищену інформацію про здоров'я (Protected Health Information, PHI) і дані споживача (Protected Consumer Information, PCI), а також зменшувати помилкові спрацьовування за допомогою класифікації даних на основі ML.

Ця аналітична інформація допомагає інформувати про стан безпеки і підтримувати залежні елементи управління безпекою, такі як запобігання втраті даних (DLP), в актуальному стані, а також дозволяє групам реагування зрозуміти вплив атаки програм-вимагачів або кіберінциденту на стан безпеки і бізнес.

4. Стимулювати співпрацю: зробити кіберстійкість командним видом спорту.

Стійкість вимагає підготовки, чутливості, стійкості та адаптивності. У сучасному світі комунікацій лідери безпеки повинні використовувати архітектуру та процеси, які включають локальні, хмарні та SaaS середовища, одночасно впроваджуючи процеси безпеки, зосереджені на безперервності бізнесу. Програми SecOps повинні використовувати превентивні рішення та процеси, щоб зупинити дії противника, коли це можливо, але також виявляти й реагувати, коли запобігти порушенням безпеки неможливо.

Стійкість досягається шляхом зупинки супротивників до того, як вони досягнуть своїх цілей у цільовому середовищі. Організації повинні чітко розуміти свій індивідуальний ландшафт загроз і вектори атак, щоб підтримувати зусилля щодо стійкості. Це досягається завдяки поглибленому аналізу загроз і поверхонь атак, який, тим не менше, має бути не узагальненим, а індивідуальним для кожної організації. Нарешті, процеси, які підтримують стійкість бізнесу, є критично важливим результатом програми безпеки. Планування реагування на інциденти і партнерство є ключовими для підтримки як бізнесу, так і корпоративної програми безпеки.

NIST рекомендує налагодити партнерство і співпрацю з іншими організаціями для обміну інформацією про загрози та найкращими практиками.

Якщо організація адаптує свої процеси, щоб спиратися на співпрацю IT/SecOps, то матиме більше шансів захистити корпоративні дані від зловмисників.

Керівники компанії мають знайти, обрати й інвестувати в надійні продукти безпеки, які бездоганно працюють разом для боротьби з шкідливим ПЗ. Сюди входять рішення для управління інформацією та подіями безпеки (SIEM) і рішення для оркестрування безпеки, автоматизації та реагування (SOAR), які прискорюють час виявлення, дослідження й усунення атак.

Попередньо створені інтегровані робочі процеси, які можна розширити, дозволяють SecOps доповнювати їх для автоматизованого реагування на інциденти й уніфікованих операцій у групах безпеки, IT та мереж. Крім того, слід переконатися, що готові інтеграції можливі за допомогою безпечного набору програмного забезпечення (SDK) і налаштованих API управління, які забезпечують гнучкість в управлінні корпоративним середовищем для протидії кіберзлочинності.

5. Консолідувати і спростити: використовувати сучасну платформу безпеки й управління даними

Масштаб і сумісність є додатковими ключами до боротьби з кібератаками. Оскільки кібервідмовостійкість вимагає співпраці, важливо скористатися перевагами розширюваної сучасної платформи захисту даних і управління даними з архітектурою, багатою на API, яка працює в різних місцях і охоплює найширший спектр джерел даних.

Консолідуючи багато функцій управління даними на одній платформі, організація може спростити операції. Замість того, щоб робити копії даних і переміщувати їх, можна використати рішення, яке дозволяє повторно використовувати дані на місці, додаючи цінні програми до даних для рутинних і складніших завдань: від сканування вірусів і маскування даних до аналізу журналів аудиту файлів і класифікації даних. Крім того, єдина розширювана платформа скорочує обсяг корпоративних даних і поверхню, доступну для кібератак.

6. Збільшити швидкість і впевненість: інтегрувати інфраструктуру

резервного копіювання з інфраструктурою безпеки та операцій

Проблеми з безпекою й управлінням даними не можна вирішити поодинці, особливо коли відбувається злом. Щоб якнайшвидше повернутися до робочої готовності протягом часу відновлення та цільових точок відновлення (RTO/RPO) потрібен інтегрований підхід, у якому резервне копіювання є не відокремленим, а невід'ємною частиною інфраструктури безпеки і операцій.

Організації, які інвестують у безпеку й управління даними, отримають вигоду від тісно інтегрованих рішень, які охоплюють увесь спектр інфраструктур безпеки. Популярним є цикл реагування на інциденти, або PICERL, від Інституту SANS, який включає такі етапи:

- Підготовка – оцінювання, плани, освіченість, управління ідентифікацією тощо.
- Ідентифікація – моніторинг обізнаності, раннє виявлення тощо.
- Стримування – сповіщення, резервне копіювання, криміналістика тощо.
- Викорінення – відновлення, аналіз першопричин, видалення зловмисного програмного забезпечення тощо.
- Відновлення – сканування вразливостей, повернення до роботи базового рівня тощо.
- Робота над помилками – звітування, аналіз, оновлення процедур тощо.

Ретельно продумана інтеграція дає корпоративній команді безпеки швидкість і впевненість у протидії атакам на всьому шляху від планування до відновлення, навіть за допомогою автоматизованого штучного інтелекту/ML для виявлення потенційних кібератак, сповіщаючи команди про незвичні моделі навколо даних компанії. У разі злому організація має спосіб у будь-який момент часу та в будь-якому місці відновити чисті дані, які були просканові на наявність уразливостей, щоб уникнути повторного зараження системи, скорочуючи час простою [56].

3.2 Оцінка ефективності стратегій кіберстійкості

Оцінка ефективності стратегій кіберстійкості є процесом, який дозволяє організаціям аналізувати й оцінювати ефективність їхніх стратегій кібербезпеки. Цей процес включає в себе розгляд того, наскільки добре ці стратегії забезпечують захист від кібератак, а також їхню здатність швидко відновлюватися після інцидентів і адаптуватися до нових загроз.

Важливість оцінки ефективності кіберстійкості полягає в тому, що вона допомагає організаціям забезпечити адекватний рівень безпеки. Через швидкий розвиток технологій і постійну зміну кіберзагроз, організації повинні регулярно переглядати й оновлювати свої стратегії кібербезпеки. Оцінка дозволяє ідентифікувати слабкі місця та зони, де можливе покращення, а також сприяє розумінню, які елементи стратегії є найбільш ефективними.

Крім того, оцінка ефективності допомагає визначити рентабельність інвестицій у кібербезпеку, дозволяючи керівництву компанії прийняти обґрунтовані рішення щодо розподілу ресурсів. Це також сприяє розвитку більш гнучких і адаптивних стратегій, які можуть швидко реагувати на зміни в кіберзагрозах і технологіях.

У підсумку, оцінка ефективності є ключовим елементом управління кібербезпекою, оскільки вона надає цінну інформацію, необхідну для забезпечення надійності та стійкості організації в цифровому світі [57].

Основними аспектами оцінювання стратегій кіберстійкості є:

1. Мета оцінювання ефективності стратегії кіберстійкості. Основна мета оцінки кіберстійкості полягає у здійсненні порівняльного аналізу між поточною або запланованою системою та ідеальним станом кіберстійкості. Цей процес передбачає вивчення різних аспектів системи, включаючи її здатність витримувати й відновлюватися після кібератак, а також її готовність адаптуватися до нових загроз та викликів.

Для досягнення цієї мети спочатку визначають специфічні метрики

кіберстійкості, які можуть включати показники надійності, відновлення й адаптивності системи. Ці метрики потім використовуються для оцінки поточного стану системи, дозволяючи виявити слабкі місця та зони для поліпшення.

Під час оцінки кіберстійкості особливу увагу приділяється тому, наскільки добре система може відповідати на різні виклики й загрози у сфері кібербезпеки. Це охоплює не лише здатність системи витримувати атаки, але й її готовність швидко відновлюватися й адаптуватися до змін у середовищі загроз. Оцінюючи поточну або заплановану систему у порівнянні з ідеалом, визначаються напрямки, де система може бути покращена або де потрібно впровадити нові заходи кіберзахисту. Такий підхід допомагає організаціям не лише забезпечити поточну безпеку своїх систем, але й планувати майбутнє, розробляючи більш стійкі й адаптивні рішення з кібербезпеки.

2. Аналіз показників ефективності (MOEs) для альтернативних рішень кіберстійкості. У цьому контексті, основна увага приділяється визначенню й оцінюванню, наскільки добре різні комбінації архітектурних рішень, технологій та оперативних процесів допомагають досягти цілей кіберстійкості. Це включає вимірювання змін у показниках ефективності або продуктивності, які можуть бути пов'язані з діяльністю противника або іншими факторами ризику.

Цей процес важливий, оскільки він дозволяє оцінити реальний вплив різних стратегій і рішень на загальну кібербезпеку системи. Завдяки цьому можна виявити, які елементи стратегії найбільш ефективні, а які потребують додаткового вдосконалення або зміни. Оцінюючи MOEs, організації можуть краще зрозуміти, які аспекти їхньої кіберстійкості є найбільш важливими та які ресурси слід вкладати для досягнення найкращих результатів.

Таким чином, цей аспект оцінки не тільки допомагає визначити ефективність поточних заходів безпеки, але й спрямовує рішення щодо майбутніх інвестицій у кібербезпеку, дозволяючи організаціям створювати більш стійкі й ефективні стратегії кіберстійкості.

3. Виклики, пов’язані з визначенням і оцінюванням метрик кіберстійкості. Ці виклики включають складність системи та її властивості емерджентності,

контекстуальність, а також практичність оцінювання метрик.

Складність системи відіграє значну роль, оскільки властивості кіберстійкості часто є емерджентними, тобто вони не можуть бути прямо виведені з властивостей окремих компонентів системи. Це створює труднощі у визначенні метрик, які повинні враховувати складні типи поведінки, такі як накопичення ефектів, каскадування та зворотні зв'язки. Такі типи поведінки притаманні для складних систем і потребують глибокого аналізу та розуміння.

Контекстуальність також є ключовою, оскільки кіберстійкість набуває значення в рамках конкретної місії, оперативних процесів і середовища загроз. Метрики кіберстійкості повинні бути визначені та оцінені з урахуванням цього контексту, що може варіюватися від загального до специфічного для кожної системи або місії.

Останній важливий виклик - це практичність оцінювання метрик. Щоб оцінка метрики була практичною, вона повинна бути чітко визначена і забезпечувати можливість повторення та відтворення. Оцінка конкретної метрики має свою вартість у термінах збору, обробки та зберігання інформації, необхідної для вироблення відповідної оцінки. Важливо, щоб необхідні дані були доступні, а оцінка метрики з цих даних була здійснена за прийнятною вартістю для зацікавлених сторін, які використовують цю метрику для прийняття рішень.

Таким чином, цей аспект оцінки вимагає детального розуміння складності систем, контексту, в якому вони функціонують, і практичності використання метрик для реального вимірювання стійкості системи до кіберзагроз.

4. Процес визначення метрик кіберстійкості. Цей процес включає визначення й інтерпретацію метрик, які повинні бути значущими і релевантними у контексті конкретних місій, бізнес-функцій та оперативного середовища системи. Це означає, що метрики повинні бути адаптовані й налаштовані з урахуванням унікальних вимог та особливостей кожної системи.

Процес визначення метрик кіберстійкості тісно пов'язаний з інженерним фреймворком кіберстійкості (CREF), який визначає цілі й завдання кіберстійкості, такі як передбачення, витривалість, відновлення та адаптація, а

також більш конкретні властивості, такі як міцність, готовність, продовження, обмеження збитків, реконституція, оперативна і технічна гнучкість.

Визначення метрик передбачає розробку підметрик або показників, які представляють ці цілі й завдання, а також відображають конкретні дії чи типи поведінки, які сприяють досягненню цих цілей. Важливість цього процесу полягає у створенні метрик, які точно відображають стійкість системи до кіберзагроз та її здатність адаптуватися до змін у середовищі загроз. Це включає не тільки технічні аспекти системи, але й її організаційні та оперативні аспекти.

Адаптація метрик до специфіки системи та її технічного середовища дозволяє отримати більш точну й релевантну оцінку кіберстійкості. Отже, цей аспект відіграє ключову роль у розробці комплексного підходу до оцінки кіберстійкості, забезпечуючи, що використовувані метрики точно відображають здатність системи протистояти кіберзагрозам в різних умовах і середовищах.

5. Адаптація метрик кіберстійкості до конкретних умов та вимог системи. Цей процес полягає в індивідуальному підході до вибору й інтерпретації метрик, враховуючи місії, бізнес-функції та оперативне середовище, в якому працює система. Особлива увага приділяється тому, як метрики пов'язані з основними принципами проектування кіберстійкості, методами й підходами, що використовуються в системі.

Цей аспект має велике значення, оскільки забезпечує, що вибрані метрики є релевантними та значущими для конкретної системи. Він враховує, що кожна система має свою унікальну архітектуру й технологічний набір, які впливають на її кіберстійкість. Наприклад, метрики для системи, яка обробляє конфіденційні дані, можуть відрізнятися від метрик для системи, що управляє фізичними пристроями на виробництві. Тому важливо, щоб метрики відображали специфіку системи, включаючи її архітектуру й технології.

Адаптація метрик також передбачає, що вони будуть відображати різні аспекти кіберстійкості, включаючи завдання, методи й підходи, які використовуються в системі. Це дозволяє визначити, наскільки добре система здатна виконувати свої функції в контексті потенційних кіберзагроз та атак.

Наприклад, метрика, яка вимірює час відновлення системи після кібератаки, може бути критично важливою для однієї системи, але менш значущою для іншої, в залежності від її ролі та використання. Врахування цього аспекту забезпечує, що оцінка кіберстійкості є точною, релевантною і корисною для прийняття обґрунтованих рішень щодо покращення захисту та стійкості системи в контексті її унікальних вимог та умов.

6. Методика оцінювання кіберстійкості. Для прикладу можна розглянути ситуативну методику оцінювання кіберстійкості (SSM-CR), яка надає відносні показники того, наскільки кіберстійкою є певна система, і визначає, наскільки різні альтернативи змінюють цей показник.

SSM-CR унікальна тим, що вона адаптована до контексту й відображає пріоритети зацікавлених сторін. Це означає, що оцінка проводиться з урахуванням специфічних цілей, завдань і можливостей, які є важливими для конкретної системи чи організації.

Другим аспектом є те, що оцінки продуктивності виконуються з урахуванням припущень щодо оперативного середовища і ландшафту загроз. Такий підхід дозволяє зробити оцінку більш точною та відповідною реальному стану речей.

Методика SSM-CR виробляє загальний рейтинг, індивідуальні оцінки для релевантних цілей та оцінки активностей нижчих рівнів або можливостей. Це дає можливість прослідкувати, як зміни у виконанні конкретних дій впливають на загальний рівень кіберстійкості системи. Важливо також відзначити, що модель загроз є невід'ємною частиною оцінки кіберстійкості, оскільки вона допомагає визначити потенційні ризики і вразливості.

Таким чином, SSM-CR є гнучким інструментом, який дозволяє оцінити кіберстійкість системи в контексті її специфічних умов і загроз, а також зробити порівняльний аналіз різних альтернативних рішень. Це допомагає керівництву компанії зрозуміти поточний рівень стійкості системи й визначити потенційні напрямки для покращення кібербезпеки.

7. Розробка програми метрик кіберстійкості.

На рисунку 3.1 представлено три основних етапи процесу визначення програми метрик кіберстійкості: вибір метрик, специфікація метрик та їх адаптація.

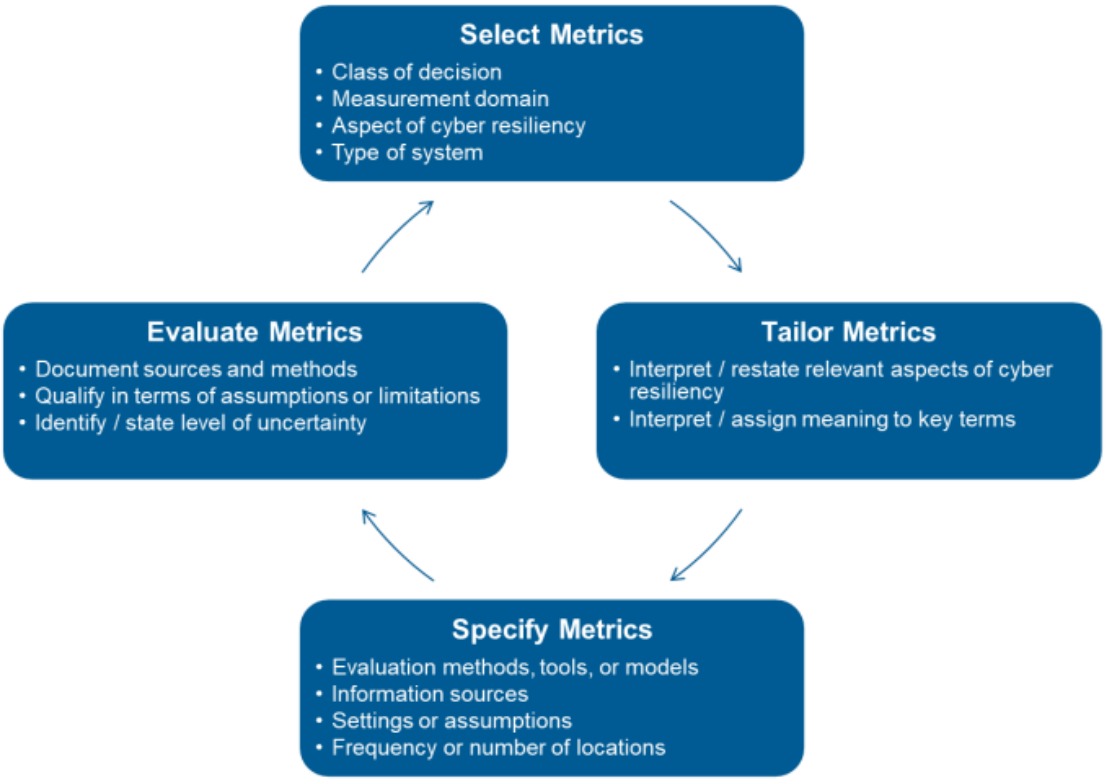

Рис. 3.1. Процес визначення програми метрик кіберстійкості

Цей процес включає в себе вибір відповідних метрик, їх адаптацію до конкретних умов та потреб системи, а також визначення способів їх оцінювання таким чином, щоб вони були повторювані та відтворювані.

Важливість цього аспекту полягає у забезпеченні того, щоб обрані метрики були релевантними і корисними для прийняття рішень у конкретному контексті. Це включає розгляд різних чинників, таких як клас рішень, які метрики призначені підтримувати (наприклад, інженерні проти інвестиційних рішень або програмні проти тактичних операцій), область вимірювання (наприклад, фізична, інформаційно-технічна, когнітивна або соціально-організаційна) і тип системи, що оцінюється.

Програма метрик кіберстійкості також охоплює визначення того, які аспекти кіберстійкості будуть оцінюватися, оцінку конкретних цілей, технік або підходів, які використовуються в системі. Вибір та пріоритезація потенційних

метрик залежать від відносної важливості цих різних чинників. Останнім елементом є процес специфікації метрик. Це включає в себе визначення параметрів метрик таким чином, щоб їх можна було точно оцінювати та відстежувати їх значення з часом або у відповідь на зміни в середовищі чи базових припущеннях. Специфікація метрик також допомагає зменшити потенціал неправильного трактування або неправильного представлення їх значень. Використання шаблону для фіксації специфікацій метрик може сприяти забезпеченню їх зрозумілості й коректності використання. Отже, розробка програми метрик кіберстійкості є ключовим елементом оцінки ефективності стратегії кіберстійкості, оскільки вона забезпечує систематичний і структурований підхід до вимірювання та відстеження кібербезпеки організації [58] .

3.3 Роль нормативно-правової бази у забезпеченні кіберстійкості на прикладі CRA

У сучасному цифровому світі, де кіберзагрози постійно еволюціонують і стають дедалі складнішими, роль нормативно-правової бази у забезпеченні кіберстійкості владних інститутів, організацій і громадян набуває особливої ваги.

Серед різноманітних законодавчих ініціатив варто насамперед відзначити Акт про кіберстійкість ЄС (Cyber Resilience Act, CRA) 2022 року, який регулює питання стандартизації та підвищення рівня стійкості до кіберзагроз у Європейському Союзі [59].

Європейська комісія розглядає прийняття цього важливого документа як важливий крок до зміцнення кібербезпеки та підвищення кіберстійкості в ЄС. Оскільки Україна вже є кандидатом у члени ЄС, на цей нормативний документ мають орієнтуватися й українські компанії, що готові втілювати серйозні підходи до забезпечення власної кіберстійкості.

CRA зосереджений на встановленні жорстких вимог до кібербезпеки для

виробників і дистриб'юторів цифрових продуктів, включаючи апаратне та програмне забезпечення, протягом усього їх життєвого циклу.

Ключовими аспектами забезпечення кіберстійкості CRA визначає:

- Кібербезпека за проектом і за замовчуванням – підкреслення важливості вбудовування стратегії кібербезпеки в продукти з самого моменту їх створення.
- Оцінка ризиків – проведення ретельної оцінки, щоб визначити потенційні ризики та вразливі місця кібербезпеки.
- Оновлення та виправлення – забезпечення своєчасних і регулярних оновлень і виправлень для усунення відомих вразливостей безпеки.
- Звітування про інциденти – обов’язкове звітування про інциденти кібербезпеки для кращого колективного захисту.
- Інформація про кібербезпеку для користувачів – надання користувачам необхідної інформації для підвищення їх обізнаності у сфері кібербезпеки [60].

Центральна роль у впровадженні CRA відведена Агентству ЄС з кібербезпеки ENISA, яке співпрацює з органами ринкового нагляду держав-членів ЄС. Останні забезпечують дотримання правил і мають право накладати штрафи за їх невиконання. У виняткових випадках Європейська комісія може втрутитися, щоб забезпечити дотримання правил і навіть обмежити або тимчасово вилучити невідповідну продукцію з ринку ЄС.

Вплив CRA є далекосяжним, він значно зміцнює кібербезпеку та стійкість до кіберзагроз на рівні ЄС, забезпечує посилення цифрового захисту інтересів споживачів і бізнесу, зменшення ризиків кібератак. Крім того, CRA сприяє покращенню ринку продуктів і послуг у сфері кібербезпеки, прокладаючи шлях до безпечнішого цифрового майбутнього.

На рисунку 3.2 показано практичне застосування Акту про кіберстійкість.

Отже, CRA розподіляє цифрові продукти на три категорії: звичайні, критичні класу I і класу II. Переважна більшість продуктів підпадає під звичайну категорію, яка становить 90% від їх загальної кількості і вимагає самооцінки від виробників.

Критичні продукти обох класів складають 10% і вимагають застосування

стандартів або оцінки третьою стороною. Для виробів класу I оцінка може бути здійснена як за стандартами, так і третьою стороною, тоді як для класу II - обов'язкова оцінка третьою стороною.

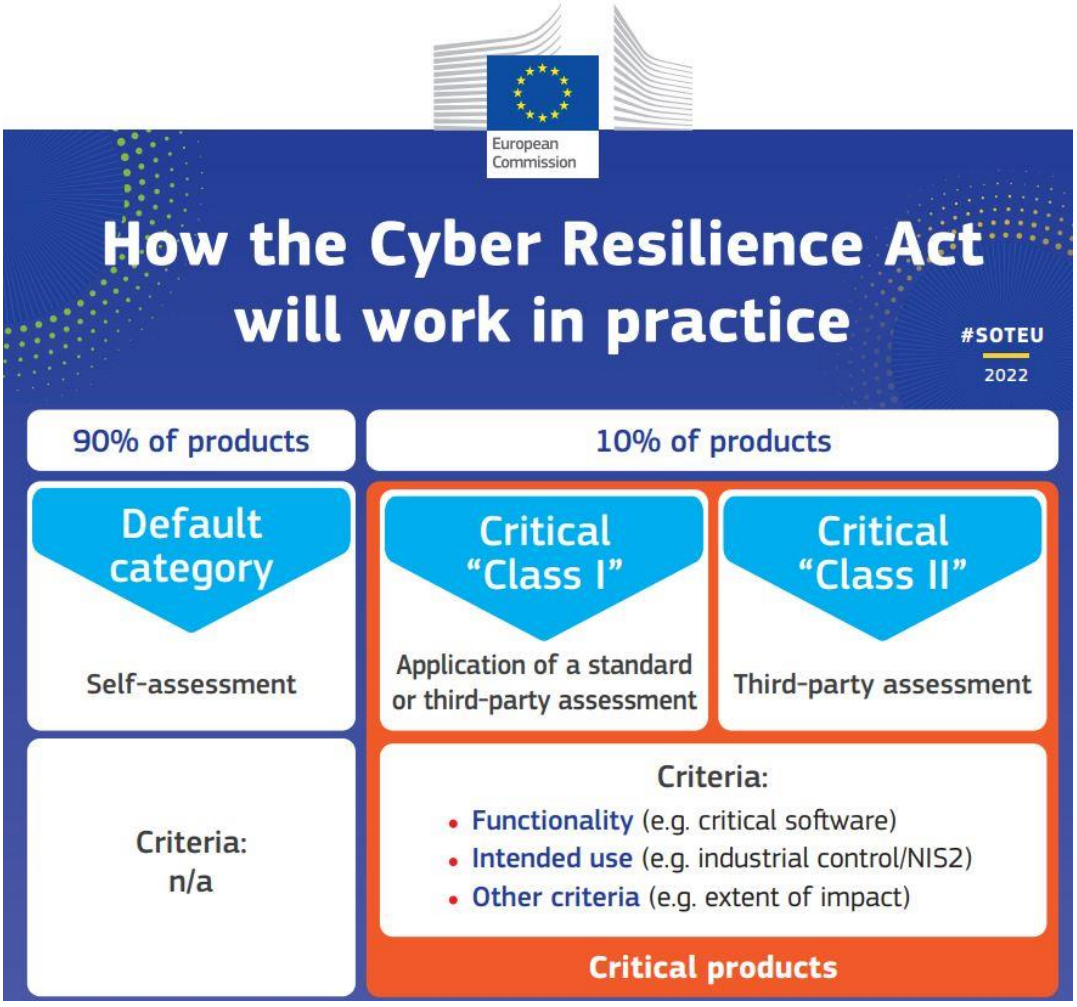

Рис. 3.2. Практичне застосування CRA

До критеріїв оцінювання критичних продуктів входять: функціональність (наприклад, критичне програмне забезпечення); передбачуване використання, як-от промислове управління чи директиви NIS2; ступінь впливу тощо.

Акт про кіберстійкість ЄС надає низку серйозних переваг для бізнесу, зокрема:

- Сертифікація та маркування CE: завдяки створенню схеми сертифікації кібербезпеки ЄС виробники можуть отримати сертифікат, щоб показати відповідність необхідним стандартам кібербезпеки. Сертифіковані продукти матимуть маркування CE, що вказує на відповідність вимогам кібербезпеки.
- Відповідність нормам ЄС: запроваджуючи вимоги щодо кібербезпеки

для виробників і роздрібних торговців, CRA забезпечує дотримання норм ЄС, підтримуючи створення більш безпечної цифрової екосистеми.

- Покращена кібербезпека: CRA встановлює вимоги щодо кібербезпеки для продуктів із цифровими елементами, що веде до вдосконалення заходів безпеки, які зменшують ризики кібератак і захищають цифрові продукти від потенційної вразливості.

- Поліпшення ринкових умов: обов'язкові вимоги CRA з кібербезпеки сприяють більш сприятливим умовах ринку продуктів і послуг у сфері кібербезпеки, заохочуючи інновації та конкуренцію, що приносить користь підприємствам і споживачам.

- Підвищення впевненості та довіри споживачів: споживачі можуть бути впевнені, що як фізичні, так і цифрові продукти на ринку ЄС забезпечують підвищену безпеку, захищаючи їхні дані, конфіденційність і зміцнюючи довіру.

- Зниження ризиків кібератак: підкреслюючи оцінку ризиків кібербезпеки та безпеку за проектом, CRA дає можливість організаціям проактивно виявляти й усувати потенційні вразливості, значно знижуючи ймовірність успішних кібератак.

- Посилений цифровий захист: встановлені CRA зобов'язання щодо виробників охоплюють моніторинг внутрішньої активності, впровадження оновлень безпеки й обмеження поверхонь для атак, що покращує цифровий захист і стійкість компаній [61].

30 листопада 2023 року Європейський Парламент та Рада оголосили, що досягли попередньої угоди щодо Акту про кіберстійкість. Це означає, що обидва законодавчі органи ЄС узгодили текст акту, і він очікує на остаточне ухвалення й офіційну публікацію, після чого набуде чинності.

Варто зазначити, що крім перелічених вище вимог до цифрових виробів, угода CRA передбачає адекватні вказівки та підтримку для компаній-виробників щодо впровадження нових вимог кіберезпеки. Це включає конкретні заходи з підвищення обізнаності та навчання персоналу, а також підтримку тестування продуктів та оцінювання їх відповідності нормативним вимогам.

Введення в дію CRA сприятиме тому, що країни-члени (а також їхні підприємства та організації) значно покращать свою кібербезпеку та стійкість до цифрових загроз, а стратегія ЄС з кіберстійкості матиме значні практичні успіхи.

Висновки до розділу 3

У розділі 3 детально досліджено засади впровадження й оцінювання ефективності стратегії кіберстійкості організації як важливого інструменту у боротьбі з кіберзагрозами. Встановлено, що стратегія кіберстійкості - це ретельно розроблена архітектура, яка дає можливість забезпечити безперервність функціонування бізнесу в умовах виявлення, реагування й відновлення після кібератак. Впровадження успішної стратегії кіберстійкості дозволяє компанії гарантувати нормативну відповідність і зміцнити довіру зацікавлених сторін, демонструючи відданість кібербезпеці і стійкість у протидії кіберзагрозам.

Для ефективного впровадження стратегії кіберстійкості організація має забезпечити постійний моніторинг стану кібербезпеки, дотримуватися принципу нульової довіри, володіти детальною й актуальною інформацією про корпоративні дані й архітектуру, стимулювати співпрацю у сфері кібербезпеки, застосовувати сучасну платформу безпеки й управління даними, забезпечити високу швидкість і надійність операцій кібербезпеки.

Оцінювання ефективності стратегії кіберстійкості дозволяє організації проаналізувати поточний стан кібербезпеки, визначити рентабельність інвестицій у цю сферу, сприяє впровадженню більш гнучких і адаптивних підходів до управління кібербезпекою. Наголошено на необхідності інтеграції стратегії кіберстійкості у загальну бізнес-стратегію організації; комплексного підходу до оцінювання кіберстійкості, включаючи технічні, оперативні і стратегічні аспекти; постійного оновлення кіберстратегії до змінних умов кіберпростору; визначення методики і ключових метрик оцінювання кіберстійкості.

Відзначено важливу роль нормативно-правової бази у забезпеченні кіберстійкості організацій і підприємств на прикладі Акту про кіберстійкість ЄС, який встановлює жорсткі вимоги до кібербезпеки для виробників і дистриб'юторів цифрових продуктів упродовж усього їх життєвого циклу.

ВИСНОВКИ

У результаті дослідження встановлено відмінності між концепціями кібербезпеки та кіберстійкості бізнесу. Так, зазначено, що метою кібербезпеки є постійний захист цифрових мереж і систем бізнесу, щоб запобігти зловмисникам в реалізації кібератак. Натомість забезпечення кіберстійкості спрямоване га готовність до реалізованих кібератак, забезпечення можливості попри це далі вести бізнес та швидко відновлюватися.

Кібербезпека використовує такі засоби як міжмережеві екрани, антивіруси, криптографію, спрямовує зусилля на запобігання порушенням безпеки і неавторизованому доступу, протидіє загрозам ззовні. Кіберстійкість впроваджує стратегії реагування на інциденти і системи резервного копіювання, спрямовує зусилля на забезпечення безперервності бізнесу навіть після інциденту, протидіє загрозам як зовнішньо, так і внутрішньо, забезпечуючи організаційну стійкість.

У рамках вивчення методів кібербезпеки розглянуто превентивні й детективні методи кібербезпеки. Превентивні методи кібербезпеки охоплюють широкий спектр технічних і адміністративних засобів, які мають на меті зменшити вразливість систем і мереж до потенційних загроз і забезпечити належну підготовку організації до виявлення, протистояння і мінімізації наслідків небажаних подій. Детективні засоби управління забезпечують видимість зловмисної діяльності, порушень і атак на IT-середовище організації, яким не вдалося запобігти з використанням превентивних заходів.

У роботі детально досліджено засади впровадження й оцінювання ефективності стратегії кіберстійкості організації як важливого інструменту в боротьбі з кіберзагрозами. Встановлено, що стратегія кіберстійкості - це ретельно розроблена архітектура, яка дає можливість забезпечити безперервність функціонування бізнесу в умовах виявлення, реагування й відновлення після кібератак. Впровадження успішної стратегії кіберстійкості дозволяє компанії гарантувати нормативну відповідність і зміцнити довіру зацікавлених сторін,

демонструючи відданість кібербезпеці і стійкість у протидії кіберзагрозам.

Для ефективного впровадження стратегії кіберстійкості організація має забезпечити постійний моніторинг стану кібербезпеки, дотримуватися принципу нульової довіри, володіти детальною й актуальною інформацією про корпоративні дані й архітектуру, стимулювати співпрацю у сфері кібербезпеки, застосовувати сучасну платформу безпеки й управління даними, забезпечити високу швидкість і надійність операцій кібербезпеки.

Оцінювання ефективності стратегії кіберстійкості дозволяє організації проаналізувати поточний стан кібербезпеки, визначити рентабельність інвестицій у цю сферу, сприяє впровадженню більш гнучких і адаптивних підходів до управління кібербезпекою. Наголошено на необхідності інтеграції стратегії кіберстійкості у загальну бізнес-стратегію організації; комплексного підходу до оцінювання кіберстійкості, включаючи технічні, оперативні і стратегічні аспекти; постійного оновлення кіберстратегії до змінних умов кіберпростору; визначення методики і ключових метрик оцінювання кіберстійкості.

ПЕРЕЛІК ПОСИЛАНЬ

1. Cyber Threats and Advisories | Cybersecurity and Infrastructure Security Agency CISA. *CISA*. URL: https://www.cisa.gov/topics/cyber-threats-and-advisories
2. Drolet M. Council Post: Eight Cybersecurity Trends To Watch For 2024. *Forbes*. URL: https://www.forbes.com/sites/forbestechcouncil/2023/12/26/eight-cybersecurity-trends-to-watch-for-2024/?sh=27023e5b4111
3. Cybersecurity Best Practices | Cybersecurity and Infrastructure Security Agency CISA. *CISA*. URL: https://www.cisa.gov/topics/cybersecurity-best-practices
4. FACT SHEET: Act Now to Protect Against Potential Cyberattacks. *The White House*. URL: https://www.whitehouse.gov/briefing-room/statements-releases/2022/03/21/fact-sheet-act-now-to-protect-against-potential-cyberattacks/
5. Cybersecurity measurement. *NIST*. URL: https://www.nist.gov/cybersecurity-measurement
6. Cybersecurity Threats Fast-Forward 2030: Fasten your Security-Belt Before the Ride! URL: https://www.enisa.europa.eu/news/cybersecurity-threats-fast-forward-2030
7. Top 11 Cybersecurity Frameworks. ConnectWise. *MSP Technology - IT Management Software - ConnectWise*. URL: https://www.connectwise.com/blog/cybersecurity/11-best-cybersecurity-frameworks
8. Cybersecurity Framework. *NIST*. URL: https://www.nist.gov/cyberframework
9. The Fundamentals of a Strong Cybersecurity Framework. *Infused Innovations*. URL: https://www.infusedinnovations.com/blog/secure-intelligent-workplace/the-fundamentals-of-a-strong-cybersecurity-framework
10. ISO/IEC 27001:2022. *ISO*. URL: https://www.iso.org/standard/27001
11. CIS Controls. *CIS*. URL: https://www.cisecurity.org/controls
12. System and Organization Controls: SOC Suite of Services. *AICPA & CIMA*. URL: https://www.aicpa-cima.com/resources/landing/system-and-organization-controls-soc-suite-of-services

13. About Us. *PCI Security Standards Council*. URL: https://www.pcisecuritystandards.org/about_us/

14. PCI-DSS certification. *Imperva*. URL: https://www.imperva.com/learn/data-security/pci-dss-certification/:

15. COBIT. Control Objectives for Information Technologies. *ISACA*. URL: https://www.isaca.org/resources/cobit

16. HITRUST. *HITRUST Alliance*. URL: https://hitrustalliance.net/

17. CSA. *CSA*. URL: https://cloudsecurityalliance.org/research/cloud-controls-matrix/

18. Chief Information Officer. *U.S. Department of Defense*. URL: https://dodcio.defense.gov/CMMC/

19. Essential Eight Compliance Guide (Updated for 2023). *Third-Party Risk and Attack Surface Management Software. UpGuard*. URL: https://www.upguard.com/blog/essential-eight

20. About Cyber Essentials. *NCSC*. URL: https://www.ncsc.gov.uk/cyberessentials/overview

21. 12 Cybersecurity Best Practices to Prevent Cyber Attacks in 2023. *Ekran System*. URL: https://www.ekransystem.com/en/blog/best-cyber-security-practices

22. Federal zero trust architecture. *The White House*. URL: https://www.whitehouse.gov/wp-content/uploads/2022/01/M-22-09.pdf

23. Modem-wiping malware was behind Viasat cyberattack. *ZDNET*. URL: https://www.zdnet.com/article/modem-wiping-malware-was-behind-viasat-cyberattack/

24. How to Build an Effective Cybersecurity Strategy for your Company. *Ekran System*. URL: https://www.ekransystem.com/en/blog/responding-to-changes

25. Conducting User Activity Monitoring Using Existing IT Infrastructure. *ISACA*. URL: https://www.isaca.org/resources/isaca-journal/issues/2019/volume-2/conducting-user-activity-monitoring-using-existing-it-infrastructure

26. Understanding Open Source Adoption: Insights from the 9th State of the Software Supply Chain Report. *Software Supply Chain Management. Sonatype*. URL: https://www.sonatype.com/state-of-the-software-supply-

chain/introduction?utm_campaign=pr&utm_source=pressrelease&utm_medium=organic

27. Shead S. Solarwinds hackers are targeting the global IT supply chain, Microsoft says. *CNBC*. URL: https://www.cnbc.com/2021/10/25/solarwinds-hackers-targeting-global-it-supply-chain-microsoft-says.html

28. Cybersecurity Supply Chain Risk Management Practices for Systems and Organizations. *NIST Special Publication. NIST SP 800-161r1*. URL: https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-161r1.pdf

29. Key Practices in Cyber Supply Chain Risk Management. *NISTIR 8276*. URL: https://nvlpubs.nist.gov/nistpubs/ir/2021/NIST.IR.8276.pdf

30. Shea S. What is Data Security? The Ultimate Guide. *Security*. URL: https://www.techtarget.com/searchsecurity/Data-security-guide-Everything-you-need-to-know

31. Біометрія. *Вікіпедія*. URL: https://uk.wikipedia.org/wiki/Біометрія

32. Data-Driven Behavioural Biometrics for Continuous and Adaptive User Verification Using Smartphone and Smartwatch. *MDPI*. URL: https://www.mdpi.com/2071-1050/14/12/7362

33. What is Multi-Factor Authentication (MFA) and How does it Work? *RSA*. URL: https://www.rsa.com/multi-factor-authentication/what-is-mfa/

34. IS Audit Basics: Auditing Cybersecurity. *ISACA*. URL: https://www.isaca.org/resources/isaca-journal/issues/2019/volume-2/is-audit-basics-auditing-cybersecurity

35. Simplicity is the Key to Enterprise Cybersecurity. *VMware Security Blog*. URL: https://blogs.vmware.com/security/2020/03/simplicity-is-the-key-to-enterprise-cybersecurity.html

36. Cybersecurity Detective Controls–Monitoring to Identify and Respond to Threats. *ISACA*. URL: https://www.isaca.org/resources/isaca-journal/issues/2015/volume-5/cybersecurity-detective-controlsmonitoring-to-identify-and-respond-to-threats

37. What Is SIEM Integration? 2023 Comprehensive Guide. *Software Selection Tool. SelectHub*. URL: https://www.selecthub.com/siem/siem-integration/

38. SIEM Implementation. Best Practices and Step-by-Step Guide. *Pendello Solutions*. URL: https://www.pendello.com/blog/siem-implementation-best-practices-and-step-by-step-guide

39. Log Management Best Practices. *RSA*. URL: https://www.robinsoninsight.com/wp-content/uploads/2017/07/LMBP_WP_0707-lowres.pdf.

40. Guide to Cyber Threat Information Sharing. *NIST*. URL: https://www.nist.gov/publications/guide-cyber-threat-information-sharing

41. Cybersecurity Detective Controls–Monitoring to Identify and Respond to Threats. *ISACA*. URL: https://www.isaca.org/resources/isaca-journal/issues/2015/volume-5/cybersecurity-detective-controlsmonitoring-to-identify-and-respond-to-threats#10

42. Incident Response Plan: Frameworks and Steps. *CrowdStrike*. URL: https://www.crowdstrike.com/cybersecurity-101/incident-response/incident-response-steps/

43. Kolodgy C. 13 incident response best practices for your organization. *TechTarget*. URL: https://www.techtarget.com/searchsecurity/tip/Incident-response-best-practices-for-your-organization

44. Best Practices for Testing Your Cyber Incident Response Plan. *RSI Security*. URL: https://blog.rsisecurity.com/best-practices-for-testing-your-cyber-incident-response-plan/

45. Geer D. Building an incident response framework for your enterprise | *TechTarget*. URL: https://www.techtarget.com/searchsecurity/tip/Incident-response-frameworks-for-enterprise-security-teams

46. Moyle E. CERT vs. CSIRT vs. SOC: What's the Difference? | *TechTarget*. URL: https://www.techtarget.com/searchsecurity/tip/CERT-vs-CSIRT-vs-SOC-Whats-the-difference

47. Understanding incident response roles and responsibilities. *Atlassian*. URL: https://www.atlassian.com/incident-management/incident-response/roles-responsibilities

48. What is SOAR (Security Orchestration, Automation and Response)? *IBM*. URL: https://www.ibm.com/topics/security-orchestration-automation-response

49. Post-Cyber Attack: 7 Critical Steps To Take Toward Full Recovery. *CyberDB*. URL: https://www.cyberdb.co/post-cyber-attack-7-critical-steps-to-take-toward-full-recovery/

50. 3 principles to help build a cyber resilient organization. *World Economic Forum*. URL: https://www.weforum.org/agenda/2021/11/3-principles-to-help-build-a-cyber-resilient-organization/

51. What Is Cyber Resilience and Why Is It Important? *RSI Security*. URL: https://blog.rsisecurity.com/what-is-cyber-resilience-and-why-is-it-important/

52. Stanik J., Napiórkowski J. Cyber Resilience as a New Strategy to Reduce the Impact of Cyber Threats. *SpringerLink*. URL: https://link.springer.com/chapter/10.1007/978-3-031-45021-1_6

53. Trusted public-private partnerships. *Cohesity*. URL: http://surl.li/oxazl

54. Cybersecurity Policy Development 101: What Should be Included in a Cybersecurity Policy? *Warren Averett CPAs & Advisors*. URL: https://warrenaverett.com/insights/cybersecurity-policy-development/

55. Best practices for achieving success with Zero Trust. AWS Prescriptive Guidance. *AWS*. URL: https://docs.aws.amazon.com/prescriptive-guidance/latest/strategy-zero-trust-architecture/best-practices.html

56. Cohesity. 6 cyber resilience best practices. *LinkedIn: Log In or Sign Up*. URL: https://www.linkedin.com/pulse/6-cyber-resilience-best-practices-cohesity/

57. The Cybersecurity Resilience Quotient: Measuring Security Effectiveness. *SecurityWeek*. URL: https://www.securityweek.com/the-cybersecurity-resilience-quotient-measuring-security-effectiveness/

58. Cyber Resiliency Metrics, Measures of Effectiveness, and Scoring. *Mitre Publication*. URL: https://www.mitre.org/sites/default/files/2021-11/prs-18-2579-cyber-resiliency-metrics-measures-of-effectiveness-and-scoring.pdf.

59. Cyber Resilience Act: agreement with Council to boost digital products' security. News. *European Parliament*. URL: https://www.europarl.europa.eu/news/en/press-

room/20231106IPR09007/cyber-resilience-act-agreement-with-council-to-boost-digital-products-security

60. The CRA, explained - the Cyber Resilience Act. *Cyber Resilience Act*. URL: https://www.cyberresilienceact.eu/the-cra-explained/

61. The undeniable benefits of making cyber resiliency the new standard. *CSO Online*. URL: https://www.csoonline.com/article/654891/the-undeniable-benefits-of-making-cyber-resiliency-the-new-standard.html