

НАЦІОНАЛЬНИЙ ТЕХНІЧНИЙ УНІВЕРСИТЕТ УКРАЇНИ
«КИЇВСЬКИЙ ПОЛІТЕХНІЧНИЙ ІНСТИТУТ
імені ІГОРЯ СІКОРСЬКОГО»
ФІЗИКО-ТЕХНІЧНИЙ ІНСТИТУТ
Кафедра інформаційної безпеки

«На правах рукопису»

УДК 004.056

«До захисту допущено»

В.о. завідувача кафедри
_____ М.В.Грайворонський
“ ____ ” _____ 2019 р.

Магістерська дисертація
на здобуття ступеня магістра

зі спеціальності: 125 Кібербезпека

на тему: Фреймворк управління процесами забезпечення інформаційної безпеки в SOC

Виконав (-ла): студент (-ка) _____ курсу, групи _____
(шифр групи)

Насвіт Євгеній Олексійович _____
(прізвище, ім'я, по батькові) (підпис)

Науковий керівник к.т.н., доц. Коломицев Михайло Володимирович _____
(посада, науковий ступінь, вчене звання, прізвище та ініціали) (підпис)

Рецензент _____
(посада, науковий ступінь, вчене звання, науковий ступінь, прізвище та ініціали) (підпис)

Засвідчую, що у цій магістерській дисертації немає запозичень з праць інших авторів без відповідних посилань.

Студент _____
(підпис)

Київ – 2019 року

РЕФЕРАТ

Представлена робота має обсяг 140 сторінок, містить 18 ілюстрацій, 32 таблиці та 40 літературних посилань.

Метою даної роботи є розробка фреймворку управління процесами безпеки для SOC, базуючись на попередньому огляді проблеми та існуючих рішеннях, що теоретично можуть застосовуватись в контексті побудови методики оперування SOC.

Об'єктом дослідження є процеси безпеки SOC, ключові складові компонентів SOC, а також наявні рішення, щодо побудови методики оперування SOC.

Предметом дослідження є архітектурні та концептуальні особливості, а також типові проблеми із моніторингом та спостережністю інфраструктури за допомогою SOC.

Результатом роботи є фреймворк управління процесами забезпечення інформаційної безпеки в SOC, для структурування, вибору необхідної методики, оцінки ризиків, пов'язаних з вразливостями та розробки методології управління процесами безпеки SOC, з можливістю оцінки здатностей операційного центру безпеки по основним складовим ключових компонентів.

Методи дослідження: ознайомлення та опрацювання літератури, що представлено монографічними та журнальними матеріалами, електронними ресурсами, а також книгами, які стосуються досліджуваної теми, структурування одержаних результатів, адаптація існуючих рішень до сучасних вимог безпеки.

Результати роботи можуть бути використані для розробки та впровадження стратегії оперування для забезпечення кращої ефективності оперування SOC, а відповідно спостережності інформаційної чи мережевої інфраструктури за допомогою SOC.

Ключові слова: SOC, управління інформаційною безпекою, стандарт, фреймворк, процеси забезпечення безпеки, методика, метрики інформаційної безпеки

ABSTRACT

The presented work has 140 pages, 18 figures, 32 tables and 40 literary references.

The purpose of this work is to develop an information security process management framework based on preliminary overview of the problem and existing solutions that could theoretically be applied in the context of constructing a SOC operating methodology.

The object of the study is SOC security processes, key components of the SOC elements, as well as existing solutions, for the construction of the SOC operating technique.

The subject of the study is architectural and conceptual features, as well as typical problems with observing and monitoring infrastructure using SOC.

The result of the work is the SOC information security management framework for structuring, selecting the appropriate technique, assessing vulnerability risks, and developing a SOC security management methodology, with the ability to evaluate the security operations center's capability across key components.

Methods of study: familiarization and processing of literature, presented by monographic and journal materials, electronic resources, as well as books related to the subject, structuring of the obtained results, adaptation of existing solutions to current security requirements.

The results of the work can be used to develop and implement an operating strategy to improve the efficiency of SOC operations and, accordingly, to monitor information of network infrastructure using SOC.

Keywords: SOC, information security management, standard, framework, security processes, methodology, information security metrics

ЗМІСТ

Перелік умовних позначень, символів, одиниць, скорочень і термінів	7
Вступ.....	9
1 Управління інформаційною безпекою та SOC	12
1.1 Управління інформаційною безпекою.....	12
1.2 Архітектура та загальні особливості операційних центрів безпеки	15
Висновки до розділу 1	21
2 Аналіз стандартів та фреймворків, які використовуються для управління процесами ІБ	22
2.1 Серія стандартів 27000	22
2.2 Стандарт COBIT.....	39
2.3 Стандарт ITIL	49
2.4 Фреймворк Six Sigma.....	60
2.5 Порівняльний аналіз стандартів управління ІБ з позицій застосування в SOC	73
Висновки до розділу 2.....	78
3 Розробка фреймворку управління процесами забезпечення інформаційної безпеки в SOC	79
3.1 Загальна ідея фреймворку управління процесами забезпечення інформаційної безпеки	79
3.2 Збір та аналіз даних метрик інформаційної безпеки.....	81
3.3 Розробка проекту вимірювання інформаційної безпеки	99
3.4 Управління вимірюванням рівня інформаційної безпеки за допомогою програми безпеки	105
3.5 Оцінка здатностей SOC	109
Висновки до розділу 3.....	115
4 Стартап.....	116
4.1 Опис ідеї проекту	116
4.2 Технологічний аудит ідеї проекту	119
4.3 Аналіз ринкових можливостей запуску стартап-проекту.....	119
4.4 Розроблення ринкової стратегії проекту	127
4.5 Розроблення маркетингової програми стартап-проекту.....	130
Висновки до розділу 4.....	134
Висновки.....	135
Перелік джерел-посилання	136

ПЕРЕЛІК УМОВНИХ ПОЗНАЧЕНЬ, СИМВОЛІВ, ОДИНИЦЬ, СКОРОЧЕНЬ І ТЕРМІНІВ

SOC – Security Operations Center (Операційний Центр Безпеки)

ІБ – Інформаційна Безпека

SLA – Service Level Agreement

СУІБ – Система Управління Інформаційною Безпекою

ISO – International Organization for Standardization

COBIT – Control Objectives for Information and Related Technologies

ITIL – Information Technology Infrastructure Library

SIEM – Security Information and Event Management

EDR – Endpoint Detection and Response

IDS – Intrusion Detection System

IPS – Intrusion Prevention System

DNS – Domain Name System

NTP – Network Time Protocol

AD – Active Directory

VoIP – Voice over IP

IEC – International Electrotechnical Commission

PDCA – Plan Do Check Act

ISACA – Information Systems Audit and Control Association

ПВП – Постійне Вдосконалення Послуг

IP – Internet Protocol

DMAIC – Define Measure Analyze Improve Control

DMADV – Define Measure Analyze Design Verify

CVSS – Common Vulnerability Scoring System

FMEA – Failure Mode and Effects Analysis

ANOVA – Analysis Of Variation

DOE – Design of Experiments

OWASP – Open Web Application Security Project

КПС – Кількість Подій на Секунду

CAQDAS – Computer Assisted Qualitative Data Analysis Software

ВСТУП

SOC - централізований підрозділ установи, який вирішує питання з інформаційної та кібербезпеки на організаційному та технічному рівні. На сьогодні такі операційні центри безпеки завойовуються величезну популярність, як в державних так і приватних структурах, що пояснюється цілим рядом переваг, від впровадження даного рішення – ефективна реакція на інциденти, зниження ризику переривань в роботі мережі, пов'язаних з подіями інформаційної безпеки, вдосконалення відповідних заходів для забезпечення безпеки, підвищення ефективності роботи, скорочення затрат, а також відповідність нормативним вимогам. Побудова та впровадження, а також, що є досить важливо, оперування SOC, зазвичай викликає труднощі, пов'язані з суттєвим набором технологій, а також великою кількістю процесів, які потрібно враховувати, та якими потрібно керувати для досягнення поставлених цілей SOC.

Після побудови та впровадження SOC, завжди виникає необхідність побудувати, або структурувати аналіз, збір даних, налаштувати управління процесами безпеки SOC. Зазвичай відбувається суттєве навантаження даними та подіями, а побудований та впроваджений SOC просто не справляється з покладеними на нього задачами, що ускладнює моніторинг мережевої інфраструктури, сповільнює виявлення та вирішення вразливостей та інцидентів, а відповідно на пряму шкодить загальній інформаційній безпеці організації та приносить, як наслідок величезні збитки.

В результаті, розробка певної програми чи фреймворку для налаштування та структурування аналізу, збору даних, оцінки ризиків та управління процесами з подальшою оцінкою здатності є важливими завданнями, які потребують виконання.

Актуальність даної роботи полягає в тому, що в ній аналізуються існуючі рішення в області управління інформаційною безпекою, на основі яких можна побудувати методологію оперування SOC. На сьогодні не представлено такої методології чи фреймворку, який би в максимально зручному форматі задавав

структуровану програму, що включала б попередню оцінку ризиків та управління вразливостями, методики та інструменти аналізу та збору даних, а також налаштування управління процесами безпеки з можливістю подальшої оцінки здатності SOC. В даній роботі представлено напрямки вдосконалення фази оперування для SOC, а також запропонований фреймворк управління процесами забезпечення безпеки для фази оперування в SOC, що базується на попередніх дослідженнях в цій галузі, а також практичному досвіді при роботі з даними та подіями в SOC.

Метою даної роботи є розробка фреймворку управління процесами безпеки для SOC, базуючись на попередньому огляді проблеми та існуючих рішеннях, що теоретично можуть застосовуватись в контексті побудови методики оперування SOC.

Завдання, які були поставлені при виконанні даної роботи:

- 1) Розглянути та проаналізувати архітектурні та концептуальні особливості операційних центрів безпеки
- 2) Виокремити основні проблеми, що виникають під час оперування SOC
- 3) Розглянути стандарти та фреймворки в області управління інформаційною безпекою, а також виокремити їх основні переваги та недоліки, а також можливість застосування в SOC
- 4) На основі результатів досліджень, а також практичного досвіду роботи з SOC розробити фреймворк, який міг би використовуватись для забезпечення спостережності інфраструктури мережі в результаті побудови методології оперування SOC.

Об'єктом дослідження є процеси безпеки SOC, ключові складові компонентів SOC, а також наявні рішення, щодо побудови методики оперування SOC.

Предметом дослідження є архітектурні та концептуальні особливості, а також типові проблеми із моніторингом та спостережністю інфраструктури за допомогою SOC.

Методи дослідження: ознайомлення та опрацювання літератури, що представлено монографічними та журнальними матеріалами, електронними ресурсами, а також книгами, які стосуються досліджуваної теми, застосування власного практичного досвіду в області SOC, структурування отриманих результатів, адаптація існуючих рішень до сучасних вимог безпеки.

Наукова новизна даної роботи полягає у тому, що було запропоновано методологію управління процесами безпеки під час оперування SOC у вигляді послідовної та чітко структурованої програми, з фокусом на збір та аналіз даних метрик безпеки, а також описом інструментів та методик, які є застосовними в контексті фреймворку.

Практичне значення результатів фреймворку управління процесами безпеки полягає у практичному застосуванні результатів дослідження для побудови структурованої програми управління збором та аналізом даних, а також процесами безпеки SOC, з подальшою оцінкою здатностей SOC. Впровадження запропонованого фреймворку допоможе забезпечити кращу ефективність оперування SOC, а відповідно і кращу спостережність інформаційної чи мережевої інфраструктури за допомогою SOC.

Апробація результатів роботи: результати оприлюднено на IV Міжнародній науково-практичній конференції «Потенціал сучасної науки» (10-11 грудня 2019 р., м.Київ).

Публікації: результати магістерської дисертації опубліковані у вигляді тез «Фреймворк управління процесами забезпечення інформаційної безпеки в SOC».

1 УПРАВЛІННЯ ІНФОРМАЦІЙНОЮ БЕЗПЕКОЮ ТА SOC

1.1 Управління інформаційною безпекою

Управління ІБ описує засоби управління, які організація повинна впровадити, щоб забезпечити захист конфіденційності, доступності та цілісності активів від загроз та вразливостей [1]. Крім того, управління ІБ включає управління інформаційними ризиками, процес, який включає оцінку ризиків, з якими організація повинна мати справу при управлінні та захисті активів, а також розповсюдження ризиків серед всіх відповідних зацікавлених сторін. Для цього необхідна належна ідентифікація активів та етапів оцінки, включаючи оцінку цінності конфіденційності, цілісності, доступності і заміни активів.

По суті, управління ІБ означає управління і зменшення різних загроз і вразливостей для активів з одночасним балансуванням зусиль по управлінню, затрачених на потенційні загрози та вразливості, шляхом вимірювання імовірності їх фактичного виникнення.

Після відповідної ідентифікації і оцінки активів, управління ризиками і їх зменшення по відношенню до активів включають аналіз наступних питань [4]:

- Загрози. Небажані події, які можуть призвести до навмисної або випадкової втрати, пошкодження або неправильному використанню інформаційних активів.
- Вразливості. Наскільки інформаційні активи та пов'язані з ними засоби управління схильні до експлуатації однієї чи декількох загроз
- Вплив та ймовірність. Величина потенційної шкоди інформаційним активам від загроз та вразливостей, а також серйозність ризику, який вони представляють для активу; аналіз затрат і вигоди також можуть бути частиною оцінки впливу чи окремо від неї
- Зменшення. Пропоновані методи для мінімізації впливу та ймовірності потенційних загроз і вразливостей

Після того, як загрози та вразливості були виявлені та оцінені як такі, які надають достатній вплив на інформаційні активи, може бути прийнятий план зменшення. Вибраний метод зменшення в значній мірі залежить від того, в якому домені інформаційних технологій знаходиться загроза або вразливість [2].

Управління ІБ забезпечує інтегрований підхід до управління послугами, виконуючи наступні дії [1]:

- Виявлення та визначення внутрішніх та зовнішніх вимог безпеки
- Планування процедур безпеки
- Створення розділу ІБ в SLA та Service Description
- Управління виконанням заходів безпеки
- Оцінка процедур безпеки і заходів безпеки
- Звіти про безпеку
- Вдосконалення безпеки

Одним з ключових понять в управлінні інформаційною безпекою є система управління інформаційною безпекою, що представляє собою сукупність усіх взаємопов'язаних/взаємодіючих елементів інформаційної безпеки організації, для гарантії того, що політики, процедури і цілі могли бути створені, впроваджені, передані та оцінені, для забезпечення загальної ІБ організації. Система управління інформаційною безпекою може бути інтерпретована як системний підхід для встановлення, реалізації, експлуатації, моніторингу, аналізу, підтримки та вдосконалення інформаційної безпеки організації. Така система зазвичай залежить від потреб, цілей, вимог безпеки, а також розміру та процесів організації. СУІБ включає та надає ефективні стратегії управління ризиками та їх зниження. Крім того, прийняття організацією СУІБ вказує на те, що вона систематично виявляє, оцінює і управляє ризиками ІБ, а також буде здатна успішно задовольняти вимогам конфіденційності, цілісності і доступності інформації. Незважаючи на важливість створення та обслуговування СУІБ, навчання персоналу СУІБ та забезпечення відповідності щоденним процесам та діям в організації – є один із основних пріоритетів для кінцевого адекватного захисту даних. Пов'язані з розробкою, впровадженням та практикою СУІБ людські фактори також повинні враховуватись,

для забезпечення кінцевого успіху СУІБ найкращим чином. Ключовими елементами функціонування СУІБ є процеси. Однак, незважаючи на свою важливість, структура процесу СУІБ з описом процесів СУІБ та їх взаємодія, а також взаємодія з іншими процесами відсутня в літературі [2, 4].

Для ідентифікації процесів у СУІБ, застосовуються наступні методи [2]:

- Аналіз серії стандартів ISO 27000
- Аналіз стандартів ITIL та COBIT відносно уже ідентифікованих процесів в ISO 27000, а також відносно можливих додаткових процесів СУІБ.

Внаслідок співставлення результатів ідентифікуються наступні ключові процеси СУІБ [1, 2, 3, 4]:

- Процес оцінки ризиків інформаційної безпеки
- Процес усунення ризиків інформаційної безпеки
- Процес управління ресурсами
- Процес забезпечення обізнаності та компетентності
- Процес зв'язку
- Процес контролю контролю документації та записів
- Процес управління вимогами
- Процес управління змінами інформаційної безпеки
- Процес управління зовнішніми процесами
- Процес оцінки продуктивності
- Процес внутрішнього аудиту
- Процес управління інцидентами інформаційної безпеки
- Процес вдосконалення інформаційної безпеки
- Процес управління відносинами і споживачем інформаційної безпеки
- Процес управління конфігураціями

Оскільки поняття безпека не є кінцевим станом, якого необхідно досягти, а відповідає процесам, направленим на забезпечення захищеності певної інфраструктури, поняття “управління інформаційною безпекою” розглядається як управління процесами безпеки або управління процесами забезпечення безпеки.

Як уже було згадано раніше, інструменти, які доступні для допомоги організаціям в реалізації відповідних програм та засобів управління для зменшення загроз та вразливостей включають сімейство стандартів ISO 27000, структуру ITIL, структуру COBIT, а також велику кількість методологій, бібліотек та фреймворків.

Одним з перспективних напрямків, що активно розвиваються та впроваджуються на сьогодні – операційні центри безпеки, які є комплексним підходом до управління інформаційною безпекою (причому як і в контексті власне внутрішньої безпеки організації, так і безпеки інших організацій, залежно від призначення SOC). Така структура може визначатись як система управління інформаційною безпекою з орієнтацією на процеси ІБ із власною специфікою, характерною саме SOC. Розглянемо базові особливості та архітектуру SOC.

1.2 Архітектура та загальні особливості операційних центрів безпеки

Операційний центр безпеки (Security Operations Center або SOC) – організаційно-штатна структура, що відповідає за обробку інцидентів ІБ та володіє усім необхідним технічним забезпеченням. Це об'єкт, де корпоративні інформаційні системи (веб-сайти, додатки, бази даних, центри обробки даних, сервери, активне мережеве обладнання, комп'ютери та інше кінцеве обладнання) контролюються, оцінюються та захищаються [5].

SOC діє як хаб або центральний командний пункт, приймаючи телеметрію, мережеві пакети, дані системних журналів з усієї IT-інфраструктури організації, включаючи її мережі, пристрої, прилади та сховища інформації, де б не знаходились ці активи. По суті, SOC - це точка кореляції для кожної події, зареєстрованої в організації, за якою ведеться моніторинг. Для кожного з цих подій SOC повинен вирішити, як ними керувати та діяти [6].

SOC зазвичай побудовані навколо архітектури “концентратор-кінцеві точки”, де система управління інформацією про безпеку та подіями безпеки (SIEM) агрегує та корелює дані з каналів безпеки. Кінцеві точки цієї моделі можуть включати різні системи, наприклад системи оцінки вразливостей, ризиків та

відповідності політиці безпеки, сканери додатків і баз даних, системи запобігання вторгнень, аналітика поведінки користувачів та організацій, системи виявлення і виправлення кінцевих точок (EDR), і платформи розвідки загроз [6].

SOC також здійснює моніторинг мереж та кінцевих точок на предмет вразливостей з метою захисту конфіденційних даних та відповідності вимогам галузевих чи урядових норм.

Команда SOC відповідає за поточну, оперативну складову інформаційної безпеки підприємства. Персонал SOC складається, головним чином, з аналітиків безпеки, які спільно працюють над виявленням, аналізом, реагуванням, звітуванням та запобіганням інцидентів кібербезпеки. Додаткові можливості деяких SOC можуть включати розширений криміналістичний аналіз, криптоаналіз та реверс-інжиніринг для аналізу інцидентів [7].

Розглянемо загальні особливості та архітектуру операційних центрів безпеки.

Основне завдання операційних центрів безпеки — аналіз на основі поточного моніторингу подій інформаційної безпеки. Далі за пріоритетністю ідуть виявлення аномалій, відповідь на інциденти безпеки та виправлення наслідків кожної відстеженої події [5].

SOC об'єднує людей, процеси та технології для забезпечення обізнаності в поточній ситуації щодо інформаційної безпеки. В організації, частиною якої є SOC, він розбирається з будь-якою загрозливою подією щодо інформаційної безпеки. Це включає належну ідентифікацію, аналіз, інформування, розслідування та подальше звітування [5].

Одним із завдань SOC є навчання та інформування користувачів, зокрема, прищеплення їм культури кібербезпеки, а також оперативне інформування про виникнення загроз та план дій на випадок кібератак. Без такої роботи з користувачами кібербезпека може виявитися неефективною.

Основними функціями SOC є [5]:

- проактивний нагляд за ІТ-системами та постійний аналіз поточного стану загроз;
- розпізнання слабких місць у ІТ-безпеці та їхнє усунення;

- централізоване управління безпеки різноманітними пристроями у системі;
- «сигналізація» у випадку розпізнання нападів та загроз;
- безпосередні заходи щодо захисту та/або мінімізації шкоди під час кібератак;
- проведення оцінки стану систем ІТ-безпеки;
- технічна підтримка в усіх пов'язаних з ІТ-безпекою питаннях;
- звітування щодо роботи SOC та усіх пов'язаних з ІТ-безпекою систем.

Окрім основних, SOC може підтримувати і розширені функції [5]:

- управління змінами (конфігураціями, патчами)
- панелі безпеки
- управління ризиками
- інтеграція з сервісним столом

Основна множина сервісів, які надає SOC включає в себе [9]:

- Управління службами безпеки
- Інженерія служб безпеки
- Оперування службами безпеки
- Сервіс розслідування та реакції на інциденти безпеки
- Сервіс управління журналами (логами)
- Сервіс виявлення вразливостей
- Сервіс управління загрозами та вразливостями
- Сервіс звітування та аналітики безпеки
- Сервіс виявлення порушень

Розглянемо основні складові найважливіших компонентів SOC – люди, процеси та технології.

Основними складовими компоненту “люди” в SOC є [6, 7, 8, 9]:

- керівництво (тобто як SOC управляється)
- структура (тобто як організація структурована)
- досвід
- навчання та сертифікація

Основними складовими компоненту “процеси” в SOC є [6, 7, 8, 9]:

- сортування по інцидентам

- звітування по інцидентах
- аналіз інцидентів
- закриття інцидентів
- активності, що відбуваються після інциденту
- виявлення вразливостей
- усунення та відслідковування вразливостей

Основними складовими компоненту “технології” є [6, 7, 8, 9]:

- мережева інфраструктура
- збір, кореляція та аналіз подій
- моніторинг
- контроль
- управління журналами (логами)
- оцінка вразливостей
- відслідковування вразливостей

Для збору та кореляції даних частіше всього застосовуються SIEM-системи, для агрегації великої кількості даних та представлення їх в зручному для перегляду, пошуку та аналізу вигляді. Перелічимо типові пристрої та рішення, які можуть бути підключені до SIEM-системи, для надсилання даних в SOC [6, 7, 8, 9]:

- Апаратні міжмережеві екрани (stateful та stateless), де типовими даними, які необхідно зібрати є:
- Програмні міжмережеві екрани
- Засоби забезпечення безпеки із “хмари”, що мають функції міжмережевих екранів
- Брандмауери рівня хоста
- Системи виявлення та попередження вторгнень IDS/IPS на основі сигнатурного та статистичного (на основі аномалій) аналізу
- Маршрутизатори/Комутатори
- Системи захисту хостів
 - Брандмауери
 - IDS/IPS рівня хоста

- Технології антивірус, антиспам
 - Технології веб-безпеки
- Системи зберігання та захисту даних
 - Системи захисту від втрати даних (локальний агент або шифрування диску)
 - “Хмарні” сховища
- Веб-проксі
- “Хмарні” проксі
- Сервери
 - DNS-сервери
 - NTP-сервери
 - AD-сервери
 - Файлові сервери
 - Веб-сервери
 - Сервери віртуалізації
 - Сервери застосунків
 - Сервери авторизації, автентифікації та обліку
- Мережева телеметрія
- Бази даних
- Інструменти для сканування та аналізу
- Системи взаємодії персоналу
 - VoIP
 - Електронна пошта
 - Внутрішні веб-сайти
 - Відеозв’язок
- Системи виявлення порушень
 - “Мережеві пастки”
 - “Пісочниці”
- Системи мережевої криміналістики (forensics)

Крім того, для аналізу даних слід враховувати також наступні джерела:

- Системні журнали
- Аудиторські звіти
- Опитування персоналу
- Політики та інші записи та документи

Типова мережева архітектура SOC може бути представлена у вигляді наступної схеми [9]:

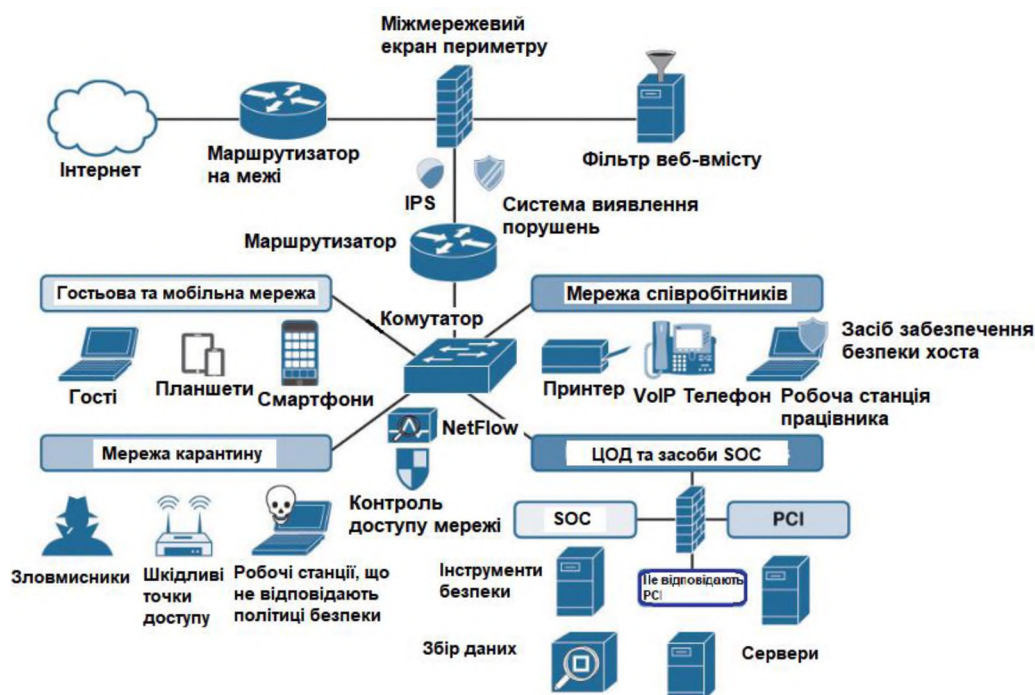


Рисунок 1.1 – Типова якісна мережева архітектура SOC

Зазвичай створення SOC здійснюється в 4 основні фази:

- Планування
- Розробка
- Побудова
- Оперування.

На фазі планування відбувається визначення стратегії SOC (визначення місії, стратегічних цілей, сфери застосування, моделі оперування, сервісів, здатностей, а також метрик та ключових показників ефективності), а також плануються основні компоненти ключових складових – люди, процеси, технології. На двох наступних фазах відбувається розробка та впровадження попередньо запланованих ключових складових та їх компонентів. Розробка SOC вимагає чітко визначеної множини

сервісів, які поставлені в ряд із потребами та очікуваннями організації. Остання фаза фактично показує, як люди, процеси та технології, як частини ефективного SOC, діють разом для реакції на події та інциденти.

Основними проблемами, які виникають після розробки та впровадження SOC є:

- перевантаження потоком даних, подій та інцидентів на початку фази оперування
- необхідне постійне вдосконалення попередньо обраних та впроваджених технологій та сервісів, а відповідно процесів та процедур
- виникає необхідність побудови методології або плану оперування з подальшою оцінкою здатності SOC (які також допоможуть закрити питання перевантаження подіями та інцидентами, а також перевірити, чи впроваджений SOC відповідає очікуванням, заданим на фазі планування)

Висновки до розділу 1

Отже, в даному розділі було розглянуто поняття управління інформаційною безпекою, а також поняття операційних центрів безпеки, їх особливостей та архітектури. Визначений компонентний склад SOC, та його функціональне наповнення. Крім того, були виділені основні проблеми, що виникають після впровадження операційного центру безпеки. Оскільки SOC можна вважати системою управління інформаційною безпекою із власними особливостями, питання управління процесами безпеки в такій організаційній структурі є критичним, особливо у співвідношенні з раніше зазначеними проблемами на фазі оперування, де люди, процеси та технології, як частини ефективного SOC, діють разом для реакції на події та інциденти.

Загальновідомими практиками для побудови та впровадження стратегії управління процесами безпеки є застосування стандартів та методологій у сфері інформаційної безпеки. Необхідно розглянути та проаналізувати існуючий набір стандартів, бібліотек, методологій та фреймворків, які використовуються для управління ІБ та процесами забезпечення ІБ в цілому

2 АНАЛІЗ СТАНДАРТІВ ТА ФРЕЙМВОРКІВ, ЯКІ ВИКОРИСТОВУЮТЬСЯ ДЛЯ УПРАВЛІННЯ ПРОЦЕСАМИ ІБ

2.1 Серія стандартів 27000

Сімейство стандартів ISO 27000 представляє собою деякі з найбільш відомих стандартів, що регулюють управління ІБ та СУІБ, та засновані та загальносвітових висновках експертів. В них викладені вимоги до встановлення, впровадження, розгортання, моніторингу, перевірки, обслуговування, оновлення та вдосконалення СУІБ.

Для управління процесами забезпечення інформаційної безпеки розглянемо стандарти, в яких безпосередньо наведено вимоги, рекомендації та моделі стосовно СУІБ.

2.1.1 ISO 27001

Стандарт (Інформаційні технології – Методи забезпечення безпеки – Системи менеджменту інформаційної безпеки – Вимоги) підготовлений для реалізації вимог по створенню, впровадженню, підтримці і постійного вдосконалення системи менеджменту інформаційної безпеки. Розробка і впровадження системи менеджменту інформаційної безпеки організації залежить від потреб і цілей організації, вимог з безпеки, існуючих процесів організації, розміру і структури організації. Всі ці фактори впливу, як очікується, з часом змінюються [10].

Система менеджменту інформаційної безпеки забезпечує конфіденційність, цілісність і доступність інформації за рахунок застосування процесу менеджменту ризиків і надає впевненість зацікавленим сторонам в тому, що ризики адекватно управляються [11].

Важливо, щоб система менеджменту інформаційної безпеки була частиною і була інтегрована з процесами організації і загальною структурою менеджменту, а

також інформаційна безпека була застосована при розробці процесів, інформаційних систем і елементів управління. Впровадження системи менеджменту інформаційної безпеки буде масштабуватись відповідно до потреб організації [10, 11].

Стандарт можуть застосовувати внутрішні та зовнішні сторони для оцінки здатності організації виконувати власні вимоги організації по забезпеченню інформаційної безпеки.

Порядок, в якому вимоги представлені в цьому стандарті, не відображає їх важливості і не має на увазі те, що вони повинні бути реалізовані в такому порядку. Елементи стандарту нумеруються тільки в довідкових цілях.

ISO / IEC 27000 є загальні положення і словник для систем менеджменту інформаційної безпеки, посилаючись на серію стандартів для систем менеджменту інформаційної безпеки (в тому числі ISO / IEC 27003, ISO / IEC 27004 і ISO / IEC 27005), в яких використовуються відповідні терміни та визначення [10].

Цей стандарт встановлює вимоги до розробки, впровадження, підтримки і постійного вдосконалення системи менеджменту інформаційної безпеки в контексті організації, а також включає вимоги з оцінки та обробки ризиків інформаційної безпеки відповідно до потреб організації. Вимоги, викладені в цьому стандарті, носять загальний характер і призначені для застосування всіма організаціями, незалежно від типу, розміри або характеру [10].

Структура основних вимог стандарту включає наступні розділи [10]:

- Контекст організації
- Лідерство
- Планування
- Підтримка
- Експлуатація
- Оцінка результативності
- Вдосконалення

Переваги впровадження стандарту можна розділити на дві категорії: плюси від впровадження в організації стандарту і позитивні результати реалізації на його базі нормативних вимог щодо захисту інформації.

До першої категорії можна віднести [10]:

- єдиний і узгоджений підхід до захисту інформації в усій організації;
- економічне обґрунтування витрат на ІБ;
- ефективну організацію діяльності щодо захисту інформації та запобігання інцидентів;

Перевагами використання стандарту ISO / ІЕС 27001 в якості бази для захисту комерційної таємниці та виконання нормативних вимог щодо захисту персональних даних, банківської таємниці, критичної інформаційної інфраструктури, державних інформаційних систем можна назвати:

- загальну систему організаційно-розпорядчої документації щодо забезпечення інформаційної безпеки в організації, що мінімізує дублювання документів та підвищує якість і зручність їх використання, аналіз і перегляд;
- концентрацію компетенцій і знань щодо забезпечення інформаційної безпеки в єдиній організаційно-управлінській структурі;
- оптимізацію витрат на впровадження організаційних і технічних заходів захисту інформації за рахунок реалізації уніфікованого набору заходів захисту інформації в масштабі всієї організації;
- зниження витрат на модернізацію і розвиток системи інформаційної безпеки організації в разі зміни нормативних вимог за рахунок можливості вузьконаправленого коригування заходів захисту замість їх повного перегляду.

У пропонованого стандартом підходу є і обмеження. Основний - низька деталізація вимог і, відповідно, необхідність залучення для їх реалізації досвідчених експертів високого рівня. Цей недолік є наслідком гнучкості і адаптивності стандарту.

Іншим важливим обмеженням впровадження стандарту може стати набір застарілих правил і підходів до забезпечення захисту інформації. У багатьох

компаніях процеси менеджменту роками формувалися шляхом надмірної формалізації, і часто керівництво неохоче береться за кардинальну перебудову системи.

2.1.2 ISO 27002

Стандарт (Інформаційні технології – Методи захисту – Звід рекомендованих правил для управління інформаційною безпекою) був розроблений для застосування організаціями в якості довідкового матеріалу при виборі засобів реалізації в рамках процесу впровадження системи менеджменту інформаційної безпеки (СУІБ), заснованої на ISO 27001 або як керівний документ для організацій, які впроваджують широко поширені засоби реалізації інформаційної безпеки [12].

Інформаційна безпека досягається впровадженням відповідного набору засобів, включаючи політики, процеси, процедури, організаційні структури, а також програмного і апаратного забезпечення відповідного призначення. Ці засоби повинні бути розроблені і впроваджені, а результати їх роботи повинні відслідковуватися, аналізуватися і вдосконалюватися там, де це необхідно, щоб гарантувати досягнення конкретних цілей організації, як таких, які відносяться до безпеки, так і бізнесу в цілому [12].

Безпека, що забезпечується тільки технічними засобами, має обмежений характер і повинна бути доповнена відповідним менеджментом і процедурами. Визначення, які засоби використовувати в конкретному випадку, вимагає ретельного планування і уваги до деталей. Для успішного функціонування СУІБ потрібно її підтримка усіма співробітниками організації. Це може також вимагати участі акціонерів, постачальників або інших зовнішніх сторін. Також можуть знадобитися поради фахівців, які залучаються ззовні [12, 13].

Засоби управління інформаційною безпекою можуть бути обрані із запропонованих цим стандартом чи іншого набору заходів, а також, якщо необхідно, можуть бути розроблені нові засоби, щоб задовольнити певні потреби. Деякі із засобів, які пропонуються в цьому стандарті, можуть застосовуватися як

керівні принципи для менеджменту інформаційної безпеки, і підходять більшості організацій.

Не всі засоби управління і рекомендації даного зводу правил можуть бути застосовними. Крім того, можуть знадобитися додаткові засоби управління і керівні вказівки, що не включені в цей стандарт [12].

Загалом, стандарт містить рекомендації для стандартів по інформаційної безпеки організацій і способи практичного застосування менеджменту інформаційної безпеки, включно з вибором, впровадженням та здійсненням засобів управління, що враховують ризики інформаційної безпеки організації, створювані її оточенням.

Стандарт розроблений для застосування організаціями, які мають намір [12, 13]:

- а) вибрати засоби управління в рамках процесу впровадження системи менеджменту інформаційної безпеки, заснованої на ISO 27001;
- б) використовувати загальноприйняті засоби управління інформаційною безпекою;
- с) розробити свої власні керівні матеріали з менеджменту інформаційної безпеки.

Загалом стандарт в 14 розділах містить опис 114 засобів управління, розділених на 35 основних категорій. Засоби управління, які описуються в кожному розділі, можуть відноситись до однієї чи більше основної категорії, а опис засобів структуровано в: метод реалізації, рекомендації по застосуванню, додаткову інформацію. В залежності від обставин засоби управління із одного або всіх розділів можуть стати важливими, відповідно, організація, застосовуючи стандарт, повинна визначати підходящі засоби управління у відповідності до їх значимості і їх використанням у конкретних бізнес-процесах [12].

Розділи стандарту включають наступні:

- Політики інформаційної безпеки
- Організація інформаційної безпеки
- Безпека персоналу

- Управління активами
- Контроль доступу
- Криптографія
- Фізичний захист та захист від зовнішніх впливів
- Безпека виробничої діяльності
- Безпека обміну інформацією
- Набуття, розробка та обслуговування систем
- Відношення з постачальниками
- Управління інцидентами інформаційної безпеки
- Аспекти інформаційної безпеки в менеджменті неперервності бізнесу
- Відповідність.

Таким чином, підхід до управління інформаційною безпекою визначається двома взаємопов'язаними стандартами – 27001, 27002, де перший стандарт грає основну роль та містить рекомендації по менеджменту ІБ в організації на основі широко використовуваного в корпоративному середовищі циклу управління якістю PDCA (Plan, Do, Check, Act), а другий стандарт носить довідковий характер, описуючи набір можливих заходів захисту інформації, з яких організація може вибрати необхідні саме їй. Управління ІБ, відповідно до вищезгаданих стандартів може бути представлене за допомогою наступної схеми:

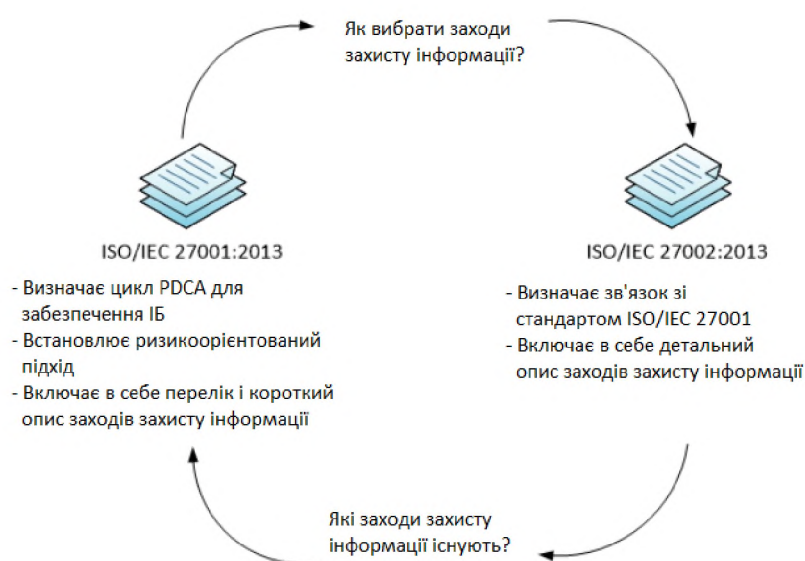


Рисунок 2.1 – Управління ІБ згідно ISO 27001 та ISO 27002

2.1.3 ISO 27003

Стандарт (Методи і засоби забезпечення безпеки – Системи менеджменту інформаційної безпеки – Керівництво по реалізації системи менеджменту інформаційної безпеки) розглядає найважливіші аспекти, необхідні для успішної розробки і впровадження системи менеджменту ІБ відповідно до стандарту ISO 27001 [14]. В ньому описується процес визначення і розробки СУІБ від запуску до створення планів впровадження. Також описується процес отримання схвалення керівництвом впровадження СУІБ, визначається проект впровадження СУІБ і представлені рекомендації по плануванню проекту СУІБ, в результаті якого отримується остаточний план впровадження СУІБ. Стандарт застосовується до всіх типів організацій. Складність структури і ризику кожної організації унікальні, і на впровадження СУІБ будуть впливати її особливі вимоги. Для невеликих організацій дії, указані в стандарті, можуть бути спрощені. Для великих організацій чи організацій зі складною структурою для ефективного виконання дій, вказаних у стандарті, може знадобитися багаторівнева система організації чи управління. Стандарт містить рекомендації та пояснення, в ньому не вказано ніяких вимог, та призначений для використання в поєднанні із стандартами ISO 27001, ISO 27002 [14].

В стандарті пояснюється впровадження СУІБ з детальним описом запуску, планування і визначення проекту. Процес планування кінцевого впровадження СУІБ включає 5 фаз, і кожна фаза представлена в окремому пункті. До фаз належать наступні [14]:

- Отримання схвалення керівництва для запуску проекту СУІБ
- Визначення області дії та політики СУІБ
- Проведення аналізу організації
- Проведення аналізу ризиків і планування обробки ризиків
- Розробка СУІБ

Усі фази планування проекту СУІБ зі вказанням стандартів ISO і основних вихідних документів можуть бути представлені у вигляді наступної схеми [14]:

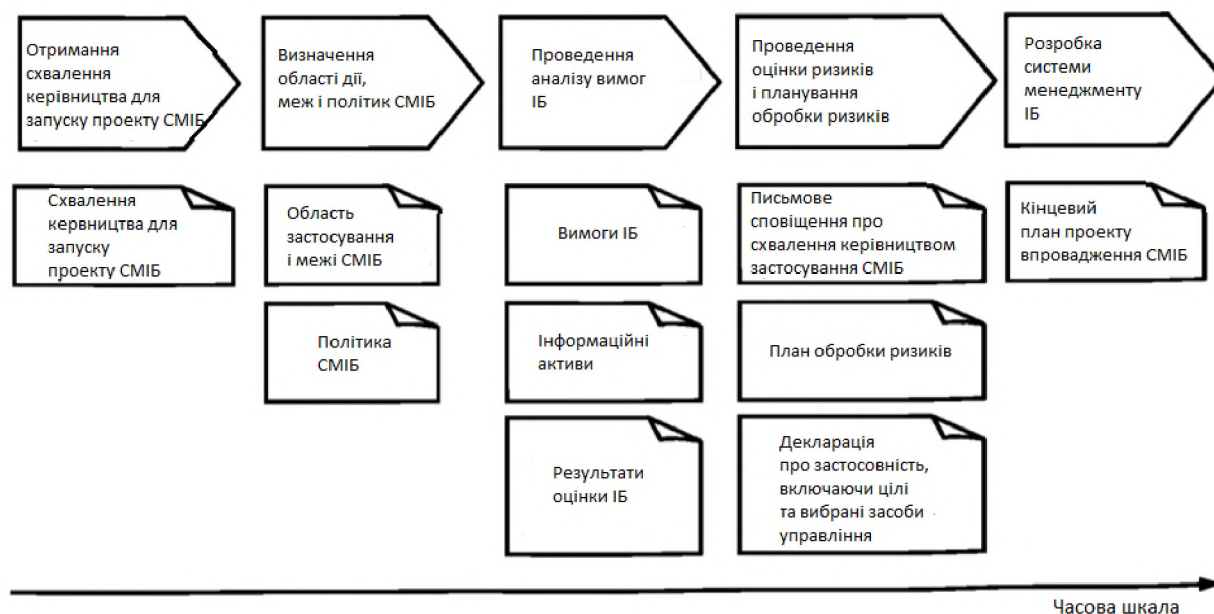


Рисунок 2.2 – Фази проекту СУІБ згідно ISO 27003

Важливими додатками стандарту є:

- Ролі та сфери відповідальності в області ІБ, де містяться додаткові рекомендації по ролям і сферам відповідальності в організації, пов'язаним з ІБ – ролі комітету по ІБ, ролі групи по плануванню ІБ, спеціалістів та зовнішніх консультантів, володільців інформаційних активів
- Інформація по внутрішньому аудиту, де містяться додаткові рекомендації по плануванню аудиту
- Структура політики, де містяться додаткові рекомендації по структурі політики, включаючи політику інформаційної безпеки
- Моніторинг і вимірювання, де представлені рекомендації по підтримці планування і розробки моніторингу та змін.

Моніторинг і вимірювання згідно ISO 27003. Модель послідовності процесу моніторингу може бути представлена у вигляді наступної схеми [14]:

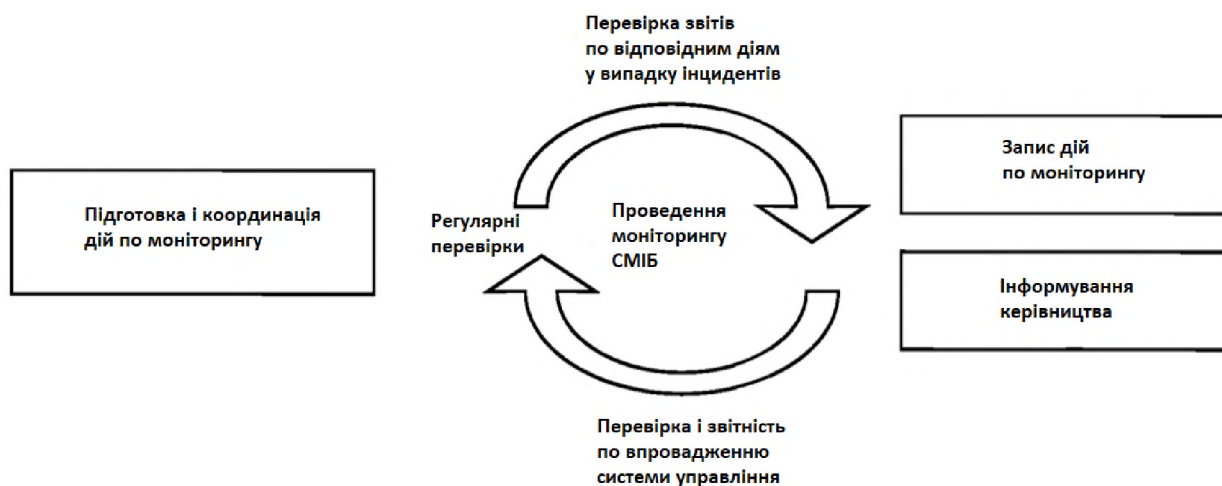


Рисунок 2.3 – Послідовність процесу моніторингу згідно ISO 27003

Розробка моніторингу. Моніторинг є неперервним процесом, і при його розробці необхідно враховувати наладку процесу моніторингу, а також розробку фактичних потреб та дій по моніторингу. Ці дії необхідно координувати, що є частиною процесу розробки. На основі інформації, встановленої на основі визначеної області дій та активів, в поєднанні з результатами аналізу ризику і вибору засобів управління можна визначити цілі моніторингу, які повинні включати: 1) що потрібно визначити, 2) коли, 3) проти чого. Для забезпечення реальної ефективності моніторингу важливо координувати і проводити кінцеву розробку всіх дій по моніторингу [14].

Дії по моніторингу. Для підтримки рівня ІБ, заходи і засоби контролю та управління ІБ, визначені як підходящі, повинні правильно застосовуватись; виявлення інцидентів безпеки і реагування на них повинні проводитись своєчасно, а функціонування системи менеджменту ІБ повинно регулярно відслідковуватись. Необхідно проводити регулярні перевірки, щоб визначити, чи всі заходи і засоби контролю та управління застосовуються і впроваджуються, як заплановано в концепції ІБ. В число таких перевірок повинні входити перевірки відповідності технічних засобів управління (наприклад, по відношенню до конфігурації) і організаційних засобів управління (наприклад, процесів, процедур і операцій) [14]. Дії по розробці можна заключити в 3 основні форми [14]:

- Звіти про інциденти

- Підтвердження відповідності або невідповідності функціональності засобів управління
- Інші регулярні перевірки

Результати моніторингу повинні бути наступними [14]:

- Записи дій по моніторингу з необхідним ступенем деталізації. По результатам дій по моніторингу повинен бути наданий звіт
- Інформація, яка необхідна керівництву для прийняття рішень, коли це вимагається для прийняття термінових заходів.

Процес вимірювання повинен бути плавно введений в цикл СУІБ проекту або організації і використовуватись для неперервного вдосконалення процесів, пов'язаних з безпекою, і результатів в рамках цього процесу або організації. Це називається програмою вимірювання інформаційної безпеки. Програма вимірювання ІБ затверджується для того, щоб отримати показники ефективності СУІБ, цілей і засобів управління. Описується в стандарті ISO 27004.

Розробку програми необхідно розглядати у відношенні циклу СУІБ. Для проведення правильних вимірювань, необхідна раніше отримана інформація, особливо [14]:

- Політики СУІБ, включаючи область дії та межі
- Результати оцінки ризику
- Вибір засобів управління
- Цілі управління
- Конкретні цілі ІБ
- Задані процеси і ресурси та їх класифікація

Програма вимірювання ІБ та її розробка мають на увазі наступні ролі:

- Вище керівництво
- Користувачі програмних продуктів, пов'язаних із безпекою
- Особи, які відповідають за інформаційні системи
- Особи, які відповідають за інформаційну безпеку

Підходящі програми вимірювання ІБ можуть відрізнятись в залежності від структури організації, а саме:

- Розміру
- Складності
- Загального профілю ризику в ІБ.

Область дії програми вимірювання повинна охоплювати область дії, цілі управління і заходи та засоби контролю і управління СУІБ. Цілі і межі вимірювання СУІБ повинні встановлюватись по відношенню характеристики організації, самої організації, її місцезнаходження, активів і технологій та включати деталізацію і пояснення будь-яких виключень із області дії СУІБ. Це може бути один із засобів управління безпекою, процес, система, область діяльності, ціле підприємство, один підрозділ або організація, яка складається із декількох підрозділів [14].

При виборі одиночного вимірювання стандарт ISO 27004 вимагає, щоб початковою точкою виступав об'єкт вимірювання. Для утвердження програми вимірювань необхідно визначити ці об'єкти. Цими об'єктами можуть бути процеси або ресурси. Фактично проведення вимірювань може відбуватись співробітниками організації, спеціалістами зі сторони або одним та іншими разом. Розміри, структура та культура організації – це фактори, які необхідно брати до уваги при оцінці внутрішніх чи зовнішніх ресурсів. Малі та середні компанії мають великі вигоди від використання підтримки зі сторони, ніж більші організації. Результати використання зовнішніх ресурсів можуть також забезпечити більш надійні результати в залежності від культури організації. Якщо в організації постійно проводиться внутрішній аудит, внутрішня перевірка може принести більш надійні результати.

2.1.4 ISO 27004

Стандарт (Методи і засоби забезпечення безпеки – Менеджмент інформаційної безпеки – Вимірювання) містить рекомендації по розробці і використанню вимірювань та мір вимірювання для проведення оцінки ефективності реалізованої системи менеджменту ІБ, а також мір та засобів контролю і управління або їх груп згідно ISO 27001 [15]. Процес вимірювань

охоплює політику, менеджмент ризику ІБ, міри та засоби контролю і управління та цілі їх застосування, процесі і процедури, а також підтримка процесу перевірки СУІБ, для визначення, чи необхідно змінювати чи вдосконалювати які-небудь із процесів чи заходів контролю і управління СУІБ. Хоча, ніякі вимірювання мір та засобів контролю та управління не можуть забезпечити повної безпеки [15].

Процес вимірювань реалізується у вигляді програми вимірювань, пов'язаних з ІБ. Програма вимірювань призначена для надання допомоги керівництву організації у виявленні та оцінці невідповідних вимогам та неефективних процесів, заходів, засобів контролю і управління СУІБ, а також у визначенні пріоритетів дій, направлених на вдосконалення чи зміну цих процесів і (або) мір та засобів контролю та управління. Програма вимірювань також може допомогти організації в демонстрації відповідності СУІБ вимогам ISO 27001 і створенню додаткової основи для проведення керівництвом організації перевірки процесів менеджменту ризику ІБ [15].

Програма вимірювань допоможе організації в наданні відповідним зацікавленим сторонам достовірної інформації, яка стосується ризиків ІБ і стану реалізованої СУІБ для управління цими ризиками.

Ефективно реалізована програма вимірювань дозволить укріпити довіру зацікавлених сторін до результатів вимірювань, а також дасть можливість зацікавленим сторонам застосовувати міри вимірювань для неперервного вдосконалення ІБ і СУІБ. Накопичені результати вимірювань дозволять слідкувати за прогресом в досягненні цілей ІБ за деякий період часу в інтересах реалізації процесу неперервного вдосконалення СУІБ організації [15].

Підхід, прийнятий організацією для виконання вимог до вимірювань, визначених в ISO 27001, буде варіюватись в залежності від ряду суттєвих факторів, які включають в себе ризики ІБ, з якими стикається організація, розмір організації, наявних ресурсів та застосовних правових, нормативних і договірних вимог. Поточна діяльність, пов'язана з постійними вимірюваннями, повинна бути інтегрована в звичайну діяльність організації з заохоченням мінімальних додаткових ресурсів.

Стандарт пропонує рекомендації, які стосуються наступної діяльності, яка є основою для виконання організацією вимог до вимірювань, встановлених в ISO 27001 [15, 16]:

- Розробка мір вимірювань (основні міри, похідні міри і показники)
- Розробка і виконання програми вимірювань
- Збір та аналіз даних
- Обробка результатів вимірювань
- Донесення оброблених результатів вимірювань зацікавленим сторонам
- Використання результатів вимірювань для виявлення потреб у вдосконаленні реалізованої СУІБ, включаючи її область дії, політики, цілі, міри і засоби контролю і управління, процеси і процедури
- Сприяння постійному вдосконаленню програми вимірювань

Структура стандарту включає:

- Загальний огляд програми вимірювань і моделі вимірювань, пов'язаних з ІБ (в загальному- модель вимірювань)
- Обов'язки керівництва по відношенню до вимірювань, пов'язаних з ІБ
- Конструктивні елементи та процеси вимірювань, які підлягають реалізації в рамках програми вимірювань.

Розглянемо модель вимірювань, пов'язаних з ІБ, згідно стандарту, детальніше.

Цілі вимірювань, пов'язаних з ІБ, в контексті СУІБ, включають в себе [15]:

- Оцінювання ефективності реалізованих мір і засобів контролю та управління або їх груп
- Оцінювання ефективності реалізованої СУІБ
- Верифікація степені, до якої були задоволені встановлені вимоги безпеки
- Сприяння підвищенню результативності ІБ з точки зору загальних ризиків основної діяльності організації
- Представлення відомостей для перевірки, яка проводиться керівництвом з ціллю сприяння прийняття рішень, які стосуються СУІБ, і обґрунтування необхідних вдосконалень в реалізованій СУІБ.

Циклічний взаємозв'язок видів діяльності, пов'язаних з вимірюваннями, по відношенню до циклу “планування – здійснення – перевірка - дія”, визначеному в ISO 27001, вказано на зображенні нижче [15]:

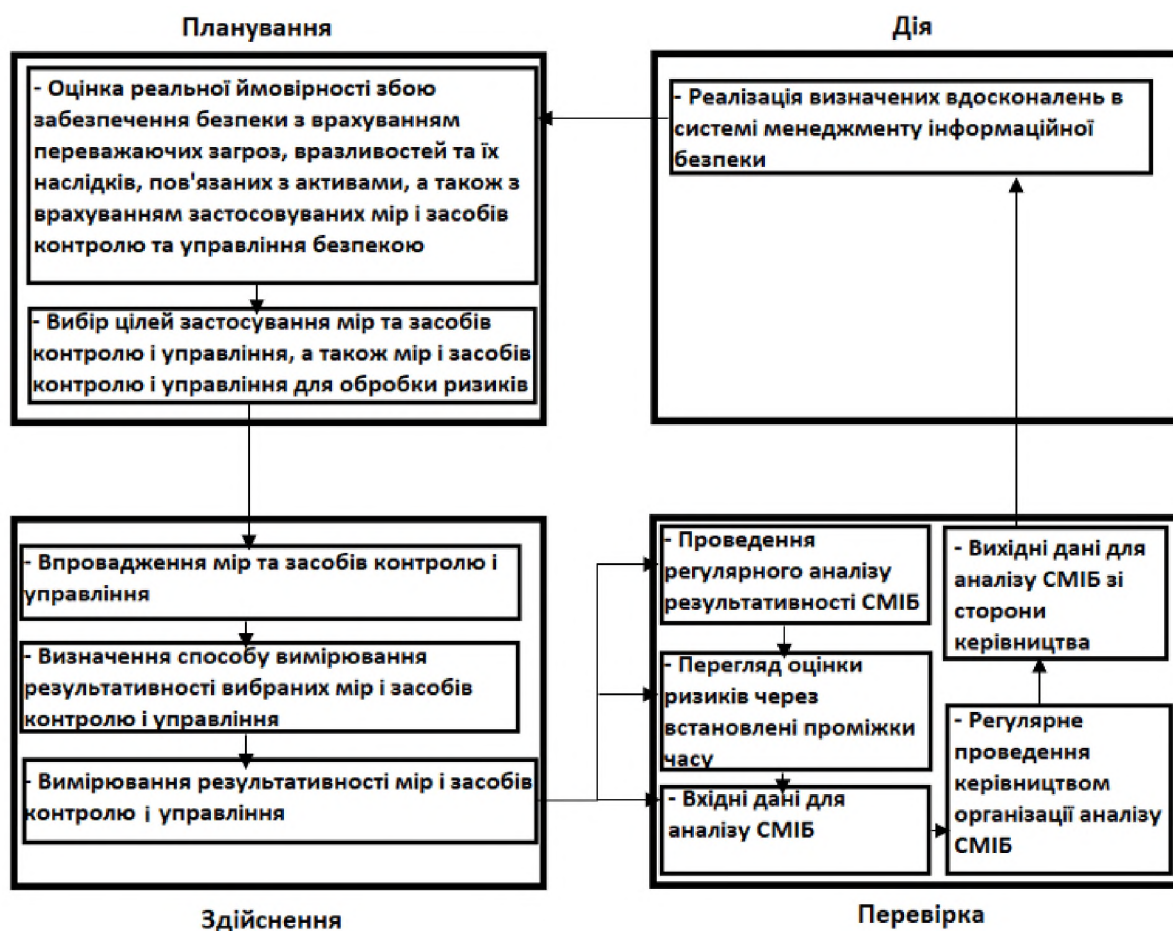


Рисунок 2.4 – Взаємозв'язок видів діяльності, пов'язаних з вимірюваннями, в циклі “планування – здійснення – перевірка - дія”

Програма вимірювань. Організації необхідно створити програму вимірювань і управляти нею для досягнення встановлених цілей вимірювань та впровадження моделі PDCA в масштабах усієї вимірювальної діяльності організації [15, 16].

Програма вимірювань і розроблені конструктивні елементи вимірювань повинні забезпечувати ефективне налагодження організацією об'єктивних та повторюваних процесів вимірювання, а також надання результатів вимірювань відповідним зацікавленим сторонам для визначення потреб у вдосконаленні реалізованої СУІБ, включаючи область її застосування, політики, цілі, міри і засоби контролю та управління, а також процеси і процедури.

Програма вимірювань повинна включати в себе наступні процеси [15]:

- Розробка вимірювань і мір вимірювань
- Проведення вимірювань
- Аналіз даних і розповсюдження результатів вимірювань
- Оцінювання і вдосконалення програми вимірювань, пов'язаних з ІБ.

Модель вимірювань. Модель вимірювань представляє собою структуру, яка пов'язує інформаційну потребу з відповідними об'єктами вимірювань та їх атрибутами. В число об'єктів можуть входити процеси, що плануються, реалізовані процеси, процедури, проекти та ресурси.

Модель вимірювань описує, як відповідні атрибути кількісно оцінюються і перетворюються в показники, які служать основою для прийняття рішень. Модель вимірювань може бути представлена за допомогою наступної схеми [15]:



Рисунок 2.5 – Модель вимірювань згідно ISO 27004

Основна міра вимірювання є найпростішою мірою, яка може бути отримана. Основна міра вимірювання є результатом застосування методу вимірювань до

вибраних атрибутів об'єкту вимірювання. У об'єкта вимірювання може бути велика кількість атрибутів, але лише деякі із них можуть надавати корисні значення, які можуть бути присвоєні основні мірі вимірювання. Один і той же атрибут може використовуватись для декількох різних основних мір вимірювань.

Метод вимірювань – логічна послідовність операцій, які використовуються для кількісної оцінки атрибуту по відношенню до заданої шкали. Операція може включати в себе такі дії, як підрахунок подій або спостереження за ходом часу. Метод вимірювань повинен бути заснований на атрибутах об'єкту вимірювань. Метод вимірювань може використовувати об'єкти вимірювань і атрибути із різних джерел, таких як [15]:

- Результати аналізу ризику і оцінки ризику
- Анкети та особисті бесіди
- Звіти про внутрішні і/або зовнішні аудити
- Документовану інформацію про події, наприклад, протоколи, статистичні дані звітів і журнали реєстрації
- Повідомлення про інциденти, особливо ті, внаслідок яких був спричинений збиток
- Результати тестування, наприклад, отримані в результаті тестування на проникнення, використання соціальної інженерії, інструментальних засобів забезпечення відповідності, а також інструментальних засобів аудиту безпеки
- Документовану інформацію, отриману із процедур і програм організації, пов'язаних з забезпеченням ІБ, наприклад, результати програм навчання, направлених на підвищення обізнаності про ІБ

Похідна міра вимірювання є комбінацією двою або більше основних мір вимірювання. Основна міра вимірювання може служити в якості вхідних даних для декількох похідних мір вимірювання.

Функцією вимірювання є обчислення, яке використовується для комбінування основних мір вимірювання, з ціллю отримання похідної міри вимірювання.

Шкала і одиниця вимірювання похідної міри вимірювання залежать від шкал і одиниць вимірювання основних мір вимірювання, на основі яких вона отримана, а також того, як вони комбінувались функцією вимірювання.

Показник є мірою, яка дає якісну та кількісну оцінку визначених атрибутів, отриману на основі аналітичної моделі по відношенню визначеної інформаційної потреби. Показники отримуються шляхом застосування аналітичної моделі до основної або похідної міри вимірювань і комбінування їх із застосуванням критеріїв прийняття рішень. Шкала і метод вимірювання впливають на вибір аналітичних методів, які використовуються для отримання показників.

Результати вимірювань формуються шляхом інтерпретації застосовних показників на основі визначених критеріїв прийняття рішень і повинні розглядатись в контексті загальних цілей вимірювання ефективності СУІБ. Критерії прийняття рішень використовуються для того, щоб визначити необхідність дії чи подальшого дослідження і характеризувати ступінь впевненості в результатах вимірювання. Критерії прийняття рішень можуть застосовуватись для ряду показників, наприклад, для проведення аналізу трендів на основі показників, отриманих в різні моменти часу.

Цільові значення задають деталізовані вимоги результативності, які застосовні до організації або її частин, виведені із цілей ІБ, таких як цілі СУІБ і цілі застосування мір і засобів контролю і управління, які повинні бути встановлені і виконані для досягнення цих цілей.

Якщо підсумувати усі вищенаведені розділи та тези стандарту – то вищенаведена серія стандартів перевантажена загальними рекомендаціями, а моделі можуть застосовуватись без спеціалізованих термінів та надлишкових логічних структур. Крім того серія стандартів ISO 27000 орієнтована на забезпечення загальної відповідності організації вимогам стандартів, наприклад для сертифікації організації згідно ISO 27000. Тобто питання відповідності організації згідно стандарту є невирішеним у випадку, коли стоїть ціль обрати набір методів та засобів, які будуть підходити саме для обраного середовища.

2.2 Стандарт COBIT

Стандарт COBIT (Розшифровується як “Задачі управління для інформаційних та суміжних технологій”) – підхід до управління інформаційними технологіями, створений Асоціацією контролю і аудиту систем та Інститутом керівництва інформаційними технологіями. Він надає менеджерам, аудиторам і користувачам інформаційних технологій набір затверджених метрик, процесів та практик з метою допомогти їм в отриманні максимальної вигоди від використання інформаційних технологій і для розробки відповідного керівництва та контролю ІТ в компанії. Є своєрідною основою для допомоги персоналу в області ІБ в розробці та реалізації стратегій управління інформацією та управління нею, при мінімізації негативних впливів і контролю ІБ та управління ризиками.

Концептуальним ядром COBIT (або фреймворком) є набір основних принципів і понять, високорівневих задач управління, а також модель управління ІТ, на базі яких будуються всі положення COBIT [17].

Основне положення стандарту – ресурси інформаційних систем управляються набором природньо згрупованих процесів для забезпечення організації необхідної та надійної інформації [18].

Розглянемо основні особливості та класифікацію факторів стандарту, в контексті яких і визначається управління ІБ. Фактори COBIT включають 7 основних категорій:

- Принципи, політики та фреймворки – рушійні сили для переведення бажаної поведінки в практичне керівництво для щоденного управління
- Процеси – описують організовану множину практик та активностей для досягнення конкретних цілей і вироблення множини виходів для підтримки досягнення загальних цілей, пов’язаних з інформаційними технологіями
- Організаційні структури – ключові суб’єкти, що приймають рішення в організації

- Культура, етика та поведінка – поняття, що відносяться як до індивідів так і до організації; часто недооцінені як успішний фактор в керівництві та управлінні активностями
- Інформація – поширювана всередині будь-якої організації. Необхідна для постійної, добре керованої роботи організації
- Сервіси, інфраструктура та застосунки – фактор, що включає інфраструктуру, технології та застосунки, що забезпечують організацію сервісами та обробкою інформаційних технологій
- Персонал, навички та компетенції – фактор, прив'язаний до людей. Необхідний для успішного завершення усіх активностей, а також для прийняття коректних рішень та виконання правильних дій

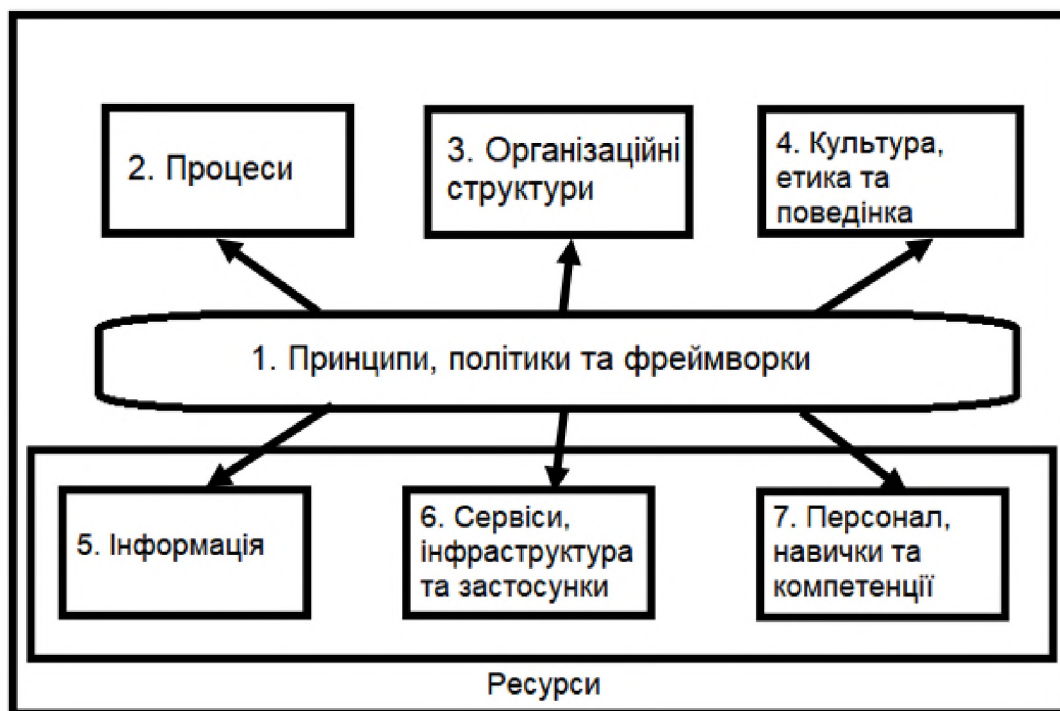


Рисунок 2.6 – Фактори стандарту COBIT

Для досягнення основних цілей організації, завжди повинна враховуватись взаємопов'язана множина факторів. Кожен фактор:

- Потребує входу інших факторів для того, щоб бути повністю ефективним. Наприклад, процеси потребують інформацію, а навички та поведінка роблять процес ефективним

- Доставляє власний вихід для переваг інших факторів. Наприклад, процеси доставляють інформацію, а навички та поведінка роблять процеси ефективними

Систематичне керівництво та управління через взаємопов'язані фактори – ключовий принцип навколо бізнес-моделі для інформаційної безпеки.

Усі фактори мають загальні розмірності. Ця множина загальних розмірностей:

- Забезпечує загальний, простий та структурований шлях взаємодії з факторами
- Дозволяє суб'єкту управляти комплексними взаємодіями
- Сприяє успішним результатам факторів

2.2.1 Управління інформаційними технологіями та інформаційною безпекою в контексті стандарту COBIT

Згідно стандарту COBIT, інформаційна безпека визначена наступним чином:

- ІБ забезпечує те, що всередині організації, інформація захищена від розкриття неавторизованим користувачам (конфіденційність), неналежної модифікації (цілісність) та недоступності, коли вона необхідна (доступність).
 - Конфіденційність визначається як збереження дозволених обмежень на доступ та розкриття інформації, включаючи засоби захисту приватності та приватної інформації
 - Цілісність визначається як захист від неналежної зміни чи знищення інформації та включає в себе забезпечення достовірності, достовірності та невідмовності
 - Доступність визначається як забезпечення вчасного та надійного доступу та використання інформації [25].

Управління інформаційною безпекою в контексті стандарту пояснює кожний компонент з точки зору інформаційної безпеки та є розширеним видом стандарту. Дана категорія містить пояснення, щодо рушійних сил, переваг, принципів з точки зору інформаційної безпеки, факторів підтримки та співставлень із іншими стандартами.

Основні рушійні сили для розвитку стандарту для інформаційної безпеки включають:

- Необхідність опису інформаційної безпеки в контексті організації
- Підвищена необхідність для організацій в:
 - Збереженні ризику на прийнятних рівнях
 - Підтриманні доступності до систем та сервісів
 - Відповідності до актуальних законів та нормативних документів
- Необхідність поєднання та співставлення з іншими важливими стандартами та фреймворками

Реалізація інформаційної безпеки в контексті стандарту відбувається в межах всіх нижчезазначених факторів стандарту, описаних раніше:

- Політики, принципи та фреймворки
- Процеси
- Організаційні структури
- Культура, етика та поведінка
- Інформація
- Послуги, інфраструктура та застосунки
- Персонал, навички та компетенції

Розглянемо кожен фактор стандарту в контексті інформаційної безпеки.

- 1) **Принципи інформаційної безпеки** - пов'язують правила організації, виражені простою мовою. Всього асоціацією ISACA розроблено 12 принципів, які підтримують 3 основні завдання – підтримка бізнесу, захист бізнесу, та сприяння відповідальній поведінці щодо захисту інформації [23].

Розглянемо детальніше вищезгадані принципи, згруповані по трьом основним завданням :

- Підтримка бізнесу
 - Принцип 1. Фокусування на бізнесі.
 - Принцип 2. Забезпечення якості та цінності для зацікавлених сторін.
 - Принцип 3. Відповідність юридичним та нормативним вимогам.
 - Принцип 4. Своєчасна та точна інформація про ефективність інформаційної безпеки
 - Принцип 5. Оцінка поточних та майбутніх інформаційних загроз.
 - Принцип 6. Сприяння постійного вдосконалення в інформаційній безпеці.
- Захист бізнесу
 - Принцип 1. Адаптування ризикоорієнтованого підходу
 - Принцип 2. Захист класифікованої інформації.
 - Принцип 3. Концентрація на критичних бізнес-застосунках.
 - Принцип 4. Надійна розробка систем
- Сприяння надійній поведінці щодо інформаційної безпеки
 - Принцип 1. Діяти професійно та етично.
 - Принцип 2. Сприяння позитивній культурі безпеки [24].

2) **Політики інформаційної безпеки.** Включають в себе:

- Політику інформаційної безпеки
- Політику контролю доступу
- Політику безпеки персональної інформації
- Політику фізичної безпеки та безпеки середовища
- Політику управління інцидентами
- Політику неперервності бізнесу і відновлення після збоїв
- Політику управління активами
- Політика набуття, розробки та обслуговування ПЗ
- Політика управління постачальниками
- Політика управління комунікаціями та експлуатацією
- Політика відповідності

- Політика управління ризиками [25]

3) **Процеси інформаційної безпеки.** Концептуальне ядро стандарту сформовано з 37 високорівневих процесів (які покривають близько 300 об'єктів контролю), згрупованих в 5 сфер діяльності.

Стандарт визначає еталонну модель процесу, яка складається з двох доменів: домену керівництва, та домену управління [25].

Домен керівництва забезпечує впевненість в досягненні цілей організації шляхом:

- Збалансованої оцінки потреб зацікавлених сторін, існуючих умов і можливих варіантів
- Встановлення напрямку розвитку через пріоритизацію і прийняття рішень
- Постійного моніторингу відповідності фактичній продуктивності і степені виконання вимог, встановленим напрямку та цілям організації.

Домен управління полягає в плануванні, побудові, виконанні і відслідковуванні діяльності, у відповідності до напрямку, заданого органом керівництва, для досягнення цілей організації [26].

Домен управління включає наступні сфери діяльності:

1. Забезпечення відповідності, планування та організація. Включає стратегію та тактику, а також визначення способів найбільш ефективного використання інформаційних технологій для досягнення бізнес-цілей. Основна роль сфери діяльності – стратегічна.
2. Створення, набуття та впровадження. Для реалізації стратегії ІТ потрібно ідентифікувати, розробити чи набути відповідні ІТ рішення, які повинні бути впроваджені та інтегровані в бізнес-процеси, а також внести зміни в інформаційні системи. Основна роль сфери діяльності – тактична.
3. Обслуговування, експлуатація та супровід. Включає надання необхідних інформаційних служб, в тому числі забезпечення безпеки та неперервності бізнесу, навчання, а також обробку даних прикладними системами. Основна роль сфери діяльності – операційна.

4. Моніторинг, вимірювання та оцінка. Якість та відповідність ІТ процесів вимогам контролю повинні оцінюватись на регулярній основі. Ця сфера діяльності включає в себе нагляд зі сторони керівництва за процесами управління в організації, а також незалежний контроль зі сторони внутрішніх та зовнішніх аудиторів. Основна роль сфери діяльності – звітність.

Домен керівництва включає оцінку, управління та відслідковування. Основна роль домену – керівництво [17, 19, 20, 21, 22]

Відповідно до стандарту, для кожного процесу задано призначення та описання, цілі та метрики процесу, входи та виходи, а також рекомендації.

Стандартом передбачена також оцінка процесу на основі моделі можливостей процесу, згідно якої процеси поділяються на 6 рівнів:

0. Неповний процес. Такий процес ще не впроваджений чи не здатний відповідати своєму призначенню. На цьому рівні відсутні ознаки систематичного досягнення процесом своїх цілей, або таких ознак мало.
1. Здійснений процес. Процес впроваджений та відповідає своєму призначенню.
2. Керований процес. Здійснений процес попереднього рівня тепер керований (планується, відслідковується та коректується). Створюються, контролюються та підтримуються робочі продукти процесу.
3. Встановлений процес. Керований процес попереднього рівня тепер має змогу отримувати очікувані результати.
4. Передбачуваний процес. Встановлений процес попереднього рівня тепер отримує результати в умовах заданих обмежень.
5. Оптимізований процес. Передбачуваний процес попереднього рівня тепер постійно вдосконалюється, щоб забезпечити досягнення поточних та майбутніх цілей організації [26].

Вищенаведена структура стандарту охоплює усі аспекти управління та використання ІТ. Виконання усіх 37 високорівневих процесів дозволяє

гарантувати володільцю бізнес-процесу, що система керування ІТ є адекватною, по відношенню до задач бізнесу [17].

4) **Організаційні структури.** Важливим організаційним елементом в ІБ – це ролі. Згідно стандарту, виділяються наступні основні ролі:

- Головний співробітник інформаційної безпеки
- Керуючий комітет з інформаційної безпеки
- Менеджер інформаційної безпеки
- Комітет по управлінню ризиками організації
- Володільці інформації/володільці бізнесу

5) **Культура, етика та поведінка.** Даний фактор включає наступні пункти:

- Співробітники застосовують підходи інформаційної безпеки в повсякденному житті
- Співробітники розуміють важливість політик і принципів ІБ
- Співробітники забезпечені необхідними матеріалами та найкращими практиками по ІБ і заохочуються до участі при вирішенні питань, пов'язаних з ІБ
- Кожен співробітник несе відповідальність за ІБ в організації
- Зацікавлені сторони обізнані щодо наявності загроз ІБ і визначають підхід до реагування на них
- Керівництво активно підтримує розвиток ІБ
- Керівники підрозділів забезпечують ефективні комунікації між відділами при вирішенні задач ІБ
- Вище керівництво визнає цінність ІБ для бізнесу

6) **Інформація.** В контексті стандарту інформація не тільки основний суб'єкт, але й ключовий фактор. Типи відповідної інформації в контексті інформаційної безпеки включають:

- Стратегія інформаційної безпеки
- Бюджет інформаційної безпеки
- План інформаційної безпеки
- Політики

- Вимоги до інформаційної безпеки, які можуть включати:
 - Вимоги до конфігурації інформаційної безпеки
 - Вимоги щодо захисту інформації
- Інформаційний матеріал
- Каталог послуг інформаційної безпеки
- Профіль інформаційного ризику, який включає:
 - Реєстр інформаційних ризиків
 - Звіти про порушення та збитки
- Звіти з огляду інформаційної безпеки, які включають:
 - Результати аудиту інформаційної безпеки
 - Управління ризиками, пов'язаними з інформаційною безпекою
- Аналіз загроз
- Звіт про оцінку вразливостей інформаційної безпеки
- Інформаційна панель інформаційної безпеки, яка включає:
 - Інциденти інформаційної безпеки
 - Проблеми інформаційної безпеки
 - Метрики інформаційної безпеки

7) Послуги, інфраструктура та застосунки

В контексті стандарту визначені наступні послуги безпеки:

- Забезпечення архітектури безпеки
- Забезпечення обізнаності в безпеці
- Забезпечення безпечної розробки (розробка відповідно до стандартів безпеки)
- Забезпечення оцінки безпеки
- Забезпечення адекватно захищених та налаштованих систем відповідно до вимог та архітектури безпеки
- Забезпечення доступу користувачів та прав доступу відповідно до вимог використання
- Забезпечення адекватного захисту від шкідливого ПЗ, зовнішніх атак та спроб вторгнення

- Забезпечення адекватної реакції на інциденти
- Забезпечення тестування безпеки
- Надання послуг з моніторингу та оповіщення щодо подій, пов'язаних із безпекою

8) Персонал, навички та компетенції

Згідно стандарту, виділяються такі компетенції в інформаційній безпеці:

- Керівництво інформаційної безпеки
- Розробка стратегії інформаційної безпеки
- Управління ризиками інформаційної безпеки
- Розробка архітектури інформаційної безпеки
- Операційна діяльність в інформаційній безпеці
- Оцінка, перевірка стан і відповідність вимогам [26]

Реалізація факторів впливу залежить від особливостей всередині середовища організації, таких як:

- Етика та культура по відношенню до інформаційної безпеки
- Застосовні політики, нормативні та законодавчі акти
- Наявні ресурси та можливості інформаційної безпеки

Визначати вимоги до інформаційної безпеки організації необхідно на основі:

- Бізнес-плану та стратегічних намірів
- Стилю управління
- Профілю інформаційного ризику

Підхід до реалізації ініціатив інформаційної безпеки буде різний для кожної організації.

Деякі ключові моменти, щодо реалізації стандарту включають:

- Створення відповідного середовища
- Розпізнавання проблемних точок та генерація подій
- Дозвіл змін

- Впровадження практики захисту інформації – не разова подія, а життєвий цикл [23]

Основними перевагами у використанні стандарту COBIT в інформаційній безпеці є:

- Зменшена складність та підвищена економічна ефективність
- Вдосконалена інтеграція інформаційної безпеки
- Обізнаність та обгрунтовані рішення щодо ризиків
- Вдосконалене попередження, виявлення загроз та відновлення
- Зменшення впливу інцидентів безпеки
- Краще розуміння інформаційної безпеки в межах усієї організації [23]

2.3 Стандарт ITIL

Стандарт ITIL – сукупність концепцій, політик та передових методів для ефективного управління інфраструктурою, послугами та безпекою інформаційних технологій.

Згідно зі стандартом ITIL, IT-інфраструктура розглядається як комбінована множина апаратного та програмного забезпечення, мереж, а також усіх інформаційних технологій, для розробки, тестування, моніторингу, контролю та підтримки сервісів IT. ITIL – згруповані сервіси в сфері інформаційних технологій, які ще позначаються як управління сервісами IT. Стандарт надає широкий спектр процедур управління, які застосовні для усіх аспектів інфраструктури інформаційних технологій, за допомогою яких організація може управляти власними IT операціями [27].

ITIL не надає детального пояснення всіх аспектів управління інформаційною безпекою, оскільки існують спеціальні та більш детальні стандарти (наприклад, ISO 27001). ITIL висвітлює найважливіші види діяльності та допомагає визначити інтерфейси з іншими процесами управління сервісом [28].

Стандарт включає в себе 5 основних сервісів:

- Стратегія сервісу – описує, як проектувати, розробляти та реалізувати управління сервісом з точки зору стратегічних активів та здатностей організації
- Проектування сервісу – описує проектування та розробку процесів, управління процесом та як розробити проектні можливості для управління процесом. Він включає зміни та вдосконалення, необхідні для підвищення або підтримки цінності протягом життєвого циклу послуг, безперервності послуг, досягнень рівнів обслуговування та відповідності стандартам і нормам, та визначає, як організація розробляти проектні можливості для управління процесом
- Перехід сервісу – пояснює, як вдосконалювати можливості для переходу нових та змінених сервісів в операції. Він також надає рекомендації щодо того, як вимоги стратегії обслуговування, закованої в проекті сервісу, ефективно реалізуються під час експлуатації сервісу, контролюючи при цьому ризики відмови та зриву.
- Оперування сервісом
- Постійне вдосконалення процесу [27]

Життєвий цикл вищеписаних сервісів можна представити у вигляді схеми, наведеної нижче:

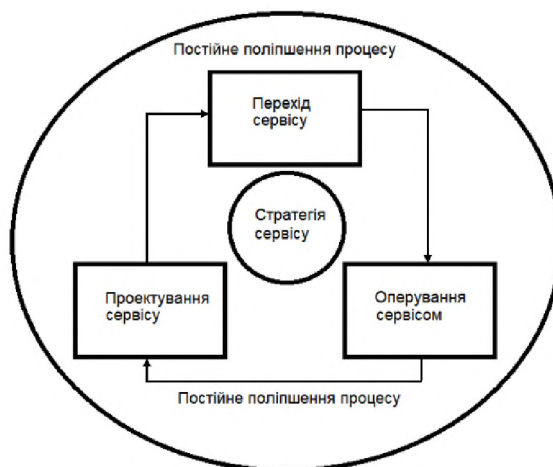


Рисунок 2.7 – Життєвий цикл сервісу в стандарті ІТІЛ

2.3.1 Управління інформаційною безпекою згідно ITIL

Управління безпекою за стандартом ITIL описує структуровану пристосованість інформаційної безпеки до організації та базується на стандарті ISO 27001.

Мета управління інформаційною безпекою полягає в тому, щоб зосередити увагу на всіх аспектах безпеки ІТ та керувати всіма діями ІТ-безпеки.

Управління інформаційною безпекою в рамках ITIL може допомогти організаціям оцінювати ризики та реагувати на інциденти. ITIL розмістив процес управління інформаційною безпекою в основній практиці проектування сервісу, де метою процесу управління інформаційною безпекою є узгодження ІТ-безпеки з безпекою бізнесу, забезпечення інформаційної безпеки в контексті безпеки бізнесу та забезпечення ефективного управління інформаційною безпекою у всіх послугах та діяльностях з управління сервісом.

Процес управління безпекою складається з активностей, які здійснюються самим управлінням безпеки, або активностей, які контролюється управлінням безпекою. Управління безпекою - це безперервний процес, і його можна порівняти з колом Демінга - Plan-Do-Check-Act (Плануй-Роби-Перевіряй-Дій), оскільки система управління інформаційною безпекою створюється за потреби організації [27].

Цілі управління безпекою згідно стандарту існують для забезпечення:

- Інформація є доступною та корисною, коли потрібна, і системи, які її надають, можуть відповідним чином протистояти атакам і відновлюватися після запобігання збоїв (або доступності)
- Інформація спостерігається або розголошується лише тим, хто має право знати (конфіденційність)
- Інформація повна, точна та захищена від несанкціонованих змін (цілісності)

- Ділові операції, а також обмін інформацією між підприємствами або з партнерами мають бути довіреними (достовірність та невідмова від авторства) [33]

Крім того, управління інформаційною безпекою розглядається не як бізнес-процес, а як стратегічний процес, який підтримує процеси до усіх інших процесів управління сервісами інформаційних технологій [30].

Основними елементами фреймворку управління інформаційною безпекою в контексті стандарту є:

- Керування – встановлення фреймворку для ініціалізації та управління інформаційною безпекою організації
- Планування – встановлення рекомендацій щодо відповідних вимірювань безпеки, побудованих на розумінні вимог організації
- Реалізація – забезпечення того, що необхідні процедури, інструменти та контролі існують для підтримки політики інформаційної безпеки
- Оцінювання – перевірка відповідності із політикою безпеки та вимогами безпеки; забезпечення регулярних аудитів технічної безпеки ІТ-систем
- Обслуговування – вдосконалення реалізації вмісту та вимірювань безпеки [27].

Елемент “Керування” можна представити у вигляді нижченаведеної схеми [29]:

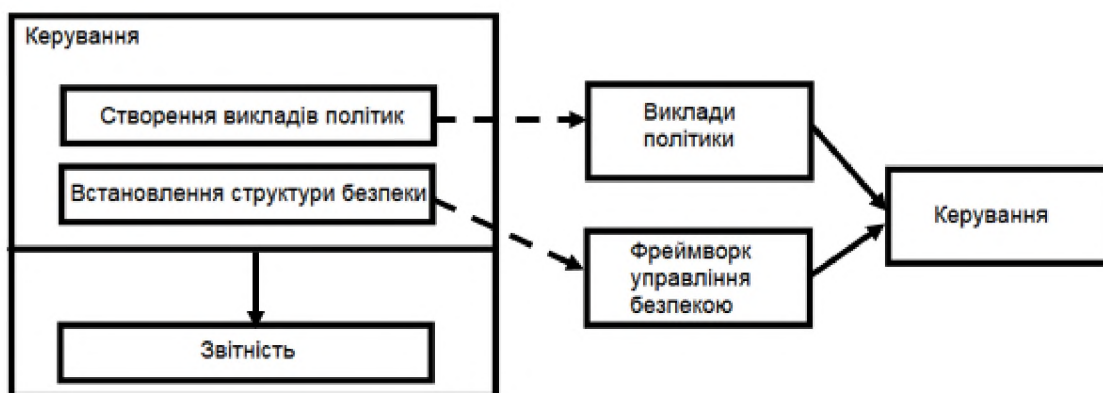


Рисунок 2.8 – Модель підпроцесу “Керування”

Елемент “Планування” можна представити у вигляді нижченаведеної схеми [29]:

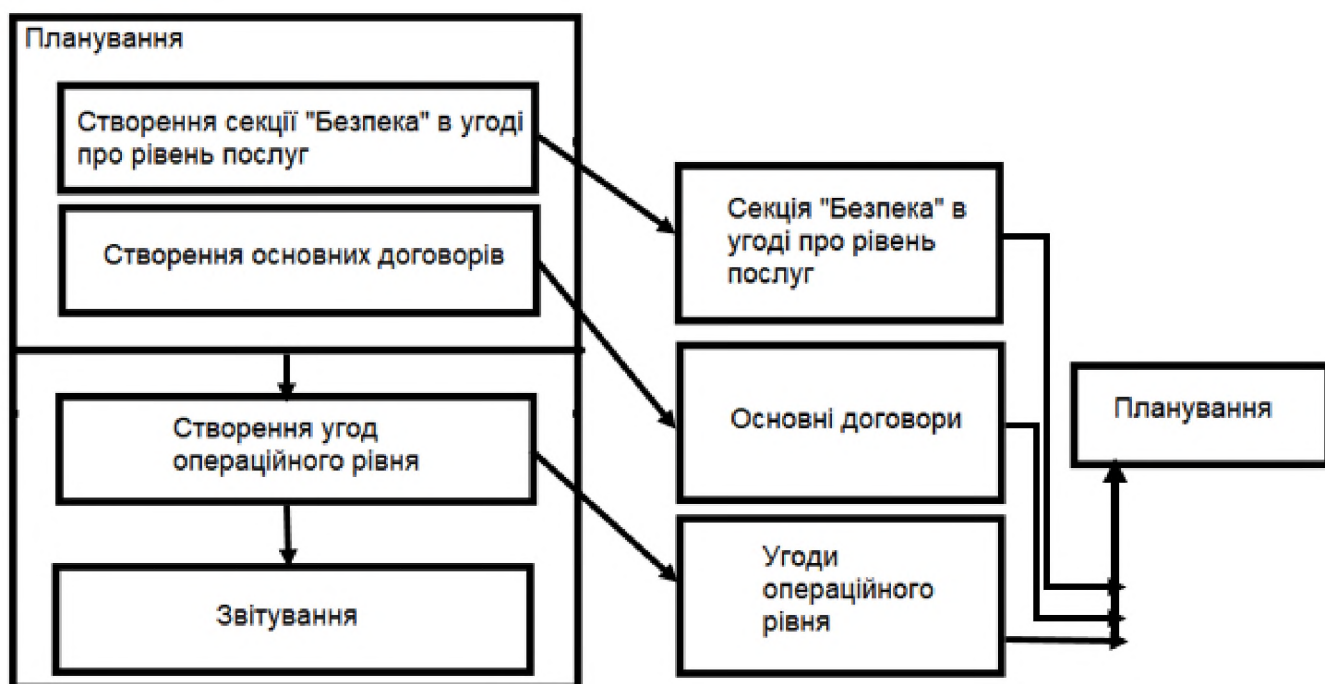


Рисунок 2.9 – Модель підпроцесу “Планування”

Елемент “Реалізація” можна представити у вигляді нижченаведеної схеми [29]:

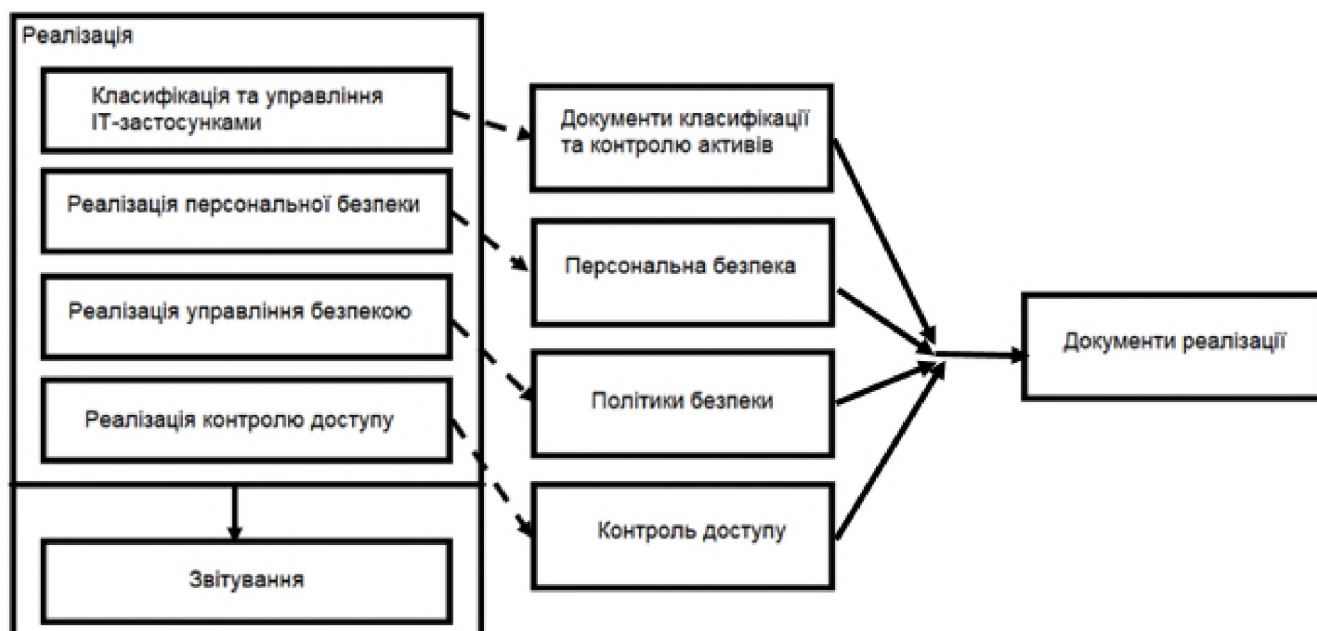


Рисунок 2.10 – Модель підпроцесу “Реалізація”

Елемент “Оцінювання” можна представити у вигляді нижченаведеної схеми [29]:

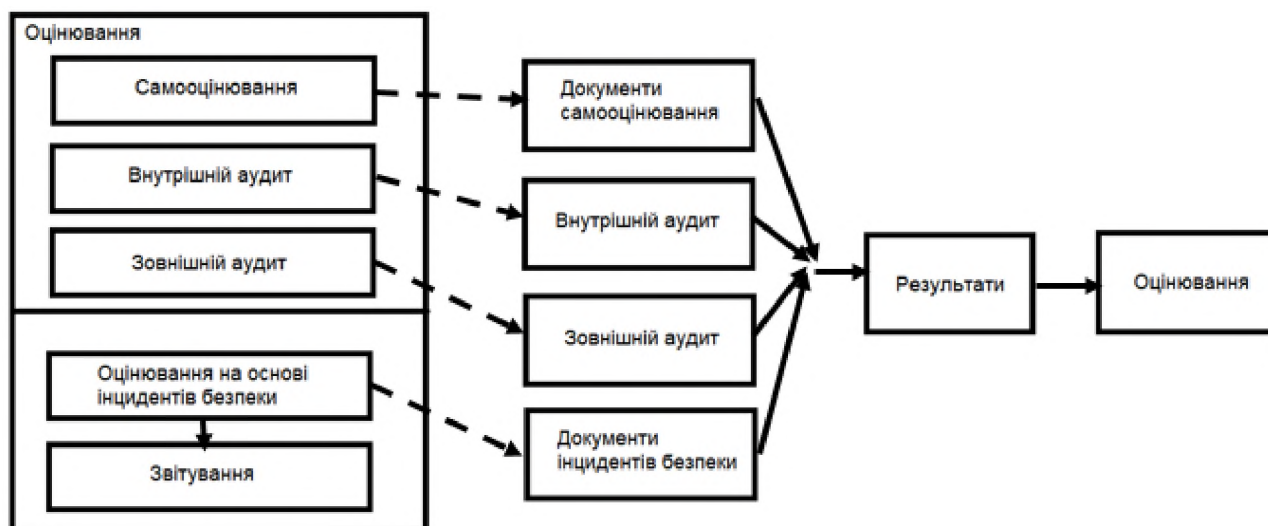


Рисунок 2.11 – Модель підпроцесу “Оцінювання”

Елемент “Обслуговування” можна представити у вигляді нижченаведеної схеми [29]:

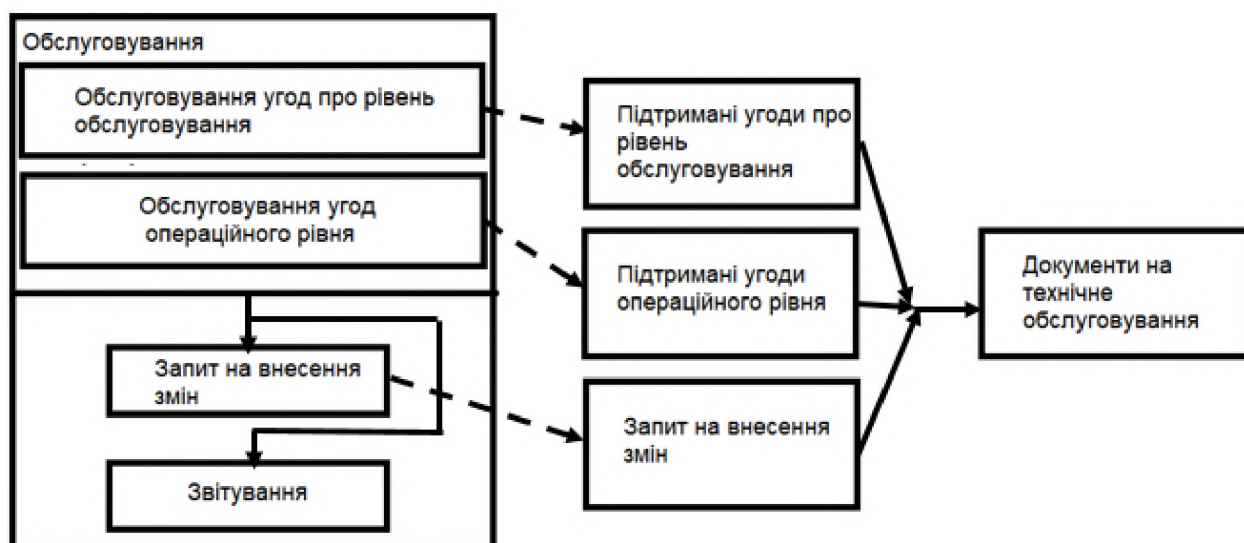


Рисунок 2.12 – Модель підпроцесу “Обслуговування”

Наведемо приклад проходження усіх фаз фреймворку стандарту управління безпекою на основі політики внутрішньої електронної пошти.

Внутрішня електронна пошта піддається численним ризикам безпеки, що вимагає відповідного плану безпеки та політики. У цьому прикладі підхід управління безпекою ITIL використовується для реалізації політики електронної пошти. Формується команда управління безпекою та формулюються керівні

принципи щодо процесу та розповсюджуються поміж всіма працівниками та постачальниками послуг. Ці дії проводяться на етапі “Контроль”.

На наступній фазі “Планування” формулюються політики. Політика, що стосується безпеки електронної пошти, формулюється та додається до договорів про рівень обслуговування. Наприкінці цього етапу весь план готовий до реалізації. Реалізація проводиться за планом.

Після впровадження, політики оцінюються або на основі самооцінки, або через внутрішніх чи зовнішніх аудиторів. На етапі технічного обслуговування електронна політика коригується на основі етапу оцінювання. Необхідні зміни обробляються за допомогою запитів на внесення змін.

Загалом фреймворк стандарту можна представити у вигляді нижченаведеної схеми [29]:

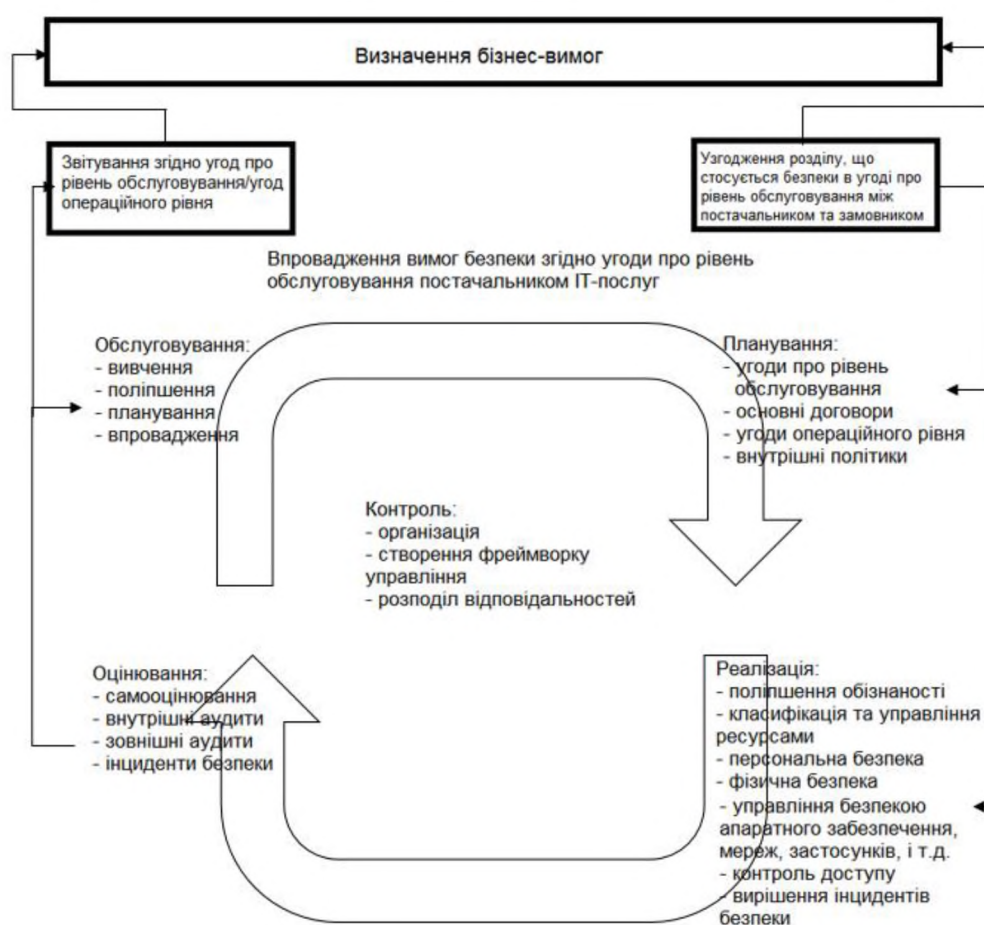


Рисунок 2.13 – Фреймворк управління безпекою стандарту ITIL

Інформаційна безпека описує діяльність, яка пов'язана із захистом активів інформації та інформаційної інфраструктури від ризиків втрати, неправильного використання, розкриття чи пошкодження. Існує потреба у наборі орієнтирів чи стандартів, які допоможуть забезпечити адекватний рівень безпеки, ефективного використання ресурсів, і адаптації кращих практик безпеки. Такі системи, як ITIL, можуть використовуватися як основа для розвитку надійного процесу захисту інформації. ITIL розглядається як одна з кращих практик управління IT-сервісом. Розробка сервісу - це фаза життєвого циклу обслуговування ITIL, оскільки безпека інформації є однією з найважливіших служб, яка потрібна впродовж життєвого циклу даних [31, 32].

2.3.2 Постійне вдосконалення послуг згідно стандарту ITIL

Постійне вдосконалення послуг (ПВП) - це тип процесу, який використовує методи управління якістю для навчання на попередніх успіхах і невдачах і має на меті постійно підвищувати ефективність та ефективність IT-сервісів та процесів [34].

Основна мета постійного вдосконалення послуг (ПВП) - це постійне узгодження IT-сервісів зі змінами потреб бізнесу шляхом визначення та впровадження удосконалень в IT-сервісах, що підтримують бізнес-процеси.

ПВП шукає шляхи підвищення ефективності процесу та економічності.

До процесів постійного вдосконалення послуг стандарту ITIL відносяться [28, 29]:

1) Огляд сервісів: метою цього процесу є періодичний огляд інфраструктури та бізнес-послуг. Огляд послуг також має на меті покращити якість обслуговування там, де це необхідно, та визначити економічні шляхи надання послуги. Ключовими показниками ефективності в контексті даного процесу є:

- Кількість оглядів сервісів – кількість формально проведених оглядів процесів впродовж періоду звітування

- Кількість ідентифікованих слабкостей – кількість слабкостей, що були ідентифіковані впродовж огляду сервісів та повинні бути усунені за допомогою ініціатив вдосконалення

2) Оцінка процесів: Метою є регулярна оцінка процесів ІТ. Він спрямований на визначення областей, в яких не досягнуто цільових показників процесу, проведення регулярних аудитів, орієнтирів, оцінок та оглядів. Ключовими показниками ефективності в контексті даного процесу є:

- Кількість оцінок продуктивності та аудитів
- Кількість оцінювань процесу
- Кількість ідентифікованих слабкостей
- Кількість ініціатив щодо постійного вдосконалення послуг
- Кількість завершених ініціатив щодо постійного вдосконалення послуг

3) Визначення ініціатив ПВП: Метою цього процесу є визначення конкретних ініціатив, спрямованих на покращення послуг та процесів на основі результатів оглядів сервісів та оцінок процесів. Ініціативи, що виникають в результаті цього - вимагають співпраці з клієнтами, або є внутрішніми ініціативами, які здійснює сам постачальник послуг. Ключовими показниками ефективності в контексті даного процесу є:

- Кількість ініціатив щодо постійного вдосконалення послуг
- Кількість завершених ініціатив щодо постійного вдосконалення послуг

4) Моніторинг ініціатив ПВП: Метою цього процесу є перевірка ініціатив щодо вдосконалення та перевірка, чи продовжуються вони згідно плану. Якщо їх немає, то він спрямований на внесення виправлень, де це потрібно [34, 35, 36].

На основі збору та аналізу результатів вимірювання будується процес вдосконалення, який складається з семи етапів. Основна мета процесу вдосконалення - визначити та керувати кроками, необхідними для ідентифікації, визначення, збору, обробки, аналізу, подання та впровадження удосконалень, які були здійснені протягом певного періоду часу.

Іншими цілями процесу вдосконалення є:

- Визначення наявних можливостей для вдосконалення послуг, процесів, інструментів
- Зниження вартості надання послуг та забезпечення того, що ІТ-сервіси дозволяють досягти необхідних бізнес-цілей та результатів.
- Визначення сфер, які необхідно виміряти, проаналізувати та звітувати, щоб встановити можливості вдосконалення.
- Повинен постійно переглядати досягнення сервісів, щоб гарантувати їх належне узгодження з вимогами організації.
- Забезпечення розуміння того, що потрібно вимірювати, причину вимірювання та визначення успішного результату.

Семикроковий процес удосконалення забезпечує задоволення поточних та майбутніх вимог бізнесу шляхом постійного моніторингу та аналізу надання послуг. Це дозволяє постійно оцінювати ситуацію, що склалася, відповідно до вимог бізнесу та визначає наявні можливості для вдосконалення надання послуг клієнтам [34].

Процес вдосконалення включає наступні 7 кроків:

- Ідентифікація стратегії для вдосконалення (підготовчий крок)
- Визначення того, що необхідно
- Визначення того, що можна виміряти
- Збір даних
- Обробка даних
- Аналіз даних
- Презентування та використання інформації
- Впровадження коригувальної [34]

Процес удосконалення може бути представлений у вигляді нижченаведеної схеми [32]:

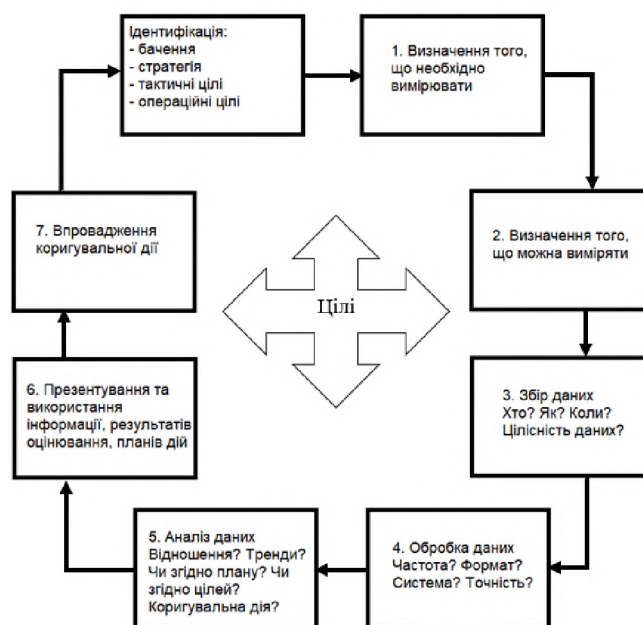


Рисунок 2.14 – Схема 7-крокового процесу вдосконалення згідно ITIL

Оскільки безпека є безперервним процесом, слід запровадити комплекс заходів і засобів контролю, які допомагають мінімізувати як загрози, так і вплив людських помилок. ITIL пропонує п'ять різних типів заходів:

- По-перше, заходи профілактики розроблені для того, щоб запобігти інциденту безпеки. Значна частина цієї практики зосереджена на таких завданнях управління доступом, як присвоєння відповідних прав та дозволів, перевірка ідентифікації та забезпечення того, що сторонні особи не можуть отримати доступ до інформації та систем.
- Редукційні заходи спрямовані на зменшення впливу інцидентів, як це відбувається, наприклад, складання планів надзвичайних ситуацій та тестування їх, наприклад, або автоматизованого резервного копіювання важливих даних та систем.
- Детективні заходи точно такі, як вони названі: вводяться контрольні засоби для виявлення ризику чи загрози якомога швидше. Це означає встановити найкращі можливі системи моніторингу - включаючи засоби моніторингу мереж та систем, попередження.
- Репресивні заходи схожі на контратаки. Якщо виявлена потенційна загроза, як, наприклад, бот, який постійно намагається увійти за допомогою

- асортименту комбінацій імен користувача та пароля - автоматичне блокування подальших спроб з IP-адреси (або тимчасове блокування імен користувачів, пов'язаних зі спробами входу) - приклад репресивного заходу.
- Нарешті, коригувальні заходи мають на меті відновити будь-яку шкоду, спричинену помилкою чи інцидентом. Відновлення резервної копії - найкращий приклад [33].

2.4 Фреймворк Six Sigma

2.4.1 Основні складові та методології стандарту

Six Sigma (шість сигм) – множина технік та інструментів, направлених на вдосконалення процесу. Стратегії фреймворку застосовуються для покращення якості результатів процесу шляхом виявлення та усунення причин недоліків та мінімізації варіативності в бізнес-процесах. Використовується набір методів управління якістю, в основному емпіричних, статистичних методів, для створення особливої інфраструктури, яка складається з людей, які є експертами в цих методах. Кожен проект Six Sigma, що виконується в організації, слідує визначеній послідовності етапів і має конкретні цілі, наприклад скоротити час циклу процесу, знизити витрати. Процес описується рейтингом сигм, що вказує на його вихід або відсоток бездефектних результатів, які він створює, зокрема, в межах, скільки стандартних відхилень від нормального розподілу відповідає частці бездефектних результатів. Основна доктрина фреймворку стверджує: постійні зусилля для досягнення стабільних та передбачуваних результатів процесу (наприклад, зменшення варіацій процесів) мають важливе значення для успіху бізнесу; виробничі та бізнес-процеси мають характеристики, які можна визначити, виміряти, проаналізувати, вдосконалити та контролювати; досягнення стійкого вдосконалення вимагає задіяння людських ресурсів від усієї організації, особливо від керівництва вищого рівня [37].

Загалом, Six Sigma стосується застосування структурованого наукового методу для вдосконалення аспектів, організації, процесу чи персоналу. Це стосується впровадження збору даних та аналізу, які дозволяють визначити найкращі способи задоволення потреб, а також мінімізувати витрачені ресурси.

Фреймворк має дві основні методології: DMAIC (Define, Measure, Analyze, Improve, Control) та DMADV (Define, Measure, Analyze, Design, Verify). Застосування Six Sigma для управління інформаційною безпекою означає проходження процесу DMAIC. Найбільш критичним етапом є Визначення (Define), на якому визначаються цілі, критичні щодо якості процесу. Такі цілі виконуються в процесі і використовуються для вимірювання успіху.

Методологія DMAIC включає наступні 5 фаз:

- Визначення (Define) високорівневих цілей проекту та поточного процесу. Наприклад, повторні вразливості збільшують накладні витрати та відкривають загрози вразливій системі
- Вимірювання (Measure) ключових аспектів поточного процесу та збір актуальних даних. встановлення наявних базових рівнів та вимірювання. Наприклад, визначення прогалин між поточною та необхідною продуктивністю. Деякі приклади вимірювання вразливостей включають:
 - Кількість просканованих систем
 - Кількість критичних вразливостей, закритих протягом останніх 48 годин
 - Процент закритих вразливостей відносно загальної кількості вразливостей
- Аналіз (Analyze) даних для верифікації причинно-наслідкових зв'язків. Визначення деталей відношень та забезпечення того, що всі фактори розглянуті. Наприклад, ідентифікація та перевірка основних причин пропущених цілей.

- Вдосконалення (Improve) або оптимізація процесу на основі аналізу даних використовуючи такі техніки, як Розробка експериментів. Виявлення, тестування та реалізація рішення проблеми, частково або в цілому. Визначення рішень для усунення основних першопричин для виправлення та запобігання проблем процесу. Метою цього кроку може бути пошук рішень без їх реалізації
- Контроль (Control), для забезпечення того, що будь-яке відхилення від цілі зкоректовано перед тим, як це призведе до дефектів. Впровадження систем контролю (наприклад статистичного контролю процесів) для постійного відслідковування процесів

Розглянемо 4 цілі, критичні щодо якості процесу, для вимірювання ефективності програми безпеки. Вони спеціально призначені для вимірювання того, наскільки ефективно виконуються стандартні рекомендації, щодо управління інформаційною безпекою:

- Політика – вимірювання якості та виконавчість політик безпеки
- Процеси – вимірювання того, наскільки ефективно виконується дотримання визначених практик відповідно до прийнятих стандартів
- Відношення – вимірювання зусиль, щодо побудови відносин між відділами персоналу та зацікавленими сторонами
- Витрати – вимірювання інцидентів та результуючих втрат

Після визначення цілей, критичних, щодо якості процесу безпеки, наступним кроком є створення плану їх вимірювання та початок фіксації цих даних. Метрики, розроблені інструментами Six Sigma, дозволяють виявляти ризики для безпеки, які потенційно заважають досягти кінцевих цілей, а також забезпечують захист перед інцидентом, а не після інциденту. Крім того, вони допомагають створювати стратегію захисту та плани пом'якшення наслідків, розроблені з метою усунення найбільш пріоритетних ризиків безпеки.

Основна ідея Six Sigma полягає в тому, що якщо є можливість виміряти скільки дефектів виникає в процесі, є можливість систематично їх усувати і

максимально наближатись до “нульових дефектів”. Для досягнення якості шести сигм, процес не повинен створювати більше 3,44 дефектів на 1 млн. можливостей. Можливість визначається як шанс невідповідності необхідним умовам [38, 39].

2.4.2 Управління політикою інформаційної безпеки згідно Six Sigma

В процесі управління політикою безпеки, Six Sigma може застосовуватись для базування процесу управління політикою безпеки завдяки широкому поширенню та ефективності в промислових умовах з чітким механізмом зворотного зв'язку, для контролю розгортання політики безпеки поряд із загрозами, що постійно розвиваються; для процесу управління політикою безпеки, щоб полегшити інтеграцію з промисловими процесами; для кількісної оцінки ризику в управлінні політикою безпеки для прийняття рішень.

Управління політикою безпеки в рамках фреймворку Six Sigma (згідно методології DMAIC):

1. Визначає цілі безпеки та кількісно оцінює цифрові активи
2. Здійснює заходи по вимірюванню та оцінюванню загроз цифровим активам та кількісно визначає ризик
3. Аналізує загальні цілі безпеки з виявленням зовнішніх та внутрішніх факторів, які впливають на активи обчислювальних сервісів
4. Вдосконалює розробку та оптимізує політики безпеки на ряду з загрозами, що постійно розвиваються
5. Контролює усунення загроз із застосуванням політики безпеки для гарантії якості обслуговування

Розглянемо кожен фазу роботи фреймворку в контексті управління політикою безпеки згідно методології DMAIC детальніше.

- **Визначення (Define).** Дана фаза використовується для ідентифікації цифрових активів та кількісної оцінки різних цілей проектування для процесу управління інформаційною безпекою. Розробка та огляд політики

відображають фазу визначення процесу управління політикою безпеки. Фаза передбачає визначення цілей, активів, загроз та факторів безпеки, пов'язаних із створенням політики безпеки. Ідентифікація активів важлива для кількісної оцінки необхідності подолання загроз. Якщо серйозність загрози активу висока, тоді необхідно розробити продукт, щоб усунути цей недолік. Наприклад, якщо база даних PostgreSQL використовується для створення служби під обмеженнями SLA, тоді:

- Під час фази визначення необхідно оцінити ідентифікацію загроз для цифрових активів. Найважливіші дані для бази даних, які можна кількісно оцінити за допомогою SLA:
 - Неправильне або несанкціоноване створення, зміна або видалення облікових записів користувача
 - Неправильне або несанкціоноване створення, зміна або видалення вмісту бази даних
 - Неправильне або несанкціоноване створення, зміна або видалення елементів контролю доступу до бази даних
 - Експлуатація керування входом (переповнення буфера), для компрометації доступності та ескалації привілеїв
- За згодою керівництва, визначаються відповідні системи усунення загроз, а також обирається версія бази даних. Інструменти, які використовуються у фазі визначення:
 - Вартість якості, коли витрати на якість можна розділити на вартість задовільної якості, де процес відповідає певним рекомендаціям, що відповідно до інформаційної безпеки має дотримуватись кращих практик управління політиками безпеки
 - Вартість незадовільної якості, що нараховується через невідповідність. Інструментом, який зазвичай використовується для орієнтації на несправності в вартості незадовільної якості, є діаграма Парето, яка підкреслює важливість певного чинника

серед різних факторів, а також важливість втрат доходу, пов'язаних із відповідною вразливістю безпеки.

- Вимірювання (Measure). Дана фаза включає вимірювання та кількісну оцінку ризиків для цифрових активів у сервісі [40]:
 - Вплив загрози, через особливості програмного забезпечення, вимірюється системою, аналогічно оцінці CVSS (Common Vulnerability Scoring System). Базова оцінка CVSS складається з:
 - Вектора доступу, що позначає, як експлуатується вразливість
 - Складності доступу, що позначає складність вразливості після отримання доступу в систему
 - Автентифікації, яка вказує на те, скільки кроків автентифікації повинен здійснити атакуючий, для експлуатації вразливості
 - Метрики впливу на конфіденційність, яка підкреслює, як вразливість впливає на несанкціоновані дані
 - Цілісність, що позначає гарантії довіри до вмісту
 - Вплив на доступність, що позначає доступність контенту перед успішною атакою.
 - Ризик, пов'язаний із особливостями апаратного забезпечення, що кількісно визначає рівень довіри, який може надати обладнання
 - Ризик під час роботи обчислювального сервісу на основі моделі загроз, створеної на етапі Визначення.

Інструменти, які використовуються на даній фазі фреймворку Six Sigma включають наступні [40]:

- Інструмент $Y=F(X)$, який ідентифікує зловмисний вхід X та пов'язаний з ним вихід Y для різних загроз, ідентифікованих як такі, що включені до фази Визначення. Зазвичай, такий аналіз показує відношення причинності векторів загроз та відповідних вразливостей обчислювальної системи. Набір даних про загрози X при обробці обчислювальною системою F визначає вразливість Y . Вектор доступу CVSS є набором даних про загрозу.

Вимірюється складність доступу та автентифікації за базовою оцінкою CVSS. Схематичне зображення роботи даного інструменту наведено нижче [40]:

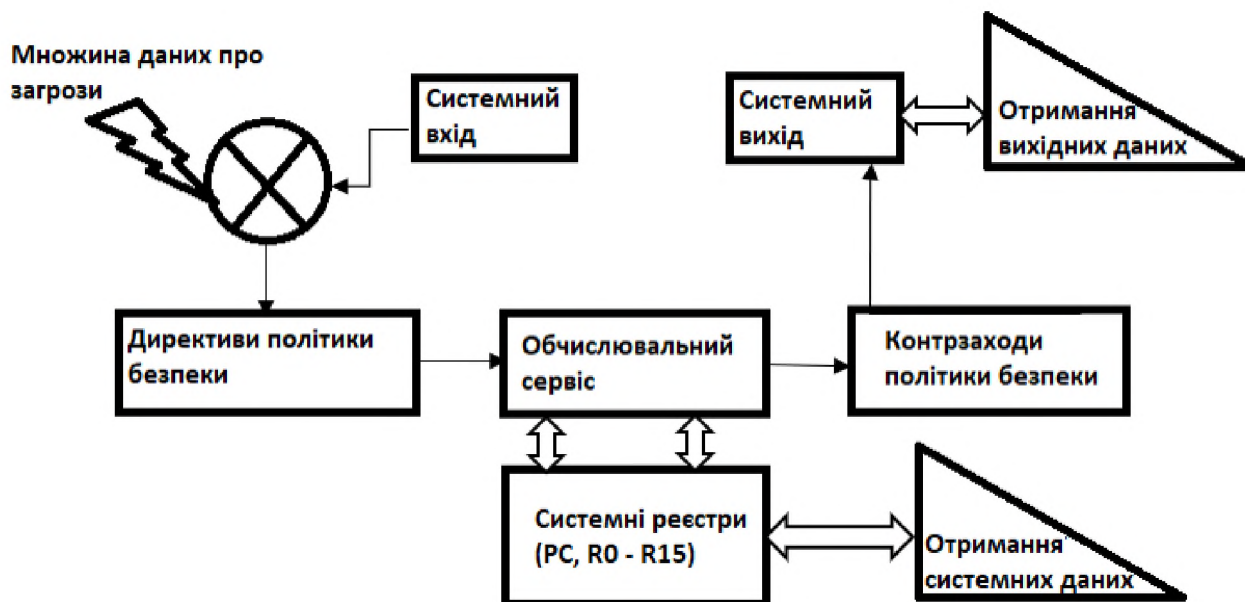


Рисунок 2.15 – Інструмент $Y=F(X)$ аналізу для інформаційної безпеки

- Інструмент FMEA (Failure Mode and Effects Analysis або Аналіз режиму відмов та наслідків). Визначає вектори загроз, ступінь серйозності загроз, причини та діючу методологію перевірки для оцінки ризиків. В даному випадку вимірюється конфіденційний вплив, вплив на цілісність та доступність базової оцінки CVSS.
- Інструмент Process Sigma допомагає кількісно визначати, чи здатні поточні політики безпеки (C_p , C_{pk}) відповідати виявленим загрозам шляхом ідентифікації сигми процесу. C_p вказує на здатність існуючих політик безпеки протидіяти відомим та модельованим загрозам, а C_{pk} вказує, наскільки ефективна політика безпеки, для протидії фактичним загрозам:
 - Важливими чинниками тут є специфікація споживача та експлуатаційна специфікація. Якщо рівень серйозності загроз кількісно визначений в рамках цих специфікацій, то оцінка ризику CVSS дає значення ризику

- Складні етапи атак, що вимагають від споживача бути активним учасником цього процесу, виходять за межі експлуатаційних характеристик обчислювальної служби. Клієнтські угоди складені з метою обмеження зобов'язань щодо надання обчислювальних послуг в таких випадках. Значення ризику C_{pk} у випадку атак, які складно використовувати, буде низьким, що надалі буде включено в користувацькі згоди.
- Інструмент GAGE. Використовується для визначення повторюваності та відтворюваності ідентифікації загроз, а також для видалення хибних спрацювань із множини зібраних даних.

У нижченаведеній таблиці вказано зіставлення різних інструментів фреймворку та заходів безпеки:

Таблиця 2.1 – Зіставлення фази вимірювання та управління безпекою

Інструмент Six Sigma	Безпека
$Y = F(X)$	Вхід/Вихід
FMEA	Статичні аналізатори, процес перевірки
Process Sigma	Оцінки CVSS
GAGE	Диференційні оцінки CVSS

- Аналіз (Analyze). Фаза аналізу визначає ефективність вже існуючих політики безпеки та моделей загроз. Цілями цього етапу є:

- Вдосконалення існуючої політики безпеки
- Ідентифікація нових загроз і тим самим змін до моделі загроз

Тимчасові показники CVSS забезпечують вимірювання та аналіз:

- Експлуатаційності, яка вимірює техніки експлойтів та наявність коду, який може використовуватися на етапі експлуатації
- Рівень виправлення, який стосується типу виправлення, доступного для певної вразливості.

- Довірених повідомлень, які стосуються існування вразливості та якості інформації про технічні деталі вразливості.

Інструменти, які використовуються у фазі аналізу, є [40]:

- Тестування гіпотез, щодо даних про загрозу для перевірки ефективності нових політик безпеки, задаючи нульову гіпотезу (H_0) або альтернативну гіпотезу (H_a). Альфа-ризик все ще зберігається на рівні промислового ризику 5% для тестування гіпотез.
- Кореляція та регресія для перевірки відомих векторів загрози для виявлення вхідних вихідних зв'язків. У цій частині йдеться про лабораторні проникнення та нечіткі тести на безпеку програмного забезпечення та забезпечення якості. Результат зазвичай визначається коефіцієнтом Пірсона. Це можна підсумувати рівнем відновлення та повідомленням про достовірність тимчасової оцінки CVSS.
- Дисперсійний аналіз (ANOVA) - тестування гіпотез з варіаціями вхідних факторів.

Елементами фази аналізу є [40]:

- Оцінка ризику: На основі доступних політик безпеки та моделей загроз:
 - Рішення можуть прийматися за ступенем ризику, який можна прийняти.
 - Деякі політики, можуть бути досить дорогі для впровадження, і не бути вартими впровадження в продукт, і відповідно ця оцінка кількісної оцінки ризику допомагає приймати фінансові та бізнес-рішення.
 - Використання моделей політики та загроз у поєднанні з обчислювальною логікою визначає, як люди використовують систему безпеки та допомагає зосередитись на критичних загрозах та політиці. Врешті-решт, вона спирається на оцінку ризику для будь-якого майбутнього рішення.

- Компонентна модель загрози: модель загрози на етапі аналізу дає огляд будь-яких модельованих загроз та моделювання будь-яких нових загроз.
 - У обчислювальній системі, побудованій з різних компонентів, існує специфічна модель загрози для кожного компонента. Наприклад, деякі компоненти в обчислювальному сервісі можуть піддаватись загрозам, орієнтованим на мережу, де, як і інші, можуть піддатись загрозам, орієнтованим на апаратне забезпечення.
 - Моніторинг використовується для аналізу ефективності політики, щоб виявити різні кореляції між вхідними/вихідними даними та загрозами цифровим активам.
- Тестування на проникнення: моделювання та постановка атаки на обчислювальний сервіс вимагає розуміння того, як використовується обчислювальна послуга. Він визначає різні вхідні характеристики на основі компонентної моделі загрози.

У нижченаведеній таблиці вказано зіставлення фази аналізу фреймворку та заходів безпеки:

Таблиця 2.2 – Зіставлення фази аналізу та управління безпекою

Six Sigma	Безпека
Тестування гіпотез	Оцінка ризиків
Аналіз варіації	Компонентна модель загроз
Кореляція та регресія	Тестування на проникнення

- Вдосконалення (Improve). Фаза вдосконалення в контексті політики безпеки повинна або створити нову політику безпеки, або вдосконалити існуючу політику безпеки. Інструменти, які використовуються у фазі вдосконалення:
 - Розробка експериментів (Design of Experiments або DOE), по суті, є аналізом варіації для всієї системи. Міра аналізу варіації у фазі аналізу

використовується для отримання варіацій для компонентів обчислювального сервісу. У розробці експериментів беруться до уваги всі зміни в обчислювальному сервісі, для розуміння ефективності системи безпеки та фіксування значення ризику політики для загрози будь-якому цифровому активу з різними варіаціями. Така оцінка необхідна після проведення GAGE вимірювання для загроз, оскільки воно визначає джерело варіацій через загрози в різних операційних умовах.

Елементами фази вдосконалення є:

- Директива політики безпеки: Директива політики безпеки - це фактичні визначення політики, які впроваджуються. Ці визначення викликаються перед виконанням фактичної логіки обчислень. Збирається зворотній зв'язок із профілю загрози, який використовувався для створення політик.
- Контрзаходи політики безпеки: Частина контрзаходу в політиці безпеки діє на будь-яку модельовану загрозу, яка виникала під час роботи. Ефективне рішення контрзаходів лежить у цьому визначенні політики.

У нижченаведеній таблиці вказано зіставлення фази вдосконалення фреймворку та заходів безпеки:

Таблиця 2.3 - Зіставлення фази вдосконалення та управління безпекою

Six Sigma	Безпека
Розробка експериментів	Системна модель загроз
	Директиви безпеки, контрзаходи безпеки, моніторинг загроз

- Контроль (Контроль). Фаза контролю політики безпеки підкреслює фактичний контроль обчислювального сервісу за допомогою політики

безпеки, що працює в режимі зворотного зв'язку. Інструменти, які використовуються у фазі управління, є:

- Статистичний контроль процесів - вимірює критичні характеристики процесу в режимі реального часу та створює контрзаходи щодо виявлених загроз для їх зменшення.
- Виправлення помилок, де визначення політики захищені від помилок, щоб їх не можна було неправильно трактувати

У нижченаведеній таблиці вказано зіставлення фази контролю фреймворку та заходів безпеки:

Таблиця 2.4 - Зіставлення фази контролю та управління безпекою

Six Sigma	Безпека
Статистичний контроль процесів	Моніторинг даних загроз та контрзаходи безпеки
Виправлення помилок	Директиви безпеки

Отже, фреймворк Six Sigma характеризується наступними аспектами управління політикою інформаційної безпеки:

- Уточнення політики безпеки, вдосконалення існуючої політики в активний та реактивний спосіб в контексті процесу управління політикою безпеки. Первинна мета існуючих моделей та моделі Six Sigma схожа, і всі моделі задовольняють цій вимозі.
- Профіль загрози, на якому виконується політика безпеки, виконується з активним профілем загрози в фреймворку Six Sigma. Через причинний зв'язок між політикою безпеки та загрозою як частиною живих обчислювальних сервісів застосовується активний профіль загрози для забезпечення постійного моніторингу та адаптації політики безпеки. Існуючі в літературі моделі вказують на необхідність моделювання загроз, але не пропонують їй бути частиною активної системи.

- Зовнішні фактори, що впливають на обчислювальний сервіс. Загрозам, які відомі та змодельовані, можна протидіяти лише за допомогою розробки.
- Зворотній зв'язок - відгуки щодо ефективності політики безпеки, зумовлені змінами загроз, вирішуються негайно під час оцінки політики та розробки в існуючих системах. У процесі Six Sigma зворотний зв'язок є явним, задано явну систему моніторингу загроз для адаптації політики безпеки.
- Впровадження змін “на льоту” - завдяки розділовій політиці безпеки та профілям загроз як явній частині обчислювального сервісу, модель може змінюватися на ходу в міру розвитку загроз. Система контролю загроз також дозволяє адаптувати політику на основі даних моніторингу. У сучасних моделях через вбудовану частину політики в обчислювальній службі без явного розмежування зміни на ходу можуть бути важко прийнятими.
- Математична модель представлена у фреймворку базується на причинному зв'язку між загрозою та політикою безпеки. Не маючи причинно-наслідкових зв'язків, інструменти Six Sigma не можна використовувати для аналізу. Тим самим рамки, які представлені в цій моделі, відрізняються від інших, де математичні рамки не представлені.
- Інтеграція виробничих процесів інтегрує процес управління політикою безпеки в промислові процеси, що сприяє галузевим цілям кількісного визначення та оцінки ризиків.

2.5 Порівняльний аналіз стандартів управління ІБ з позицій застосування в SOC

На основі розглянутих особливостей вищезгаданих фреймворків та стандартів для управління інформаційною безпекою, опишемо їх основні переваги та недоліки з позицій застосування в SOC.

1) ISO 27000

Таблиця 2.5 – Переваги та недоліки серії стандартів ISO 27000

Переваги	Недоліки
<ul style="list-style-type: none"> - Поняття інформаційної безпеки розглядається як комплекс - Процесний підхід - Модель PDCA - Забезпечення детального керівництва та інтерпретація для реалізації процесів PDCA та вимог, визначених в ISO 27001 - Розгляд оцінок відповідності або галузевих вимог до СУІБ - Фокус на організаційних процесах та конкуруючих процедурах - Допомагає вдосконалювати адаптацію процесів відповідно технологічному прогресу • 27001 - Вимоги до планування, впровадження, оперування та вдосконалення СУІБ сформульовані для відповідності усім організаціям, незалежно від розміру, цілей, бізнес-моделі. 	<ul style="list-style-type: none"> • 27001 - Низька деталізація вимог і, відповідно, необхідність залучення для їх реалізації досвідчених експертів високого рівня. - Набір застарілих правил і підходів до забезпечення захисту інформації • 27002 - Не описано еквівалентів Управління проблемами та Управління конфігурацією (що має вагомий вплив на ІТ-середовище) як в ITIL. - Не розглянуті питання фінансових проблем стосовно управління інформаційною безпекою. Це описано з точки зору управління ризиками.

Продовження таблиці 2.5

Переваги	Недоліки
<ul style="list-style-type: none"> • 27002 - Описує набір можливих заходів захисту інформації, з яких організація може вибрати необхідні саме їй. - Основна перевага – застосування для забезпечення загальної безпеки на всіх рівнях організації - Перевага в описі процесу інформаційної безпеки над відповідними у ITIL та COBIT. • 27003 - Опис повного циклу впровадження СУІБ від розробки до плану/проекту впровадження - Застосовний для усіх типів організацій (як і невеликих, для яких дії, описані в стандарті можуть бути спрощені, так і великих, де для багаторівневої системи організації або управління дії, описані в стандарті також застосовні) - Використовується в поєднанні із 27001 та 27002 - Додаткові рекомендації по підтримці планування і розробки моніторингу та вимірювань • 27004 - Повна інтеграція із СУІБ, які базуються на 27001 	<ul style="list-style-type: none"> • 27004 - Перевантажений загальними рекомендаціями, а модель може застосовуватись без спеціалізованих термінів та надлишкових логічних структур. В порівнянні із стандартами ITIL та COBIT, де надано приклади метрик та ключових показників ефективності по визначених процесам, які можна адаптувати і під процеси СУІБ, згідно ISO 27001 - ISO 27004 таких прикладів не надано. - Для процесу збору та аналізу даних не наведено ніяких математичних складових (моделей, методів, величин, алгоритмів)

Кінець таблиці 2.5

Переваги	Недоліки
<ul style="list-style-type: none"> - Забезпечення індикаторами рішень для постійного вдосконалення СУБ - Спрощений процес звітування про безпеку 	

2) ITIL

ITIL – набір бібліотек, вказує на те, як правильно побудувати IT-процеси, як зв'язати їх між собою і яким чином ними управляти.

Таблиця 2.6 – Переваги та недоліки стандарту ITIL

Переваги	Недоліки
<ul style="list-style-type: none"> - Зміщення фокусу на управління послугами, які надають інформаційні технології - Надає пояснення стосовно фінансування та розподілу витрат для реалізації IT-сервісів - Детальний опис важливих процесів (конфігурація, інциденти та проблеми, зміни і т.д.) 	<ul style="list-style-type: none"> - Сфера інформаційної безпеки покрита поверхово

3) COBIT

COBIT – високорівневий стандарт, який створювався для управління і контролю IT з точки зору цілей бізнесу і висунутих вимог. Найбільш підходящий для державних органів влади.

Таблиця 2.7 – Переваги та недоліки стандарту COBIT

Переваги	Недоліки
<ul style="list-style-type: none"> - Вимоги не є жорсткими та обов'язковими для виконання 	<ul style="list-style-type: none"> - Не вказано, на відміну від ITIL, яким чином організувати діяльність IT і правильно побудувати процеси

Кінець таблиці 2.7

Переваги	Недоліки
<ul style="list-style-type: none"> - Опираючись на COBIT, компанія може самостійно оцінити, які області діяльності ІТ необхідно контролювати для досягнення бізнесом поставлених цілей і підібрати відповідні контролі - Дозволяє оцінити діяльність ІТ, поставивши чіткі і вимірювані цілі і відслідковувати їх виконання - Модель здатності процесів - Зв'язок ІТ та бізнесу - Допомогає вдосконалювати критерій для прийняття інформованих рішень на управлінському рівні - Визначає стратегічні ІТ-плани, базуючись на мережевій архітектурі, інформації та асоційованому обладнанні - Сфокусований на документах 	<ul style="list-style-type: none"> - Відсутній еквівалент Управління інцидентами, як в ITIL - Обмежений стосовно визначених тем, та має бути адаптований окремо (для управління, безпеки, якості, розробки) - Суттєвий розрив між управлінням та операціями

ITIL та COBIT покривають одну і ту ж область, та орієнтовані на ефективне управління ІТ у відповідності з цілями бізнесу, на основі процесного підходу. В більшій мірі оперують загальною термінологією.

ITIL дозволяє організувати роботу ІТ-служби, а COBIT – контролювати її. Для створення або впровадження комплексного фреймворку необхідно опиратись на концепції/процеси, активності, вартості/вигоди та планування до впровадження згідно ITIL та аудити згідно COBIT. Крім того, можна будувати комплексний фреймворк управління інформаційною безпекою на основі одразу 3-х стандартів – ITIL, COBIT та ISO 27002, де перший буде використовуватись для визначення стратегій, планів та процесів; другий буде застосовуватись для визначення метрик,

еталонних тестів та аудитів; третій буде використовуватись для усунення проблем безпеки зі зменшенням ризиків.

4) Six Sigma

Таблиця 2.8 – Переваги та недоліки стандарту Six Sigma

Переваги	Недоліки
<ul style="list-style-type: none"> - Орієнтація на весь процес, який стоїть за завершенням послуги, а не на кінцевий результат - Структурований спосіб рішення проблем якості та часу - Вимірювані вдосконалення через підхід, заснований на даних - Сильний акцент на причинно-наслідковий аналіз - Описано інструменти для визначення, вимірювання, аналізу, вдосконалення та контролю 	<ul style="list-style-type: none"> - Генерація великих об'ємів емпіричних даних через постійну перевірку бізнес-процесів, що призводить до довготривалих та складних процедур - Процес вдосконалення якості часто призводить до підвищенню загальних затрат - В деяких моментах занадто багато уваги приділяється інструменту, замість пошуку коректного рішення

Висновки до розділу 2

В результаті аналізу стандартів та фреймворків управління процесами безпеки зроблено наступні висновки:

- Для операційних центрів безпеки відсутні будь-які вузькоспеціалізовані стандарти чи методології, які б допомагали побудувати процес оперування та управління процесами безпеки враховуючи аспекти даної організаційної структури
- Окреме застосування попередньо описаних стандартів та фреймворків не дає бажаних результатів в побудові та управлінні фазою оперування SOC. Потенційно застосовними методиками можуть бути розробка програми безпеки на основі ISO 27001 та 27002, розробка методики вимірювань інформаційної безпеки в контексті загальної програми безпеки на основі ISO 27003 та 27004, застосування методів та інструментів в контексті методики вимірювань ІБ на основі Six Sigma, оцінка процесів на основі моделі здатності процесів COBIT
- Застосування стандартів на практиці зазвичай складне та не відповідає встановленим очікуванням на фазі планування SOC
- Попередньо описані стандарти та фреймворки не пропонують інструментів та методів, які могли б застосовуватись в процесі роботи з даними при оперуванні SOC
- Виникає необхідність розробити певну програму чи фреймворк, який би враховував особливості оперування SOC, а також включав би для оцінки певних складових (наприклад оцінка ефективності процесу, оцінка ризиків в управлінні вразливостями) найкращі практики попередньо описаних стандартів

3 РОЗРОБКА ФРЕЙМВОРКУ УПРАВЛІННЯ ПРОЦЕСАМИ ЗАБЕЗПЕЧЕННЯ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ В SOC

3.1 Загальна ідея фреймворку управління процесами забезпечення інформаційної безпеки

На основі проведеного раніше дослідження в контексті управління інформаційною безпекою та аналізу стандартів та фреймворків, для управління процесами безпеки, а також на основі набутих практичних та теоретичних навичок в робочому середовищі – буде запропоновано фреймворк управління процесами безпеки для SOC.

Фреймворк управління процесом безпеки – це застосування управління бізнес-процесом в галузі інформаційної безпеки, розроблене з фокусом на придатність для використання та практичність. Опишемо основні його складові:

- На найнижчому рівні фреймворку знаходяться метрики безпеки, які визначаються залежно від особливостей системи/середовища, для початку процесу вимірювання, аналізу та оцінки діяльностей, пов'язаних з процесом безпеки, для даної системи/середовища. Метрики розробляються та застосовуються в чітко обмеженому та керованому контексті впродовж часу, і результати таких активностей можуть бути збережені, вивчені та використані навіть після завершення початкового проекту. Спеціальний метод “Цілі-Запитання-Метрики” обмежує метрики в контексті заданих цілей і забезпечує їх організацію, діючи при цьому як спосіб створення проектів вимірювання безпеки в межах конкретної цілі метрик.
- Стратегічний підхід фреймворку до безпеки включає в себе координацію багатьох різних діяльностей рівня проекту, які позначаються як проекти вимірювання безпеки. Проект вимірювання – технічна та організаційна структура, яка застосовується по відношенню до цілей, запитань, метрик безпеки. В таких проектах ініціативи по вимірюванню безпеки, що за своєю

основою мають бути обмеженими та з чітко визначеними межами, повинні активно проводитись, відслідковуватись та координуватись в більшу систему. Такі проекти дозволять вирішувати питання вдосконалення безпеки за допомогою керованих приростів, які документують та вирішують особливі цілі та задачі проекту в напрямку до глобальних цілей, які існують в інших проектах, в межах загальної програми вдосконалення безпеки організацій. Усі проекти є компонентами інтегрованої активності, зі входами з одних проектів та виходами до інших.

- Попередньо зазначений модулярний підхід до вимірювань безпеки підтримує глобальніше, стратегічне поняття – програма вдосконалення безпеки. Така програма повинна працювати для комбінування та координування активностей, що відносяться до різних проектів по вимірюванню, в систему постійного вимірювання, аналізу та вдосконалення безпеки. В межах програми вдосконалення, метрики, а також результати проектів категоруються та зберігаються для повторного використання в майбутньому, а між проектами будуються перехресні посилання. Усе це включається в організаційну систему навчання, для впровадження управління знаннями в контексті безпеки та обміну досвідом в межах SOC.
- Кінцевим результатом повинно стати управління процесами безпеки, в якому широкий набір характеристик, включаючи людські ресурси та організаційні процеси, а також технології – зрозумілі, вимірювані та постійно вдосконалюються. Краще розуміння процесу безпеки призводить до зменшення ризиків та втрат внаслідок витоків даних та порушень безпеки.
- Оцінка результатів роботи програм вдосконалення безпеки, на основі застосування моделей здатності процесів для оцінки впроваджених та підтримуваних процесів безпеки в SOC

Розуміння меж впливу, яких необхідно досягти з допомогою метрик безпеки та вдосконалень процесу безпеки задає об'єм самої програми управління процесом безпеки. Визначення меж впливу повинно відбуватись перед плануванням програми метрик безпеки.

3.2 Збір та аналіз даних метрик інформаційної безпеки

3.2.1 Оцінка ризиків, пов'язаних з вразливостями в інфраструктурі

Перед збором та аналізом даних, важливим питанням для SOC є управління вразливостями. Для забезпечення процесу управління вразливостями в SOC, необхідно розглянути оцінку ризику. Оцінка ризику, пов'язаного із вразливостями дозволяє визначити імовірний вплив та ймовірність експлуатації вразливості. Застосуємо для оцінки вразливостей в SOC методологію ранжування ризиків OWASP.

Загальна формула для обчислення ризику включає значення ризику (R), ймовірність ризику (P), та наслідки впливу ризику (C):

$$R = P * C$$

Згідно методології OWASP, ймовірність того, що конкретна вразливість буде проексплуатована, включає в себе агенти загроз та фактори вразливості, що оцінюються по шкалі від 0 до 9.

До факторів агентів загроз належать:

- Рівень навичок атакуючого (наприклад 1 – прогресивні навички, 3 – мережеві та програмні навички, 4 – прогресивний користувач, 6 – наявність декількох технічних навичок, 9 – без технічних навичок)
- Мотивація (наприклад 1 – невелика чи мала нагорода, 4 – можлива нагорода, 9 – висока нагорода)
- Можливість (наприклад 0 – велика кількість ресурсів та часу, 4 – необхідність спеціального доступу чи ресурсів, 7 – необхідність обмеженої множини прав доступу та ресурсів, 9 – немає необхідності в доступі чи в ресурсах)
- Розмір (а саме які типи атакуючих можуть отримати доступ до вразливості) (наприклад 2 – обмежена група розробників та адміністраторів, 4 –

користувачі внутрішньої мережі, 5 – партнери, 6 – авторизовані користувачі, 9 – анонімні користувачі з мережі Інтернет.

Кожна складова фактору загроз оцінюється по шкалі від 0 до 9. Далі оцінки додаються та використовуються разом із оцінками, отриманими від факторів вразливості, для обчислення ймовірності ризику.

До факторів загроз належать:

- Легкість відкриття (наприклад 1 – практично неможливо, 3 – складно, 7 – легко, 9 – наявні автоматичні інструменти)
- Легкість експлуатації (наприклад 1 – теоретична, 3 – складно, 5 – легко, 9 – наявні автоматичні інструменти)
- Відомість (тобто як добре відома вразливість потенційному атакуючому) (наприклад 1 – невідома, 4 – прихована, 6 – очевидна, 9 – загальновідома)
- Виявлення вторгнення (тобто ймовірність виявлення атаки) (наприклад 1 – активне виявлення в застосунку, 3 – журналювання та перегляд, 8 – журналювання без перегляду, 9 – не журналюється).

Ймовірність обчислюється як середня оцінка факторів агентів загроз та факторів вразливостей. Фінальне значення ризику ранжується для представлення рівня безпеки, наприклад низький ризик, середній, високий та екстремальний.

Тоді ймовірність P обчислюється як:

$$P = \frac{\frac{1}{n} (\sum_{i=1}^n x_i + \sum_{i=1}^n y_i)}{2}$$

Де $n = 4$, x_i – значення фактору агентів загроз, а y_i – значення фактору загроз.

Згідно методології OWASP, збитки, внаслідок того, що конкретна вразливість буде проексплуатована, включає в себе агенти фактори технічного впливу, та фактори впливу на бізнес, що оцінюються по шкалі від 0 до 9.

До факторів технічного впливу належать:

- Втрата конфіденційності (наприклад 2 – втрата некритичних даних, 6 – втрата критичних даних, 9 – втрата усіх даних)
- Втрата цілісності (наприклад 1 – незначне пошкодження даних, 3 – мінімальне пошкодження даних, 5 – серйозне пошкодження даних, 7 – інтенсивне пошкодження даних, 9 – пошкодження усіх даних)
- Втрата доступності (наприклад 1 – переривання мінімальної кількості другорядних служб, 5 – переривання мінімальної кількості основних служб, 7 – переривання великої кількості основних служб, 9 – переривання усіх служб)
- Втрата звітності (тобто чи можна відслідкувати загрозу прямо до атакуючого) (наприклад 1 – повністю відслідковувана, 7 – можливо відслідковувана, 9 – повністю анонімна)

До факторів впливу на бізнес належать:

- Фінансова шкода (наприклад 1 – шкода, менша ніж витрати на відновлення, 3 – невелика шкода, 7 – серйозна шкода, 9 – ймовірне банкрутство)
- Шкода репутації (наприклад 1 – невелика шкода, 4 – втрата основних рахунків, 5 – втрата довіри замовником, 9 – серйозна шкода бренду)
- Невідповідність (наприклад 2 – невелике порушення, 5 – серйозне порушення, 7 – високопрофільне порушення)
- Порушення приватності (наприклад 3- індивідуальне, 5 – сотні людей, 7 – тисячі людей, 9 – мільйони людей)

Обчислення збитків аналогічне обчисленню ймовірності загроз, проте технічні фактори та фактори впливу на бізнес обраховуються окремо, оскільки асоційований ризик може бути технічним, але не обов'язково впливати на бізнес та навпаки.

В такому випадку:

$$C = \frac{\sum_{i=1}^n t_i}{n}$$

Де $n = 4$, а t_i – значення факторів технічного впливу або факторів впливу на бізнес.

Тепер, обчислення ризику згідно методології OWASP виглядає наступним чином:

$$R = P * C = \frac{\frac{1}{n}(\sum_{i=1}^n x_i + \sum_{i=1}^n y_i)}{2} * \frac{\sum_{i=1}^n t_i}{n}$$

Фінальне значення ризику, залежно від факторів вразливості співставляються рангам, відповідно до матриці рівнів ризиків:

Таблиця 3.1 – Матриця рівнів ризиків

Ймовірність	Збитки				
		0 – 2,5	2,5 - 5	5 – 7,5	7,5 - 9
	8 - 9	Високий	Високий	Екстремальний	Екстремальний
	6 - 8	Середній	Високий	Високий	Екстремальний
	4 - 6	Низький	Середній	Високий	Екстремальний
	2 - 4	Низький	Низький	Середній	Екстремальний
	0 - 2	Низький	Низький	Середній	Високий

Після присвоєння рангів вразливостям, в SOC необхідно переглянути всі визначені вразливості та розставити пріоритети стосовно того, які ризики необхідно усувати першим чином.

Подальше управління та реакцію на вразливості можна здійснювати як за допомогою автоматизованих інструментів, так і за допомогою моделей реакції на вразливості. Наприклад, в контексті SOC можна застосувати наступну модель реакції на вразливості від Cisco:

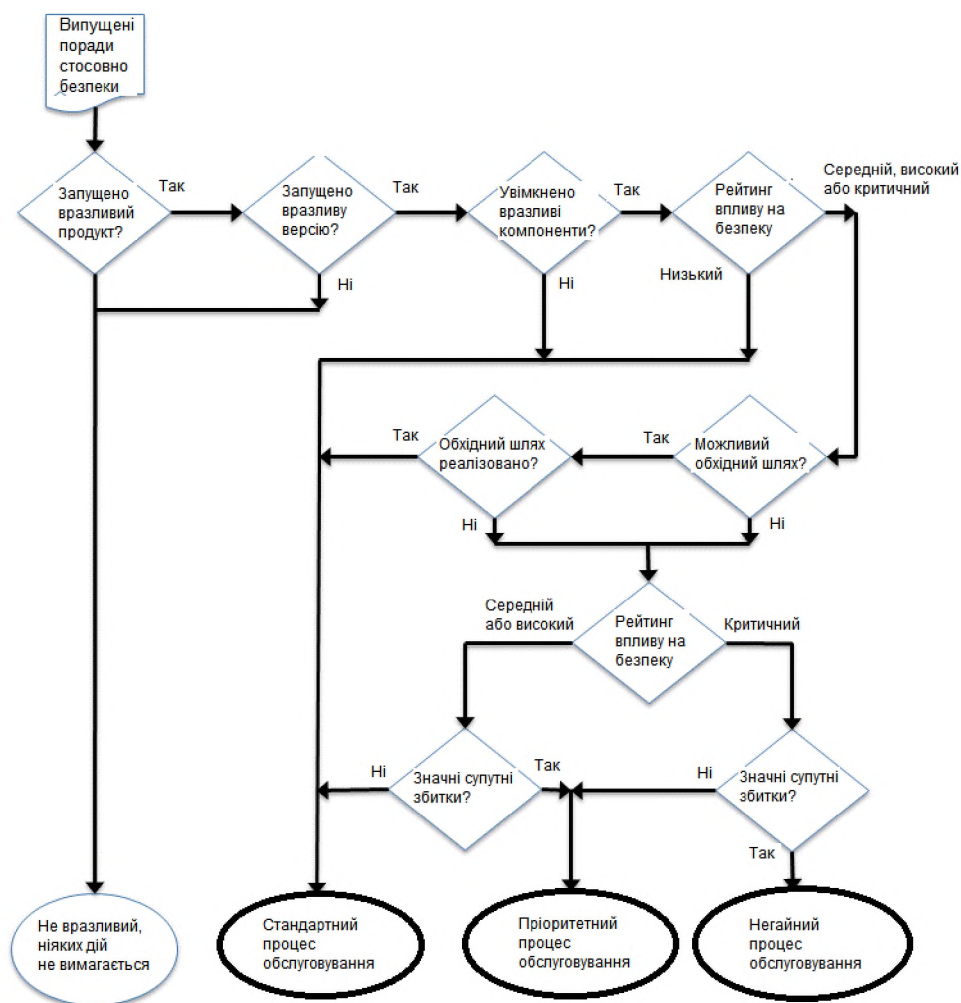


Рисунок 3.1 – Модель реакції на вразливості від Cisco

3.2.2 Розробка метрик інформаційної безпеки

Після оцінки ризиків, для забезпечення розробки метрик безпеки можна скористатись методом “Цілі-Запитання-Метрики”, що є трьохетапним процесом та включає: 1) визначення специфічних цілей, яких необхідно досягнути, 2) транслювання цілей в більш специфічні запитання, на які мають бути знайдені відповіді перед оцінкою досягнення поставлених цілей, 3) відповіді на запитання, шляхом ідентифікації та розробки підходящих метрик та збору даних, що асоційовані з вимірюваннями.

Для прикладу, розпишемо даний метод в контексті проекту посилення примусового виконання політики безпеки для SOC:

Компоненти цілі:

- Результат – посилення
- Елемент 1 – примусове виконання політики безпеки
- Елемент 2 – обізнаність користувачів
- Елемент 3 – підтвердження користувачем документів політики безпеки
- Точка зору – менеджер ІБ

Визначення цілі: Ціль даного проекту є посилення примусового виконання та обізнаності стосовно політики безпеки шляхом підтвердження користувачами документів політики безпеки з точки зору менеджера ІБ.

Запитання 1: Який поточний рівень примусового виконання політики безпеки?

Метрика 1.1: Кількість звітованих порушень політики безпеки за попередні 12 місяців

Метрика 1.2: Кількість примусових дій, прийнятих по відношенню до порушення політики безпеки за попередні 12 місяців

Запитання 2: Яка поточна структура політики безпеки?

Метрика 2.1: Кількість документів, включених в політику безпеки

Метрика 2.2: Формати документів політики безпеки

Метрика 2.3: Місцезнаходження документів політики безпеки

Метрика 2.4: Типи механізмів підтвердження політики безпеки

Метрика 2.5: Проміжок часу, від якого політика безпеки була останній раз переглянута

Запитання 3: Чи прочитав та зрозумів політику безпеки персонал?

Метрика 3.1: Кількість інформувань або навчань стосовно політики безпеки, проведених за попередні 12 місяців

Метрика 3.2: Співвідношення працівників, які офіційно прийняли політику безпеки за попередні 12 місяців

Метрика 3.3: Результати опитування користувачів стосовно того, наскільки користувачі ознайомлені з політикою та наскільки правильною та корисною є політика

Запитання 4: Чи посилюється впровадження політики безпеки?

Метрика 4.1: Підвищення ефективності процесу політики безпеки

Метрика 4.2: Посилення виконання політики безпеки п відношенню з початковим рівнем

Отже, шаблони “Цілі-Запитання-Метрики” можна застосовувати для структуризації та побудови процесу збору метрик, а також для безпосередньої розробки більш комплексних структур – проектів вимірювання.

3.2.3 Обчислення кількості подій на секунду

Перед початком збору даних необхідно розглянути наступні важливі аспекти:

- Скільки пристроїв надсилають дані?
- Скільки подій на секунду генеруються кожним пристроєм?
- Які вимоги стоять до зберігання отриманих даних?

Крім того, перед початком збору даних необхідні обчислення кількості подій, що генеруються пристроями, для уникнення завищення або заниження розмірів етапу збору даних. Такий підхід може бути застосований для мережі, де немає можливості протестувати пристрої для обчислення апроксимованого значення кількості подій та секунду. Позначимо кількість подій як N , а період часу, потягом якого вони були згенеровані, як t . Тоді кількість подій за секунду обраховується як:

$$\text{КПС} = \frac{N}{t}$$

Кількість подій залежить від великої кількості факторів, тому для врахування коливань КПС необхідно враховувати також і пікові значення КПС. Пікові значення важливі для розгляду, оскільки зазвичай тоді відбуваються інциденти. Врахування пікових значень може бути виконане за допомогою врахування наступних факторів:

- Очікувана кількість пікових значень
- Тривалість піку (в секундах)
- Коефіцієнт відхилення між нормальними КПС (наприклад від 2 до 5 КПС)

Позначимо очікувану кількість пікових значень як λ , тривалість піку як τ , а коефіцієнт відхилення – d . Тоді для обчислення загальної кількості пікових значень КПС (Λ) на день застосовуємо наступну формулу:

$$\Lambda = \text{КПС} * \lambda * \tau * d$$

Відповідно пікове значення КПС обчислюємо наступним чином:

$$\text{ПКПС} = \frac{\text{КПС} * \lambda * \tau * d}{86400} = \frac{\Lambda}{86400}$$

Після налаштування відповідних джерел даних та визначення попередньої кількості подій, що потенційно буде генеруватись з кожного джерела необхідно переходити до аналізу даних.

3.2.4 Методики та інструменти аналізу даних метрик інформаційної безпеки

Для метрик інформаційної безпеки можна застосовувати такі види аналізу:

- Прикладний аналіз – коли аналіз даних метрик безпеки розробляється для відповіді на відомі, специфічні питання, щодо аспектів програми безпеки. Зазвичай, уже відомо, що необхідно отримати від аналізу даних метрик та ймовірно уже існує певне усвідомлення, щодо результатів аналізу (наприклад –

адміністратор міжмережевого екрану повинен щомісячно звітувати про кількість прийнятих та відкинутих з'єднань через периметр захисту)

- Дослідницький аналіз – коли аналіз даних метрик інформаційної безпеки направлений на знаходження відповідей на нові питання, розробку таких нових питань на основі існуючої інформації та знань. Зазвичай аналіз даних якісних метрик є дослідницьким, оскільки ці техніки направлені на дослідження більш комплексних характеристик безпеки які є метою інтерпретації і розроблені для побудови абстрактних відношень та характеристик між організацією та персоналом

Аналіз даних метрик є найбільш ефективним, якщо він відбувається в контексті цілей для розробки та використання цих метрик впродовж часу. Перед початком аналізу важливо задати декілька уточнюючих питань: чого очікується досягти під кінець процесу аналізу? Чи аналіз відбувається для підтримки рішень чи вимог, чи це здійснюється для отримання нових знань? Основна ціль зрозуміти та описати зібрані дані чи використання даних для передбачень щодо програми безпеки?

Шкали даних, які можуть застосовувати в процесі аналізу можуть включати в себе:

- Номінальна (позначення та імена)
- Порядкова (вказує порядок ранжування)
- Інтервальна (дистанція між даними, що не включає в шкалу точку “нуль”, з якою можна було б провести порівняння)
- Співвідношення (дистанція між даними має кількісне значення, а також вводиться нульова точка)

Важливо розуміти, що може виникнути необхідність перенести дані з одної шкали в іншу, перед тим як ці дані використовувати.

Іншим важливим аспектом при роботі з даними – можуть виникнути значення, які не включені множину значень, або які випадають за межі нормальних діапазонів, в яких знаходиться основна маса даних. В таких випадках, необхідно

приймати рішення стосовно того, як обробляти такі ситуації, починаючи з того, чому такі значення взагалі з'явилися в даних.

Для перетворення, нормалізації, очищення даних можна застосовувати наступні техніки:

- Переведення значень даних в десяткові дробки або відсотки для простоти порівняння
- Групування та агрегування необроблених даних в категорії або контейнери для полегшення аналізу
- Зміна порядку значень або стандартизація оцінок значень для множин даних які застосовуються інші структури кодування
- Застосування описових статистик, таких як середнє значення, медіана, мода для порівняння значень
- Мінімум-максимум перетворення, які переводять усі отримані значення в новий діапазон попередньо заданих мінімальних та максимальних значень

Опишемо техніки та інструменти, які можуть бути застосовані для аналізу даних.

1) Описові статистики

На базовому рівні, аналіз даних включає підсумування та опис результатів спостережень та вимірювань, які були вжиті.

Аналіз даних зазвичай починається з підрахунку індивідуальних спостережень або значень, що містять дані вимірювань. Найбільш загальним результатом таких підрахунків є розподіл частот, де представлені та підраховані усі значення (прикладом зображення розподілу частот є використання гістограм). Взагалі поняття розподілу включає де і як конкретні значення та результати вимірювань знаходяться по відношенню до деякої шкали в загальному наборі даних.

Досить часто важливо розуміти, які значення в даних є найбільш наочними, найбільш середніми, найбільш очікуваними для загального набору даних. Такі характеристики кількісних даних лежать в основі багатьох статистичних аналізів,

особливо тих, які включають нормальний розподіл. В основі таких “центральных схильностей” лежать наступні описові статистики:

- Мода – значення, яке найчастіше зареєстровано в даних, що аналізуються (крім того, дані можуть бути мультимодовими, де мода розділена серед усіх значень з однаковою найвищою частотою). Особливо корисна для даних в номінальних шкалах. Для інтервального ряду мода визначається за формулою:

$$M_0 = X_{M_0} + h_{M_0} * \frac{f_{M_0} - f_{M_{0-1}}}{((f_{M_0} - f_{M_{0-1}}) + (f_{M_0} - f_{M_{0+1}}))}$$

де, X_{M_0} – ліва межа модального інтервалу, h_{M_0} – довжина модального інтервалу, $f_{M_{0-1}}$ – частота передмодального інтервалу, f_{M_0} – частота модального інтервалу, $f_{M_{0+1}}$ – частота післямодального інтервалу.

- Медіана – середина розподілу даних. Може бути обчислена для даних, що знаходяться в порядковій, інтервальній або шкалі співвідношень. Особливо корисна, коли дані містять сторонні значення або спотворені дані, які можуть негативно вплинути на загальне середнє значення. Медіана може забезпечити альтернативне вимірювання “центральных схильностей”, на яке не впливають сторонні/спотворені дані та яке надає більш точну картину. В загальному вигляді представлена формулою:

$$P(X < \chi) = P(X > \chi) = 0,5$$

де того, що випадкова величина матиме значення більше або менше за медіану однакова і дорівнює 0,5

- Середнє значення, що відповідає формулі:

$$\chi = \frac{1}{n} \sum_{i=1}^n x_i = \frac{1}{n} (x_1 + \dots + x_n)$$

де n – кількість елементів вибірки, x_i – власне елементи вибірки

Іншими описовими статистиками, які працюють з даними в контексті розподілу даних поміж спостережень – розсіювання. Розсіювання включає в себе наступні описові статистики:

- Діапазон – різниця між найвищим та найнижчим спостереженими значеннями в наборі даних
- Квартилі (поділ набору даних на 4 секції, кожна з яких буде містити 25% спостережених значень) та інтерквартилі (різниця між першим та третім кuartилями). Діапазони кuartилів можуть застосовуватись як базові дескриптори, які дозволяють швидко ідентифікувати низькі та високі значення в даних). Наприклад, перший кuartиль може бути представлений у вигляді математичної формули:

$$Q_1 = X_{Q_1} + i * \frac{0,25 \sum f - S_{Q_1-1}}{f_{Q_1}}$$

- Дисперсія – показує, як значення розподілене, по відношенню до середнього значення набору даних. За означенням – математичне сподівання квадрату відхилення випадкової величини від її математичного сподівання (середнього значення) – що представлено у вигляді математичної формули:

$$\sigma^2 = \sum_x (x - \mu)^2 p(x)$$

Де σ^2 – дисперсія випадкової змінної, x – значення випадкової змінної, $p(x)$ – імовірність появи значення x_i випадкової змінної x , μ - математичне сподівання (середнє значення) випадкової змінної x

- Стандартне відхилення - найбільш загальна показник мінливості та розсіювання в наборі даних. Означає, наскільки імовірно чи не імовірно поява конкретного спостереження чи значення. Представлено в вигляді математичної формули:

$$\sigma = \sqrt{\sigma^2}$$

Зростання в стандартному відхиленні набору даних свідчить про зростання в поширенні даних в межах середнього значення набору даних. В нормальному розподіл в контексті стандартного відхилення, 68% усіх значень потраплять

всередину першого стандартного відхилення від середнього значення, 95% значень потрапить всередину двох стандартних відхилень від середнього значення; всередину трьох стандартних відхилень не потрапить лише 0,27% значень.

Серед інструментів для роботи з описовими статистиками слід виділити:

- Електронні таблиці – дозволяються створювати таблиці даних, підсумовувати дані. Надають можливості створення карт та діаграм результатів для кількісного аналізу
- Статистичне ПЗ (наприклад Minitab, R)

2) Математичні висновування (або виведені статистики)

Математичні висновування працюють лише з безпосередніми даними. Застосовуються для використання даних в контексті узагальнення знаходжень в сферах, для яких відсутні дані або для передбачення результату, на основі обмежених наборів даних, що відповідно вимагає нестандартних технік та аналітичних методів. За допомогою математичних висновувань можна будувати заключення про щось, що не було спостережене, на основі того, що уже було спостережене. Важливо при цьому визначити, наскільки необхідно бути впевненим в тому, чого необхідно досягти в результаті аналізу, та наскільки серйозний ризик слід прийняти стосовно того, що результати можуть бути невірними.

Основним поняттями математичних висновувань є:

- Виведення – включає загально використовувані шляхи узагальнення від зразка до популяції, з якої зразок був отриманий
- Передбачення – все що дає обізнаність в тому, що може відбутись, на основі того, що вже відбулось. Включає в себе знаходження шаблонів та тем в даних для прогнозування майбутніх подій шляхами, що відрізняються від аналогії зразок/популяція
- Симуляція – відображення речей, які складно спостерігати або зрозуміти в речі, які легше спостерігати та зрозуміти.

Найпоширенішою технікою в математичних висновуваннях є тестування гіпотез – пояснень які можуть бути або можуть не бути вірними. Тестування гіпотез необхідно для визначення чи гіпотеза, яка розглядається, коректно пояснює щось, що потребує пояснення. Найбільш часто для тестування гіпотез застосовуються t-критерій Стюдента та хі-квадрат-тест, які корисно застосовувати в аналізі метрик безпеки.

T-критерій Стюдента порівнює середнє значення набору даних з середнім значенням популяції. Іншими словами, виконується порівняння середніх значень двох наборів для визначення того, чи ці набори сильно відрізняються одне від одного. Математична формула для даної статистики представлена наступним чином:

$$t = \frac{|M_1 - M_2|}{\sqrt{\frac{\sigma_1^2}{N_1} + \frac{\sigma_2^2}{N_2}}}$$

де M_1 – середнє арифметичне першої вибірки, M_2 – середнє арифметичне другої вибірки, σ_1 – стандартне відхилення першої вибірки, σ_2 – стандартне відхилення другої вибірки, N_1 – об'єм першої вибірки, N_2 – об'єм другої вибірки. Після чого на основі отриманого значення визначається рівень значимості по таблиці критичних значень Стюдента, та робиться висновок про наявність відмін між групами даних.

Для прикладу, застосування такого тесту в метриках інформаційної безпеки може включати спостереження за довільним набором кінцевих точок системи на наявність екземплярів шкідливого програмного забезпечення, а потім використання тесту для виведення із набору середніх екземплярів доступу шкідливого ПЗ до всіх кінцевих точок компанії. Ще одним прикладом може бути оцінка результатів експерименту, який порівнює наслідки нової процедури безпеки у випадковому наборі системи в протиставленні контрольному набору в якому нові процедури не були впроваджені.

Хі-квадрат-тест може бути застосований для визначення, чи існує взаємозв'язок між значеннями даних, якщо дані аналізуються в категоризованих (номінальних чи порядкових) шкалах. Дозволяє порівняти спостережні розподіли частот з очікуваними розподілами частот, для визначення того, чи вони співпадають. Наприклад, нульова гіпотеза – відмінність між типами інцидентів безпеки поміж організаційними підрозділами – випадкова. Альтернативна гіпотеза – спостереження були незалежними, що сигналізує про зв'язок між типами інцидентів безпеки та організаційними підрозділами, в яких вони стались. Хі-квадрат-тест може бути використаний для відкидання чи прийняття нульової гіпотези. Статистика критерію хі-квадрат визначається співвідношенням:

$$\chi^2 = n \sum_{i=1}^k \frac{(\frac{n_i}{n} - P_i(\theta))^2}{P_i(\theta)}$$

де n_i – число вибірових значень, що потрапили в i -й інтервал, $P_i(\theta)$ – ймовірність потрапляння в інтервал. В основі даної статистики лежить вимірювання відхилень $\frac{n_i}{n}$ від $P_i(\theta)$. Гіпотеза, що перевіряється, відхиляється при більших значеннях статистики, коли обчислене по вибірці значення статистики χ_n^2 більше критичного значення $\chi_{r,\alpha}^2$.

Інструменти, що можуть застосовуватись для тестування гіпотез включають: Gnumeric, Minitab, R.

Окрім вищенаведених статистичних технік, при аналізі даних можуть застосовуватись також наступні:

- Прийняття рішень на основі довірчих інтервалів, де довірчий інтервал – це статистичний термін для діапазону, який має певний шанс утримувати конкретне значення. Довірчим інтервалом параметру Θ розподілу випадкової величини X , з рівнем довіри p , що породжений вибіркою (x_1, \dots, x_n) є інтервалом з межами $l(x_1, \dots, x_n)$ та $u(x_1, \dots, x_n)$, які є реалізаціями випадкових величин $L(X_1, \dots, X_n)$ та $U(X_1, \dots, X_n)$, таких, що

$$P(L \leq \Theta \leq U) = p$$

де граничні точки довірчого інтервалу l та u є довірчими границями. Якщо рівень довіри p високий (наприклад 0,95), то довірчий інтервал містить істинне значення Θ .

Така техніка може бути корисною при тестуванні гіпотез, де попередньо задається рівень значущості, який дозволяє бути певною мірою бути певним, що конкретне значення дозволить/не дозволить відхилити нульову гіпотезу. Заміна оцінок висока, середня, низька (наприклад загроза) в оцінці ризиків на довірчі інтервали для поточних втрат на основі експертизи та досвіду персоналу, який задіяний в оцінці є яскравим прикладом застосування довірчих інтервалів. Проте тут необхідно зазначити про важливість калібрування оцінок експертів.

Важливими для аналізу даних окрім прикладного та дослідницького аналізу є кореляційний та поздовжній аналізи.

Кореляційний аналіз відноситься до встановлення наявності відношень між об'єктами. Вимірювання проводяться за допомогою коефіцієнту кореляції. Кореляція широко адаптована в SIEM-системах та системах аналізу журналів. Є надійним джерелом для дослідницького аналізу.

Поздовжній аналіз призначений для переміщення програми аналізу метрик безпеки в сферу прикладного дослідження та розгляду інцидентів безпеки не тільки в розрізі того, що відбувається на даний момент, а у зв'язку з минулими та можливими майбутніми подіями. Вимагає чіткого розуміння цілей та метрик в контексті часу.

Окрім кількісного аналізу даних, важливим аспектом також є і якісний та змішаний (кількісно-якісний) методи аналізу. Причому кінцева мета як і кількісного, так і якісного аналізу однакова – ідентифікація шаблонів і прийняття заключень стосовно аналізованого набору даних. Основні відмінності обох методів аналізу даних можна звести в нижченаведену таблицю:

Таблиця 3.2 – Основні відмінності кількісного та якісного методів аналізу даних

	Якісні методи аналізу	Кількісні методи аналізу
1	Побудова оповідей (історій) на основі даних	Присвоєння даним номерів
2	Ідентифікація людей, місць, дій та тем, які є важливими для оповіді (історії)	Статистичні опис та тестування
3	Побудова широкої, строгої та деталізованої картини даних	Забезпечення специфічного пояснення окремих аспектів даних
4	Аналіз “вглибину” та забезпечення розуміння проблем, які не скрізь можуть мати місце	Аналіз “вширину” та забезпечення розуміння проблем, які можуть бути узагальненими для інших сфер

Основою якісних аналітичних технік є концепція кодування, або присвоєння тем та категорій даним.

Найчастіше кількісні та якісні методи аналізу даних застосовуються разом. Техніки, які при цьому можуть застосовуватись, включають наступні:

- Картографування та аналіз процесів.

Включає розробку карти процесу, яка є блок-схемою, що показує кожну активність та відношення між активностями для заданого процесу. Тобто інформаційна безпека розглядається та аналізується як бізнес-процес. Карта процесу генерується за допомогою збору вхідних даних від персоналу, який описує свої думки та точки зору стосовно процесу, з подальшим візуальним кодуванням цих даних в специфічні фігури та символи, які інтерпретуються аналітиком процесу. Описові статистики в створенні карти процесу допомагають зрозуміти, де можуть виникнути неефективні або “вузькі” місця в якісній карті процесу. Вивідні статистики в створенні карти процесу є

частиною експериментів або тестувань гіпотез для визначення того, чи зміна частин процесу вдосконалить результати метрик.

- Опитування та інтерв'ю.

Зворотній зв'язок можна використовувати як частину більшого набору даних для отримання більш точних та цінних знань. Фактично включає в себе якісне кодування у зв'язку із кількісним аналізом.

- Аналіз вмісту та тексту.

Текст є важливим елементом процесу забезпечення безпеки. Під текстом маються на увазі політики та процедури, бюджети та звіти, вихідні коди, файли конфігурацій, а також артефакти, що можна отримати в результаті написання з документів та записів. Текстовий аналіз може включати каталогування частот слів та оцінку граматичних структур. Незалежно від того, наскільки зрозумілою є впроваджена політика безпеки, чи скільки незалежних виразів існує у вихідному коді – текстовий аналіз може забезпечити корисні інструменти для дослідження таких метрик.

- Етнографія.

Включає в себе документування та аналіз усього, що відбувається в середовищі з подальшим структуруванням для представлення результатів в майбутньому. Крім того, аналітик, який відповідає за використання такої техніки аналізу не тільки веде спостереження за середовищем, а й сам приймає в ньому участь. Наприклад, необхідно оцінити в середовищі операційного центру безпеки, що співробітники такої організаційної структури роблять кожного дня. В такому випадку, множина описових статистик та вивідних гіпотез – не застосовна. А впровадження проекту вимірювання безпеки у формі вправ для спостереження за учасниками дозволить зручно вирішити питання такої оцінки середовища.

Для якісних та змішаних методів аналізу можна застосовувати такі інструменти:

- Програмне забезпечення для аналізу якісних даних (або CAQDAS), наприклад Atlas.ti, Nvivo, TAMS analyzer, Weft QDA, Transana.

- ПЗ для картографування та аналізу процесів, наприклад Microsoft Visio, smart-Draw, OmniGraffle
- Програмне забезпечення для аналізу тексту та вмісту, наприклад ті ж CAQDAS, або більш лінгвістично сфокусоване ПЗ, яке пропонує тести та вимірювання стосовно структурних, граматичних та лексичних елементів текстових даних – WordStat, WordSmith.

Підсумовуючи вище сказане, аналіз метрик інформаційної безпеки, які виробляють після створення проектів вимірювання, є критичним компонентом досягнення успіху в управлінні процесами забезпечення інформаційної безпеки. При розгляді статистичного аналізу, шкала вимірювання є дуже важливим елементом, оскільки деякі статистики застосовуються лише до даних в інтервальних шкалах та шкалах співвідношень.

3.3 Розробка проекту вимірювання інформаційної безпеки

Проектом вимірювання інформаційної безпеки будемо називати певну організаційну структуру, яка містить і направляє процес збору метрик безпеки. Такі проекти дозволять модулювати діяльності, пов'язані з метриками і створювати більш прості для управління структурні блоки для вдосконалень безпеки в довгій перспективі.

Передумови побудови проекту. Необхідними передумовами побудови проекту є:

- Аналіз “Ціль-Запитання-Метрика” (причому такий аналіз повинен бути формально задокументований та застосовний як базовий документ в репозиторії проекту)
- Огляд попередніх проектів/програм
- Збір та аналіз метрик безпеки

Вибір типу проекту. При розробці проектів вимірювання безпеки важливо з самого початку вирішити, який тип проекту буде розроблятися. На основі опису методів аналізу метрик безпеки визначаються і проекти:

- Описовий проект
- Експериментальний проект

Описовий проект описує поточний стан в деяких аспектах інформаційної безпеки. Наприклад, якщо відбувається збір даних в контексті статистики подій та інцидентів для представлення їх на управлінській зустрічі – описовий проект завершено.

Експериментальний проект застосовує тести та процедури для отримання подальших знань, аналізу передіснуючої інформації. До експериментальних може відноситись будь який проект, в якому порівняння спостережень веде до деяких заключень щодо становища безпеки. Ціллю такою проекту є управління аналізом та результатами спостережень для формування ідеї, щодо причин наявності відмінностей між різними станами середовища.

Окремо слід виділити проекти відповідності, метою яких є дотримання програмою безпеки певних критеріїв чи специфікацій, розроблених органами влади. Важливою деталлю таких проектів є визначення зовнішніх зацікавлених сторін, яких потрібно залучити, для підвищення імовірності досягнення успіху.

Для забезпечення зв'язку між проектами вимірювання безпеки можна вбудувати міжпроектний функціонал в програму метрик безпеки. Будь який спосіб такого вбудовування вимагає, щоб власники та зацікавлені особи проектів спершу взяли на себе відповідні зобов'язання, для забезпечення того, що проекти залишаться пов'язаними. Крім міжпроектного функціоналу необхідно побудувати каталог проекту – описові документи та таблиці для більшої структурованості даних.

Оцінка ресурсів. Після вибору типу проекту, визначення власників та включення необхідних зацікавлених сторін необхідно оцінити ресурси, які наявні для реалізації проекту. Надійною практикою є розробка проекту в обмеженій сфері застосування, який є керованим та може забезпечити додаткову цінність для безпеки. Тобто, невеликий, добре зкоординований проект надасть більш точний

контроль над програмою інформаційної безпеки. При простішому масштабі завершити проект також буде набагато легше. Важливим аспектом оцінки ресурсів є проведення аналізу ризиків проекту вимірювання.

Ресурси та специфічні проблеми, пов'язані з ними, як частина аналізу ризиків – можна поділити на наступні:

- 1) Людські ресурси. Типовими питаннями при аналізі ризиків є: які ризики представлені власне зацікавленими особами проекту? Що може статися з проектом у результаті відмови зацікавленої сторони в підтримці проекту? Що може статись при втраті ресурсів через непередбачувані обставини?
- 2) Матеріальні та операційні ресурси. Типовими питаннями при аналізі ризиків є: які ресурси є критичними для успіху проекту? Чи можуть конкретні джерела даних, інструменти, місцезположення, грошові ресурси серйозно впливати на проект, при втручаннях в них, або при недоступності?
- 3) Технічні та аналітичні ресурси. Типовими питаннями при аналізі ризиків є: які ризики накладаються обраними технологіями та інструментами? Які інструменти обрані для завершення проекту – комерційні чи з відкритим вихідним кодом? Що може статись, якщо знадобиться новий інструмент протягом виконання проекту?
- 4) Планування надзвичайних випадків. Типовими питаннями при аналізі ризиків є: для усіх ризиків, асоційованих з проектом, якими є плани на надзвичайні випадки для вирішення будь-якого можливого ризику? Чи доступні обхідні шляхи та чи будуть конкретні ризики загрожувати успішному завершенню проекту? Чи повідомлені всі ризики та надзвичайні ситуації зацікавленим сторонам проекту?

Окрім оцінки ресурсів не менш важливим етапом розробки проекту є розробка його формального економічного обґрунтування. Таке формальне економічне обґрунтування повинно включати визначення та опис:

- Зацікавлених сторін проекту
- Цілей, запитань, метрик
- Вартості та переваг проекту

- Результатів аналізу ризиків
- Офіційне прийняття проекту

Підготовчі етапи розробки проекту завершені. Далі необхідно переходити до основних етапів розробки проекту.

Етап 1. Побудова плану проекту та збір відповідальної команди

Планом проекту вважаємо задокументовану операційну карту всього проекту, яка розроблена для запису усіх деталей в одному місці. План повинен охоплювати цілі, результати, кроки проекту на рівні деталізації, яка перевищує формальне економічне обґрунтування проекту та робить проект ефективно керованим.

- Цілі проекту. Повинні включати опис зацікавлених сторін та асоційованих з ними пріоритетів, які відображають економічне обґрунтування.
- Практичні результати проекту. Повинні включати описові звіти, отримані дані від експериментів чи виведених статистик, готовність пройти аудит, встановлення інших проектів, які є частиною програми вдосконалення. Результати повинні бути задокументовані та явно узгоджені з цілями, яким вони повинні слідувати та які вони повинні підтримувати.
- Етапи проекту. Повинні бути встановлені для всіх практичних результатів проекту, беручи при цьому до уваги доступні для проекту ресурси та складність кінцевих практичних результатів. Етапи повинні розроблятися на індивідуальній основі для кожного завдання та підзавдання проекту. Ці завдання повинні бути присвоєними власникам всередині команди відповідальних працівників. Часові рамки проекту також мають бути розроблені та встановлені разом з етапами.
- Деталі проекту. План проекту повинен надавати можливість учасникам відповідальної команди додавати деталі та відслідковувати проект по мірі його протікання.

Команда проекту. Являє собою співробітників відділу інформаційної безпеки, яких призначено на проект, на основі ролей та володіння ресурсами, які проект розроблений виміряти. Основними аспектами при присвоєння проекту команді співробітників є:

- Навички. Потрібно, принаймні, співставити співробітників із задачами проекту, для яких вони є найбільш підходящими.
- Зобов'язання
- Співробітництво. Визначає, як команда буде співпрацювати, а також забезпечує документування важливої проектної інформації як частини каталогу проекту.

Етап 2. Збір даних метрик інформаційної безпеки

Важливими аспектами при зборі даних метрик на другому основному етапі проекту є:

- Розгляд питання чи необхідні дані є безпосередньо доступними через існуючі системи та ресурси?
- Якщо дані залежать від взаємодії з людьми, через опитування, інтерв'ю, чи інші типи взаємодії, необхідно визначити, з ким необхідно спілкуватись та отримати відповідне підтвердження
- При виявленні факту відсутності необхідних даних необхідно шукати інше сховище або змінювати вимоги та цілі на основі джерел даних, які насправді можна знайти

Етап 3. Аналіз даних метрик та побудова заключень

Аналіз даних метрик та побудова заключень відбувається на основі попереднього розділу.

Важливими аспектами при аналізі метрик та побудові заключень є:

- План аналізу повинен бути розробленим достроково та явно включений в план проекту

- Розробка критеріїв та порогових значень як частини підтвердженого та підтриманого плану проекту дозволить більш легко уникнути неочікуваних знахідок чи заключень, особливо при звітуванні зацікавленим сторонам
- Необхідно впевнитись, що включено адекватний часовий проміжок для вивчення даних та розробки заключень

Етап 4. Презентування результатів проекту

Групи осіб, яким результати проекту повинні бути представлені включають:

- Нетехнічні менеджери
- Технічні менеджери
- Операційний персонал
- Користувачі
- Зовнішні зацікавлені сторони

Результати проекту можна представити у вигляді тексту (письмових звітів), візуальних елементів (гістограм, кругових діаграм, лінійних графіків; карт – для візуального опису процесів, відношень між джерелами даних та результатами), показників та матриць.

Етап 5. Повторне використання даних

Зазвичай спостерігається негативна тенденція недостатньої тривалості та повторного використання даних безпеки в проектах та впродовж життєвого циклу об'єкту дослідження. Для цього слід застосовувати спеціалізоване ПЗ управління проектами, для планування та виділення ресурсів, відслідковування етапів та аналізу ризиків проекту).

Підсумовуючи вище сказане, проекти вимірювання інформаційної безпеки дозволять створити модулярну програму метрик безпеки, в контексті чітко обмежених цілей, які пов'язані та повторно використовуються протягом часу, для полегшення постійного вдосконалення інформаційної безпеки.

3.4 Управління вимірюванням рівня інформаційної безпеки за допомогою програми безпеки

Програма безпеки розробляється для контекстуалізації вимірювань безпеки, щоб метрики та дані, які є результатами певних операцій вимірювання безпеки застосовувались як і у стратегічний, так і у тактичний спосіб. Найбільш важливим аспектом у програмі безпеки є відношення між індивідуальними проектами вимірювання безпеки. Проекти вимірювання безпеки можуть забезпечити даними та знаннями, але лише через програмний підхід програми безпеки, де індивідуальні активності, спрямовані на вимірювання безпеки можуть бути застосовані для управління інформаційною безпекою як бізнес процесом.

Проекти вимірювання безпеки стосуються збору та аналізу даних, для підтримки цілей та запитань за шаблоном “Цілі-Запитання-Метрики”, які були встановлені для кожного проекту. В свою чергу, програма безпеки повинна робити дані, отримані від проектів, більш корисними для більшої кількості людей та в більшій кількості контекстів.

Підхід програми безпеки фокусується не на негайних результатах кожного окремого проекту, а на спробі визначити чи змінювався рівень безпеки, як результат усіх проектів вимірювання безпеки.

Важливим моментом, в контексті створення програми безпеки, є орієнтація на репліковані або на повторювані проекти. В першому випадку, це здатність переносу запитань та вимог від першого проекту вимірювання безпеки до нового, відокремленого проекту. В другому випадку, це здатність співставлення результатів відповідних проектів серед усіх інших проектів.

Вимоги. Необхідними вимогами до розробки програми безпеки мають бути:

- Документація проектів вимірювання безпеки та усіх діяльностей, пов’язаних з ними
- Розповсюдження результатів вимірювання безпеки

- Забезпечення взаємозв'язку між проектами впродовж часу

Особа, відповідальна за розробку та впровадження програми безпеки, повинна слідкувати за забезпеченням координування індивідуальних проектів, генерації та зберігання для майбутнього використання відповідної документації, звітування результатів програми на основі регулярних інтервалів.

Визначення елементів та цілей програми безпеки

- Визначення безпеки
- Визначення вдосконалення. Вдосконалення повинне бути визначене не як корекція наявних проблем, а як ідентифікація кореневих причин проблем, для зменшення імовірності їх повторення в будь-яких формах. Вдосконалення також повинно розглядатись як встановлення базових рівнів та метрик рівня програми безпеки, які дозволять визначити чи здійснюється процес вдосконалення та в якій степені.

Документування програми безпеки

Запис мети та критерію успіху проектів вимірювання безпеки можуть бути представлені на найбільш базовому рівні за допомогою шаблону “Цілі-Запитання-Метрики”.

Для повноцінного документування проектів можуть застосовуватись такі джерела:

- Нотатки та записи учасників команди, яка відповідає за проект
- Документи та презентації проекту
- Результати аналізу проекту та одержані висновки
- Зворотній зв'язок від зацікавлених сторін та учасників команди, яка відповідає за проект

Визначимо базові компоненти документації програми безпеки:

- Оглядовий шаблон. Застосовується для ідентифікації, опису та визначення цілей програми безпеки

- Каталог проектів. Застосовується для відслідковування цілей, запитань та метрик, що асоційовані з індивідуальними проектами вимірювання безпеки
- Каталог метрик безпеки. Застосовується для документування видів та типів діяльностей, пов'язаних з вимірюванням безпеки, які були здійснені.
- Каталог результатів аналізу. Застосовується для зберігання висновків, а також можливостей та складностей, які можуть бути корисними для інших команд, які відповідають за проекти вимірювання безпеки.
- Журнали проектів. Застосовуються для полегшення збору інформації, специфічної для кожного проекту, яка не міститься в каталогах проектів чи фінальних звітах проектів.

Розповсюдження результатів вимірювання інформаційної безпеки

Після документування проектів, збору інформації впродовж та в результаті проектів – інформацію необхідно розповсюдити серед усіма уповноваженими особами. На базовому рівні, загальна інформація щодо проектів, метрик, результатів аналізу та зроблених висновків повинна бути широко доступною, як частина програми безпеки. Основні питання, які повинні розглядати при розповсюдженні необхідної інформації можуть бути наступними:

- Де будуть зберігатись відповідні документи?
- Яким чином будуть організовані документи? Чи будуть вони індексовані та з можливістю пошуку?
- Який контроль доступу буде встановлено на документи? Який процес підтвердження доступу до документів необхідно буде розробити?
- Як довго документи будуть зберігатись та обслуговуватись? Чи будуть архівуватись, та чи на регулярній основі?
- Яким чином будуть відслідковуватись документи, та як буде підтверджуватись їх автентичність?

Забезпечення взаємозв'язку між проектами впродовж часу

Метою програми безпеки є підвищення обізнаності, щодо специфічних проектів вимірювання безпеки, та діяльностей, пов'язаних з цим, для включення проектних команд, які можуть бути ведучими схожих проектів, а також для більш ефективної та значимої розробки нових проектів. Взаємозв'язок може бути забезпечений наступними шляхами:

- Миттєва комунікація за допомогою e-mail, месенджерів
- Мозкові штурми та відображення результатів на карті проектів
- Системи рецензування

Метрики програми безпеки

Вимірювання програми безпеки включає більш специфічні та програмно-орієнтовані метрики. Метою вимірювань в даному випадку є те, як часто програма безпеки використовується та наскільки якісно. Метою метрик програми безпеки є констатація факту, чи здійснюються щоденні активності, які сприяють довгостроковому вдосконаленню безпеки. Прикладами таких метрик можуть бути:

- Скільки проектів вимірювання безпеки включають формальний огляд попередніх, пов'язаних проектів?
- Скільки проектів (кількість чи коефіцієнт) було задокументовано та зроблено доступними?
- Як часто активності та метрики, пов'язані з програмою безпеки включаються в список предметів для обговорення, в плани проектів?
- Для скількох працівників цілі вдосконалення інформаційної безпеки формально включені в робочі обов'язки чи плани виконання?

Для доведення факту, що програма безпеки дійсно працює, слід шукати наступні докази:

- Чи змінюються базові рівні потягом часу? Чи відрізняються якість, кількість чи характер вимірюваних активностей, пов'язаних з інформаційною

безпекою між собою після кожного успішного проекту? Якщо виявлено зміни, то чи суттєві вони?

- Чи додано, переглянуто та впроваджено більшу кількість проектів в програму безпеки? Чи призводять активності, пов'язані з вимірюваннями, до повторюваних активностей, та чи утворюють нові активності, які вдосконалюють вимірювання безпеки та надають більше знань?
- Чи стає інформаційна безпека більш помітною всередині організації?
- Чи зменшуються з допомогою вимірювань безпеки ризики? Чи дозволяють результати метрик безпеки та програми безпеки приймати більш обгрунтовані рішення (включаючи рішення, де зазвичай інформаційна безпека не бере участь)?

3.5 Оцінка здатностей SOC

При досягненні рівня програм вимірювань безпеки, важливим моментом є оцінка поточних здатностей SOC. Необхідно визначити по яким основним процесам чи критерія необхідно виконувати оцінку основних складових 3-х ключових компонентів SOC.

Опишемо основні оцінки, які повинні бути розглянуті в контексті усіх складових ключових компонентів SOC.

Для компоненту “люди” опишемо оцінки по складових:

Керівництво:

- Оцінка рівня обізнаності вищих керівників стосовно важливості SOC
- Оцінка рівня залучення та інвестування вищих керівників в підтримці SOC
- Оцінка рівня існуючих здатностей звітування

Структура:

- Оцінка організаційної структури та моделі звітування
- Оцінка якості формалізації та документування організаційної структури

- Оцінка взаємовідносин між різними ролями та департаментами, які включені в оперування безпекою
- Оцінка процесу обміну інформацією між людьми та департаментами

Досвід:

- Оцінка управління інцидентами
- Оцінка цифрового розслідування
- Оцінка вразливостей
- Оцінка управління журналюванням
- Оцінка роботи з SIEM

Для компоненту “процеси” опишемо оцінки по складових:

Сортування по інцидентам:

- Оцінка формалізації процесу сортування по інцидентам
- Оцінка процесів класифікації та пріоритизації інцидентів

Звітування по інцидентам:

- Оцінка наявності процесів для ідентифікації необхідних типів звітів, частоти звітності, структури звітів
- Оцінка здатності звітування по інцидентам в робочі та неробочі години

Аналіз інцидентів:

- Оцінка процесів аналізу інцидентів безпеки у співставленні із класифікацією інцидентів
- Оцінка процедур отримання та аналізу даних з різних технічних елементів
- Оцінка наявності процесів включення внутрішніх та зовнішніх сторін в аналізі та розслідування інцидентів безпеки

Закриття інцидентів:

- Оцінка наявності процесів ліквідації компрометацій безпеки
- Оцінка наявності процесів маркування інцидентів, як закритих

Активності після інцидентів:

- Оцінка процесів зберігання зібраної інформації та обміну цією інформацією під час інцидентів
- Оцінка обговорення серйозних інцидентів

Виявлення вразливостей:

- Оцінка наявності процесів виявлення вразливостей
- Оцінка наявності процесів отримання повідомлень про нові вразливості
- Оцінка наявності процесів оцінювання впливу вразливостей та пріоритизації дій щодо відновлення

Усунення та відслідковування вразливостей:

- Оцінка наявності процесів поширення інформації про вразливості серед власників та операторів
- Оцінка наявності процесів усунення та відслідковування статусу виявлених вразливостей

Для компоненту “технології” опишемо оцінки по складових:

Мережева інфраструктура:

- Оцінка сфери застосування та покриття мережі (фізичної чи логічної), яка використовується для управління та моніторингу систем SOC
- Оцінка здатностей високої доступності критичних систем
- Оцінка рівнів продуктивності мережі

Збір, кореляція та аналіз подій

- Оцінка плану збору подій
- Оцінка масштабованості платформи збору, кореляції та аналізу подій
- Оцінка налаштованості систем до передачі подій
- Оцінка наявності списку сценаріїв використання
- Оцінка оптимізації платформи аналізу та кореляції подій для списку сценаріїв використання

Моніторинг

- Оцінка перехоплення та аналізу мережевих потоків
- Оцінка перехоплення та аналізу мережевих пакетів
- Оцінка здатності звітування
- Оцінка проблем в моніторингу, наприклад місць, які не відслідковуються, чи затримки між звітами
- Оцінка здатностей моніторингу протягом робочого та після робочого часу

Контроль

- Оцінка відповідних контролів безпеки, як от чи міжмережевий екран або IDS/IPS захищають сервери
- Оцінка правильності налаштування безпеки, тобто чи генеруються відповідні події
- Оцінка наявності застосованого рольового контролю доступу та усіх критичних пристроях для забезпечення доступу лише авторизованих користувачам

Управління журналами

- Оцінка відповідності платформи управління журналами політиці організації по збереженню журналів
- Оцінка кількості пристроїв, які надсилають журнали та кількості тих, які їх не надсилають
- Оцінка звітування, сповіщення та здатності розповсюдження інформації між іншими системами системи управління журналами

Оцінка вразливостей

- Оцінка наявності інструментів для виявлення вразливостей
- Оцінка здатності інструментів виявляти різні типи вразливостей
- Оцінка підтримки інструментів
- Оцінка інтеграції вихідних даних інструментів із іншими платформами безпеки, наприклад SIEM

Відслідковування вразливостей

- Оцінка використання інструментів для відслідковування статусу невиявлених вразливостей

Для опису процесів управління з орієнтацією на стандартизацію, повторюваність та результати, а також вимірювання ефективності можна застосувати підхід під назвою “модель здатності процесу”. На основі аналогічних моделей зі стандарту COBIT, а також SEI інституту опишемо рівні, які визначають здатність процесу:

Рівень 0. Неіснуючий процес. Повна відсутність будь якого впізнаваного процесу.

Рівень 1. Початковий процес. Процес непередбачуваний, погано контрольований та реактивний. Організацією не забезпечено стабільне середовище для підтримки процесу.

Рівень 2. Керований процес. Процес характеризується проектами та зазвичай є реактивним. Процес задокументовано та підтверджено, але він не є завершеним або не підходить даному контексту організації.

Рівень 3. Визначений процес. Процес характеризується як визначений. Процес задокументовано та підтверджено. Процес є повним та відповідає контексту організації.

Рівень 4. Кількісно керований процес. Процес є вимірюваним та контрольованим. Встановлені контролі для оцінки застосування підтвердженого процесу.

Рівень 5. Оптимізований процес. Фокус на постійному вдосконаленні процесу. Регулярний процес перегляду дозволяє оцінити застосування раніше підтвердженого процесу та дозволяє організації постійно його оновлювати.

Оцінки в даній моделі побудовані на кількісній шкалі від 0 до 5. Застосування такої моделі дозволяє виміряти поточні можливості та відслідковувати прогрес по відношенню до заданих цілей. Оцінка здатностей SOC повинна проводитись стосовно усіх складових ключових компонентів – людей, процесів та технологій.

Візуалізація оцінок в контексті кожного ключового компоненту може бути представлена у вигляді наступної діаграми:

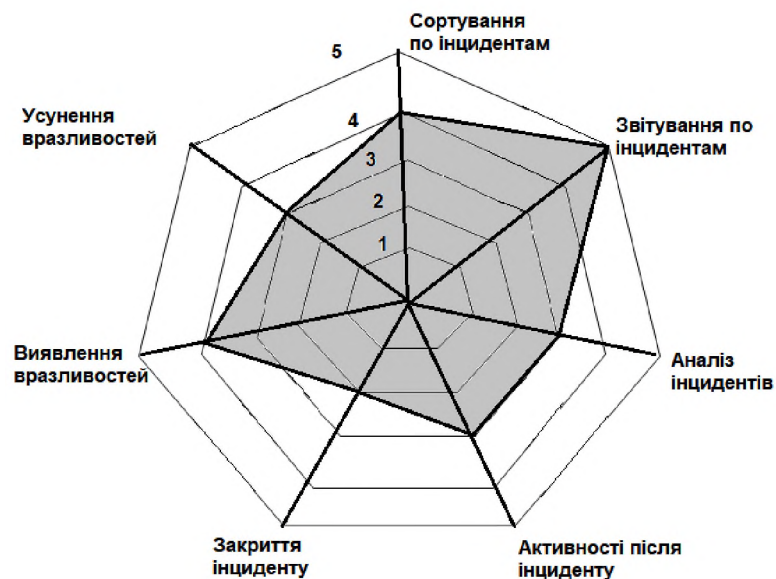


Рисунок 3.2 – Діаграма оцінки здатності основних складових процесів SOC

Висновки до розділу 3

Отже, на основі попередніх досліджень в контексті управління інформаційною безпекою та аналізу стандартів та фреймворків, для управління процесами безпеки, було запропоновано та описано фреймворк управління процесами безпеки для SOC, з орієнтацією на методики збору та аналізу даних.

Крім того, визначено компонентний склад SOC, в контексті усіх складових ключових компонентів. Визначена загальна архітектура фреймворку управління процесом ІБ на основі модульного підходу. Обрана методика оцінки ризиків, для якої визначено набір метрик. Зформульована методика розробки, збору та аналізу даних метрик ІБ. Розроблено поетапний проект вимірювання ІБ. Обрана методика оцінки здатностей SOC.

Представлений фреймворк дозволяє структурувати, вибрати необхідні методики, оцінити ризики, пов'язані з вразливостями та розробити стратегію управління процесами безпеки SOC, з можливістю оцінки здатностей операційного центру безпеки по основним складовим ключових компонентів.

4 СТАРТАП

4.1 Опис ідеї проекту

Таблиця 4.1 - Опис ідеї стартап-проекту

Зміст ідеї	Напрямки застосування	Вигода для користувача
Впровадження фреймворку управління процесами безпеки SOC. Створення стратегії фази оперування в SOC.	SOC в державних структурах в мережі замовника	Побудова, структурування та впровадження стратегії фази моніторингу SOC. Завершення циклу впровадження SOC. Більш досконале відслідковування безпеки мережі.
	SOC в приватних структурах в мережі замовника	Побудова, структурування та впровадження стратегії фази моніторингу SOC. Завершення циклу впровадження SOC. Більш досконале відслідковування безпеки мережі.
	SOC, які виведено на аутсорсинг	Побудова, структурування та впровадження стратегії фази моніторингу SOC. Завершення циклу впровадження SOC. Більш досконале відслідковування безпеки мережі.

Таблиця 4.2 - Визначення сильних, слабких та нейтральних характеристик ідеї проекту

1	2	3		4	5	6
№ п/п	Техніко - економ ічні характ еристи ки ідеї	(потенційні) товари/концепції конкурентів		W (слабка сторона)	N (нейтр аль на сторон а)	S (сильна сторона)
		Мій проект	Розробники та інтегратори SOC (Cisco, IBM, ISSP)			
1.	Еконо- мічні	Витрати на розробку та інтеграції рішення в існуючу інфраструктуру замовника, закупку відповідного ПЗ для роботи з даними, ліцензій, навчання спеціалістів та маркетинг – 30,000\$	Витрати на проектування, розробку та впровадження рішення, що включає повний цикл SOC, окрім фази оперування, закупку ліцензій, підтримку, зарплати спеціалістам, та маркетинг – 2,500,000 \$	Недостатній рівень витрат на маркетинг та рекламу	Немає	Дешевша реалізація проекту, з використанням конкретного підходу до створення та впровадження стратегії фази оперування SOC
2.	Техні- чні	Використання сучасних підходів в управлінні ІБ та роботі з даними	Автоматизовані засоби управління та аналізу	Складність у розробці стратегії враховуючи особливості інфраструктури	Немає	Більша кількість сфер використання рішення для забезпечення інформаційної безпеки

Кінець таблиці 4.2

1	2	3		4	5	6
№ п/п	Техніко- економі чні характ еристи ки ідеї	(потенційні) товари/концепції конкурентів		W (слабка сторона)	N (нейтр аль на сторон а)	S (сильна сторона)
		Мій проект	Розробники та інтегратори SOC (Cisco, IBM, ISSP)			
3.	Техноло -гічні	Немає	Немає	Немає	Немає	Немає
4.	Ергоно мічні	Можливість проектування та реалізації стратегії відповідно цілям та інфраструктури організації	Стратегія оперування проектується та впроваджується за допомогою готових шаблонів	Додаткова складність при впровадже нні	Немає	Різноманітність способів використання, що відповідає конкретним вимогам
5	Органо лепти- чні	Швидкодія моніторингу та виявлення інцидентів залежить від адаптації до існуючої інфраструктури	Швидкодія моніторингу та виявлення інцидентів залежить від розробки та впровадження нової інфраструктури	Немає	Немає	Можливість налаштування під конкретну інфраструктуру та цілі організації

4.2 Технологічний аудит ідеї проекту

Таблиця 4.3 - Технологічна здійсненність ідеї проекту

<i>№ n/n</i>	<i>Ідея проекту</i>	<i>Технології її реалізації</i>	<i>Наявність технологій</i>	<i>Доступність технологій</i>
1	Впровадження фреймворку управління процесами безпеки	Розробка та впровадження комплексної програми управління фазою оперування SOC	Потрібно реалізовувати самостійно	Так, ця технологія є доступною
2	Визначення та підключення необхідних джерел даних до SOC	Використання наявних технологій журналювання, генерації подій, перехоплення мережових пакетів та генерації мережової телеметрії поточної інфраструктури для інтеграції з SOC	Потрібно налаштовувати самостійно	Так, ця технологія є доступною
3	Застосування набору програмних засобів для кількісного та якісного аналізу даних	Використання програмного забезпечення, що входить в пакет підиски	Потрібно придбати ліцензії на програмне забезпечення	Так, ця технологія є доступною
Обрана технологія реалізації ідеї проекту: так як для реалізації ідеї проекту, всі технології є наявними та доступними, тому обираються всі вище описані технології.				

4.3 Аналіз ринкових можливостей запуску стартап-проекту

Таблиця 4.4 - Попередня характеристика потенційного ринку стартап-проекту

<i>1</i>	<i>2</i>	<i>3</i>
<i>№ n/n</i>	<i>Показники стану ринку розробки та впровадження SOC</i>	<i>Характеристика</i>
1	Кількість головних гравців, од	CISCO, IBM, ISSP

Кінець таблиці 4.4

<i>1</i>	<i>2</i>	<i>3</i>
<i>№ n/n</i>	<i>Показники стану ринку розробки та впровадження SOC</i>	<i>Характеристика</i>
2	Загальний обсяг продаж, грн/ум.од	1 млрд грн.
3	Динаміка ринку (якісна оцінка)	Зростає
4	Наявність обмежень для входу	Потреба у кадрах із високим рівнем компетентності у сфері інформаційної безпеки
5	Специфічні вимоги до стандартизації та сертифікації	Проведення експертиз щодо відповідності рішення вимогам, для отримання експертного висновку ДССЗІ у державних установах
6	Середня норма рентабельності в галузі, %	Не менше 100

Таблиця 4.5 - Характеристика потенційних клієнтів стартап-проекту

<i>№ n/n</i>	<i>Потреба, що формує ринок</i>	<i>Цільова аудиторія (цільові сегменти ринку)</i>	<i>Відмінності у поведінці різних потенційних цільових груп клієнтів</i>	<i>Вимоги споживачів до товару</i>
1	<p>Структурування та вдосконалення загального процесу збору та аналізу даних інформаційних систем на основі наявних методів та інструментів</p> <p>Оцінка здатностей інформаційних систем на основі простих в застосуванні та стандартизованих практик</p> <p>Структурування та вдосконалення загального процесу моніторингу, аудиту безпеки інформаційних систем</p>	<p>- SOC в державних структурах в мережі замовника</p> <p>- SOC в приватних структурах в мережі замовника</p> <p>- SOC, які виведено на аутсорсинг</p>	<p>Для кожної категорій існують окремі цінності пропонованого рішення, наприклад для приватних замовників важливо побудувати та структурувати процес моніторингу та вдосконалення безпеки власної мережевої/ інформаційної інфраструктури. Державні установи прагнуть отримати рішення, для відслідковування найбільш критичних елементів інфраструктури, а також для можливості отримання експертного висновку на основі стандартизованого продукту, або такого, що побудованих на основі наявних стандартів в інформаційній безпеці</p> <p>Замовники, чиї SOC виведені на аутсорсинг прагнуть отримати структуровану та документовану програму оперування SOC та здатність оцінити дієвість результатів надання послуг постачальниками.</p>	<p>- Забезпечення відмовостійкої та надійної роботи обладнання та сервісів, підтримка та оперування у режимі 24/7</p> <p>- Використання відповідного апаратного та програмного забезпечення, швидке усунення неполадок, проведення консультацій та навчання користувачів</p>

Таблиця 4.6 - Фактори загроз

<i>№ n/n</i>	<i>Фактор</i>	<i>Зміст загрози</i>	<i>Можлива реакція компанії</i>
1	Цінова конкуренція	Демпінг цін на послуги конкурентів	Зниження вартості продукту
2	Зниження доходів потенційних споживачів	Зниження купівельної спроможності клієнтів	Зниження вартості продукту
3	Поява аналогічних вузькоспеціалізованих конкурентів, або аналогічних послуг в поточних конкурентів	Поява аналогічних вузькоспеціалізованих конкурентів, або аналогічних послуг в поточних конкурентів	Зменшення ринкових можливостей продукту

Таблиця 4.7 - Фактори можливостей

<i>№ n/n</i>	<i>Фактор</i>	<i>Зміст можливості</i>	<i>Можлива реакція компанії</i>
1	Поява нових технологій, програмних інструментів та стандартів	Розширення спектру надаваних послуг для клієнтів, збільшення ефективності роботи сервісу,	Швидке впровадження нових технологій, створення нових сервісів
2	Залучення нових відомих компаній до співробітництва	Розширення використання пропонованого продукту	Розробка та впровадження нових засобів та програмних комплексів
3	Стабілізація політичного та економічного становища в державі	Зменшення рівня інфляції, збільшення кількості клієнтів	Спроби просування інтересів стартапу в державних та недержавних установах
4	Збільшення кількості кіберзагроз та кібератак	Збільшення попиту на послуги стартапу	Залучення нових клієнтів, можливе підвищення вартості послуг

Таблиця 4.8 - Ступеневий аналіз конкуренції на ринку

<i>Особливості конкурентного середовища</i>	<i>В чому проявляється дана характеристика</i>	<i>Вплив на діяльність підприємства (можливі дії компанії, щоб бути конкурентоспроможною)</i>
1. Олігополістична конкуренція	Динаміка цін, яка майже не залежить від рівню попиту на продукцію. Конкуренція зміщується в сторону реклами, рівня якості надаваних послуг та індивідуалізації	Вдосконалення рішення для підвищення якості надаваних послуг для клієнтів
2. За рівнем конкурентної боротьби - національний	Надання послуг для різних груп та типів клієнтів в Україні та в перспективі за її межами	Застосування нових технологій, стандартів, математичних моделей та підходів для вдосконалення рішення
3. За галузевою ознакою - міжгалузева	Рішення може використовуватися користувачами SOC різних галузей, що потребує розробки, структурування та автоматизацію рішень для досягнення індивідуальних цілей	Розширення функціоналу фреймворку, розширення сфери надання послуг, додання нових підходів сервісу та послуг для клієнтів
4. Конкуренція за видами товарів: - товарно-видова	Рішення, що використовується для задоволення потреб клієнтів, але технологічно відрізняються від рішень конкурентів на користь вузькоспеціалізованості, структурованості та якості сервісу	Надання послуг із розробки, адаптації та впровадження програми оперування SOC, збору та аналізу даних, базової оцінки здатностей SOC

Кінець таблиці 4.8

<i>Особливості конкурентного середовища</i>	<i>В чому проявляється дана характеристика</i>	<i>Вплив на діяльність підприємства (можливі дії компанії, щоб бути конкурентоспроможною)</i>
5. За характером конкурентних переваг - цінова	Цінова	Надання більш вузькоспеціалізованого спектру послуг, порівняно із конкурентами
6. За інтенсивністю - марочна	Сукупність характеристик та властивостей рішення	Підвищення якості відслідковування та моніторингу мережевої/ інформаційної інфраструктури клієнтів

Таблиця 4.9 - Аналіз конкуренції в галузі за М. Портером

	<i>Прямі конкуренти в галузі</i>	<i>Потенційні конкуренти</i>	<i>Постачальники</i>	<i>Клієнти</i>	<i>Товари-замінники</i>
<i>Складові аналізу</i>	CISCO, IBM, ISSP	Розмір капіталовкладень; доступ до ресурсів у конкурентів; наявність патентів та товарних знаків.	Поділ витрат, залежно від розмірів поставок.	Розміри закупівель державних підприємств та органів влади, силових структур;	Ціна товару та змінні витрати
Висновки:	Наявна досить інтенсивна конкурентна боротьба з боку прямих конкурентів	Є можливості входу на ринок, але існує багато конкурентів	Постачальники диктують умови роботи на ринку; при здійсненні більшого обсягу продажів слідує отримання привілеїв	Клієнти диктують умови на ринку; при організації закупівель товарів та послуг	Обмеження, через відсутність вузькоспеціалізованих послуг замінників – не наявні

Даний проект має принципові можливості для роботи на ринку з огляду на конкурентну ситуацію. Серед сильних сторін, можна виділити використання структурованого, вузькоспеціалізованого підходу, що надається в якості основної послуги, а не у вигляді підтримки за залишковим принципом, та на основі стандартизованих підходів в управлінні інформаційною безпекою, що не має аналогів в Україні, розробка, адаптація та впровадження під кожного конкретного замовника.

Таблиця 4.10 - Обґрунтування факторів конкурентоспроможності

<i>№ n/n</i>	<i>Фактор конкурентоспроможності</i>	<i>Обґрунтування (наведення чинників, що роблять фактор для порівняння конкурентних проектів значущим)</i>
1	Ціна	Ціноутворення індивідуальне для кожного клієнта
2	Гнучкість цін на продукт	Є можливість зменшення цін на продукт, в залежності від складності розробки та впровадження відповідно до інфраструктури замовника
3	Застосування структурованого, стандартизованого та вузькоспеціалізованого підходу в якості основної послуги	Вузькоспеціалізоване, проте комплексне надання послуг, з можливістю отримання експертного висновку в державних установах

Таблиця 4.11 - Порівняльний аналіз сильних та слабких сторін «Довірений монітор»

<i>№ n/n</i>	<i>Фактор конкурентоспроможності</i>	<i>Бали 1-20</i>	<i>Рейтинг товарів-конкурентів у порівнянні з довіреним монітором</i>						
			-3	-2	-1	0	+1	+2	+3
1	Ціна	10				+			
2	Гнучкість цін на послуги	13			+				
3	Різноманітний підхід	16		+					

Таблиця 4.12 - SWOT-аналіз стартап-проекту

<i>Сильні сторони:</i> структурований, вузькоспеціалізований та стандартизований підхід в якості основної послуги	<i>Слабкі сторони:</i> низький рівень маркетингу; покриває лише фазу моніторингу SOC; покриття конкурентами повного циклу SOC
<i>Можливості:</i> розробка, адаптація та впровадження унікального фреймворку залежно від особливостей інфраструктури та цілей замовника	<i>Загрози:</i> цінова конкуренція; зниження доходів потенційних споживачів;

Таблиця 4.13 - Альтернативи ринкового впровадження стартап-проекту

№ п/п	Альтернатива (орієнтовний комплекс заходів) ринкової поведінки	Ймовірність отримання ресурсів	Строки реалізації
1	Концентрація на одному чи двох типах клієнтів	Висока ймовірність отримання ресурсів	4 місяці
2	Побудова рішення на основі інфраструктури, де використовуються апаратні та програмні засоби одного вендора	Середня ймовірність отримання ресурсів та залучення підтримки вендора	3 місяці
3	Побудова та впровадження рішення в контексті повного циклу SOC	Мала ймовірність отримання ресурсів та залучення підтримки основного виконавця	8 місяців

З означених альтернатив ринкового впровадження даного стартап-проекту було вирішено обрати розробку та впровадження фреймворку з концентрацією на одному чи двох типах клієнтів при цьому часові межі реалізації приблизно становитимуть 4 місяці.

4.4 Розроблення ринкової стратегії проекту

Таблиця 4.14 - Вибір цільових груп потенційних споживачів

<i>1</i>	<i>2</i>	<i>3</i>	<i>4</i>	<i>5</i>	<i>5</i>
<i>№</i> <i>n</i> <i>/</i> <i>n</i>	<i>Опис профілю</i> <i>цільової групи</i> <i>потенційних</i> <i>клієнтів</i>	<i>Готовність</i> <i>споживачів</i> <i>сприйняти</i> <i>продукт</i>	<i>Орієнтовний</i> <i>попит в межах</i> <i>цільової групи</i> <i>(сегменту)</i>	<i>Інтенсивність</i> <i>конкуренції в</i> <i>сегменті</i>	<i>Простота</i> <i>входу у</i> <i>сегмент</i>
1	Державні організації та органи державної влади	Клієнти потребують продукту/ послуги такого типу та готові ним (нею) користуватись	Високий попит, пов'язаний із необхідністю отримання послуг у сфері кібербезпеки та управління інформаційною безпекою	Високий рівень конкуренції	Фактична відсутність вузькоспеціалізованих постачальників даного типу послуг.
2	Компанії середнього та великого бізнесу	Клієнти зацікавлені продуктом	Середній рівень попиту	Середній рівень конкуренції	Фактична відсутність вузькоспеціалізованих постачальників даного типу послуг

Таблиця 4.15 - Визначення базової стратегії розвитку

<i>№ n/n</i>	<i>Обрана альтернатива розвитку проекту</i>	<i>Стратегія охоплення ринку</i>	<i>Ключові конкурентоспроможні позиції відповідно обраної альтернативи</i>	<i>Базова стратегія розвитку</i>
1	Флангова атака	Стратегія диференційованого маркетингу	Вузькоспеціалізованість, сильні сторони та можливості рішення	Стратегія диференціації

Таблиця 4.16 - Визначення базової стратегії конкурентної поведінки

<i>№ n/n</i>	<i>Чи є проект «першопрохідцем» на ринку?</i>	<i>Чи буде стартап шукати нових споживачів, або забирати існуючих у конкурентів?</i>	<i>Чи буде стартап копіювати основні характеристики товару конкурента, і які?</i>	<i>Стратегія конкурентної поведінки</i>
1	Ні	Так	Ні	Стратегія виклику лідера

Таблиця 4.17 - Визначення стратегії позиціонування

<i>№ п/ п</i>	<i>Вимоги до товару цільової аудиторії</i>	<i>Базова стратегія розвитку</i>	<i>Ключові конкуренто- спроможні позиції власного стартап- проекту</i>	<i>Вибір асоціацій, які мають сформувати комплексну позицію власного проекту</i>
1	Отримання структурованої програми оперування SOC, а відповідно комплексного бачення управління процесами забезпечення безпеки та кращої спостережності та відслідковуваності мережевої/інформаційної інфраструктури з “одних” рук. Отримання знань від спеціалістів щодо управління інформаційною безпекою. Мінімізація втрат (як фінансових так і репутаційних), а також забезпечення управління інформаційною безпекою як складовою бізнесу.	Стратегія диференціації	Сильні сторони та можливості рішення	Побудова, адаптація та впровадження програми оперування та моніторингу безпеки в державних, приватних та аутсорсингових операційних центрах безпеки

4.5 Розроблення маркетингової програми стартап-проекту

Таблиця 4.18 - Визначення ключових переваг концепції потенційного товару/послуги

<i>1</i>	<i>2</i>	<i>3</i>	<i>4</i>
<i>№ п / п</i>	<i>Потреба</i>	<i>Вигода, яку пропонує товар/послуга</i>	<i>Ключові переваги перед конкурентами (існуючі або такі, що потрібно створити)</i>
1	Побудова та впровадження програми моніторингу, аудиту інформаційної безпеки в SOC	Побудова, впровадження, адаптація та структурування моніторингу, аудиту безпеки інформаційних / мережових інфраструктур на основі SOC	Отримання комплексних послуг з “одних” рук. Отримання знань від спеціалістів щодо управління процесами забезпечення інформаційної безпеки. Отримання єдиної програми моніторингу безпеки в SOC, унікальної для кожного клієнта.
2	Отримання єдиного сервісу моніторингу безпеки в SOC	Структурований, вузькоспеціалізований фреймворк управління інформаційною безпекою	Надання вузькоспеціалізованого спектру послуг, що не має аналогів; адаптивність цін на послуги. Кваліфіковані та сертифіковані кадри для виконання поставлених задач (розробка, адаптація, впровадження, аналіз подій та розслідування інцидентів, консалтинг).

Таблиця 4.19 - Опис трьох рівнів моделі товару/послуги

<i>Рівні товару/послуги</i>	<i>Сутність та складові</i>
I. Товар/послуга за задумом	Розробка, впровадження та адаптація програми управління процесами забезпечення безпеки (або програми оперування та моніторингу) в SOC. Консалтинг та підтримка.

Кінець таблиці 4.19

<i>Рівні товару/послуги</i>	<i>Сутність та складові</i>		
II. Товар/послуга у реальному виконанні	Властивості/характеристики	М/Нм	Вр/Тх /Тл/Е/Ор
	1. Використання методології OWASP Risk Assessment	М	Тх/Тл/Е
	2. Розробка метрик інформаційної безпеки для SOC	Нм	Вр/Тл/Е
	3. Використання готових математичних та програмних інструментів для роботи з даними метрик безпеки	М	Тх/Е/Ор
	4. Оцінка здатностей SOC на основі моделі здатності процесу	Нм	Тл/Е/Ор
	Якість: Забезпечення структурованою програмою моніторингу безпеки в SOC		
	Марка: SOC ISPM Framework		
III. Товар/послуга із підкріпленням	До продажу: для стимулювання попиту на продукт можна розробити програму проведення “пілотних проектів” та тестових впроваджень		
	Після продажу: Розробка та проведення рекламної кампанії		
За рахунок чого потенційний товар буде захищено від копіювання: захист інтелектуальної власності			

Таблиця 4.20 - Визначення меж встановлення ціни

<i>№ п/п</i>	<i>Рівень цін на товари- замінники</i>	<i>Рівень цін на товари- аналоги</i>	<i>Рівень доходів цільової групи споживачів</i>	<i>Верхня та нижня межі встановлення ціни на товар/послугу</i>
1	1500000 ум.од	Відсутня	Високий або середній	Ціна на розробку, впровадження та адаптацію фреймворку – 250000 ум. од.

Таблиця 4.21 - Формування системи збуту

<i>№ п/ п</i>	<i>Специфіка закупівельної поведінки цільових клієнтів</i>	<i>Функції збуту, які має виконувати постачальник товару</i>	<i>Глибина каналу збуту</i>	<i>Оптимальна система збуту</i>
1	Прийняття рішення про необхідність розробки стратегії моніторингу та керування безпекою, вибір джерела задоволення своїх потреб для забезпечення безпеки інформаційних систем і укладення угоди	Пристосування збутової мережі до запитів споживачів; пошук перспективних засобів просування товарів; розробка та вдосконалення маркетингової політики; вибір посередників	Дворівневий канал збуту (із залученням посередника та дистриб'ютора)	Залучення компаній посередників та партнерів для формування системи збуту

Таблиця 4.22 - Концепція маркетингових комунікацій

<i>№ п/ п</i>	<i>Специфіка поведінки цільових клієнтів</i>	<i>Канали комунікацій, якими користуються цільові клієнти</i>	<i>Ключові позиції, обрані для позиціонування</i>	<i>Завдання рекламного повідомлення</i>	<i>Концепція рекламного звернення</i>
1	Дослідження властивостей та якостей рішення, можливість тестової розробки та впровадження рішення, прийняття рішення про необхідність використання продукту для задоволення своїх потреб	Канали інтегрованих маркетингових комунікацій	Використання сильних сторін рішення: структурована програма побудови фази моніторингу SOC; використання методології OWASP Risk Assessment, розробка метрик інформаційної безпеки для SOC, оцінка здатностей SOC на основі моделі здатності процесу	Повідомлення, пов'язані з особистою вигодою аудиторії, що показують, як рішення може задовольняти потреби покупця;	Реклама, що демонструє якість рішення, його економічність, цінність або можливості експлуатації

Висновки до розділу 4

Результатом проведеного аналізу та оцінки ризиків, було виявлено, що даний проект має можливість для ринкової комерціалізації. Для представленого рішення є високий рівень попиту, що пов'язаний із відсутністю вузькоспеціалізованих послуг такого характеру, тому робота над проектом має гарну рентабельність на ринку послуг у сфері кібербезпеки. Для цього стартап-проекту є непогані перспективи входження в ринок, але наявні певні бар'єри, подолання яких підвищують конкурентоспроможність представленого рішення. Щодо альтернативи впровадження стартап-проекту та його ринкової реалізації, доцільно обрати механізми для побудови рішення з використанням компонентів однієї компанії постачальника

ВИСНОВКИ

В результаті попереднього дослідження були розглянуті поняття управління інформаційною безпекою та операційних центрів безпеки; проаналізовані архітектурні особливості, визначено компонентний склад SOC, та його функціональне наповнення, виділені основні проблеми, що виникають після впровадження операційного центру безпеки; проаналізовані основні підходи та методики в сучасних стандартах та фреймворках управління інформаційною безпекою. В результаті проведеного аналізу було виявлено наступне:

- Для операційних центрів безпеки відсутні будь-які вузькоспеціалізовані стандарти чи методології, які б допомагали побудувати процес оперування та управління процесами безпеки враховуючи аспекти даної організаційної структури
- Окреме застосування попередньо описаних стандартів та фреймворків не дає бажаних результатів в побудові та управлінні фазою оперування SOC.
- Застосування стандартів на практиці зазвичай складне та не відповідає встановленим очікуванням на фазі планування SOC

На основі попереднього аналізу розроблено фреймворк управління процесами безпеки для SOC, з орієнтацією на методики збору та аналізу даних.

Розроблений фреймворк дозволяє структурувати, вибрати необхідні методики, оцінити ризики, пов'язані з вразливостями та розробити методологію управління процесами безпеки SOC, з можливістю оцінки здатностей операційного центру безпеки по основним складовим ключових компонентів. Впровадження запропонованого фреймворку допоможе забезпечити кращу ефективність оперування SOC, а відповідно і кращу спостережність інформаційної чи мережевої інфраструктури за допомогою SOC.

ПЕРЕЛІК ДЖЕРЕЛ-ПОСИЛАННЯ

- 1 Information Security Management [Електронний ресурс] / Режим доступу до ресурсу: <https://www.sumologic.com/glossary/information-security-management/>
- 2 Information Security Management [Електронний ресурс] / Режим доступу до ресурсу: https://en.wikipedia.org/wiki/Information_security_management
- 3 Information Security Management [Електронний ресурс] / Режим доступу до ресурсу: <https://whatis.techtarget.com/definition/information-security-management-system-ISMS>
- 4 What is an Information Security Management System (ISMS) & How Should it be implemented? [Електронний ресурс] / Matt Klassen Режим доступу до ресурсу: <https://www.cherwell.com/library/blog/what-is-an-information-management-security-system/>
- 5 Операційний центр безпеки [Електронний ресурс] / Режим доступу до ресурсу: https://uk.wikipedia.org/wiki/Операційний_центр_безпеки
- 6 What is a Security Operations Center (SOC)? [Електронний ресурс] / Режим доступу до ресурсу: <https://www.mcafee.com/enterprise/ru-ru/security-awareness/operations/what-is-soc.html>
- 7 What is a Security Operations Center (SOC)? [Електронний ресурс] / Nate Lord Режим доступу до ресурсу: <https://digitalguardian.com/blog/what-security-operations-center-soc>
- 8 Как быстро запустить свой Security Operation Center (SOC)? [Електронний ресурс] / Т.Ниязов Режим доступу до ресурсу: <https://www.anti-malware.ru/analytics/Technology Analysis/How fast run SOC Security Operation Center>

- 9 Joseph Muniz, Gary McIntyre, Nadhem AlFardan, Security Operations Center: Building, Operating and Maintaining your SOC [Текст] / Cisco Systems, Inc. 2016. 448 р.
- 10 Международный стандарт ISO/IEC 27001:2013 [Электронный ресурс] / Режим доступа до ресурсу: https://www.certification.ua/wp-content/uploads/2018/03/ISO_27001_2013_МНС-ГРУПП.pdf
- 11 ISO/IEC 27001 [Электронный ресурс] / Режим доступа до ресурсу: https://ru.wikipedia.org/wiki/ISO/IEC_27001
- 12 Международный стандарт ISO/IEC 27002:2013 [Электронный ресурс] / Режим доступа до ресурсу: <https://pqm-online.com/assets/files/pubs/translations/std/iso-mek-27002-2013.pdf>
- 13 ГОСТ Р ИСО/МЭК 27002-2012 Информационная технология (ИТ) [Электронный ресурс] / Режим доступа до ресурсу: <http://docs.cntd.ru/document/1200103619>
- 14 ГОСТ Р ИСО/МЭК 27003-2012 Информационная технология [Электронный ресурс] / Режим доступа до ресурсу: <https://meganorm.ru/Data2/1/4293776/4293776736.pdf>
- 15 ГОСТ Р ИСО/МЭК 27004-2011 Информационная технология. Методы и средства обеспечения безопасности [Электронный ресурс] / Режим доступа до ресурсу: <https://meganorm.ru/Data2/1/4293796/4293796402.pdf>
- 16 Про ISO 27004 [Электронный ресурс] / Режим доступа до ресурсу: <https://www.securitylab.ru/blog/personal/80na20/25896.php>
- 17 Обзор стандарта COBIT (Control Objectives for Information and related Technology) v. 4.1. Методология, процессы, критерии, внедрение Cobit [Электронный ресурс] / Режим доступа до ресурсу: <https://www.itexpert.ru/rus/biblio/cobit/>

- 18 Стандарт COBIT [Электронный ресурс] / Баронов В.В. Режим доступа до ресурсу: <https://econ.wikireading.ru/44172>
- 19 COBIT 5 Introduction [Электронный ресурс] / ISACA, 2012 Режим доступа до ресурсу: <https://www.isaca.org/COBIT/Documents/COBIT5-Introduction.ppt>
- 20 Governance of Enterprise IT based on COBIT 5 [Электронный ресурс] / Geoff Harmer Режим доступа до ресурсу: <https://www.oreilly.com/library/view/governance-of-enterprise/9781849285193 /xhtml/chapter06.html>
- 21 COBIT 5 [Электронный ресурс] / Ravi Mudigonda Режим доступа до ресурсу: <https://www.pinterest.com/pin/263390278185464616/?nic=1a>
- 22 COBIT 5 [Электронный ресурс] / Режим доступа до ресурсу: <http://megapolis-profi.ru/cobit5>
- 23 ISACA's Guide to COBIT 5 for Information Security [Электронный ресурс] / Christos Dimitriadis, Robert Stroud Режим доступа до ресурсу: http://docs.bankinfosecurity.com/files/webinars/pdf/313_COBIT5InfoSec.pdf
- 24 Principles for Information Security Practitioners [Электронный ресурс] / ISACA Режим доступа до ресурсу: <https://www.isaca.org/Knowledge-Center/Standards/Documents/Principles-for-Info-Sec-Practitioners-poster.pdf>
- 25 COBIT 5 for Information Security v2 [Электронный ресурс] / ISACA Режим доступа до ресурсу: <https://studylib.net/doc/5554400/cobit-5-for-information-security-v2>
- 26 Идеи и модели COBIT 5 для специалистов по информационной безопасности [Электронный ресурс] / Андрей Прозоров Режим доступа до ресурсу: <https://www.slideshare.net/AndreyProzorov/cobit5-dlp-expert-201312>
- 27 ITIL Framework as a Standard of Information Security [Электронный ресурс] / Ashraf Khaza'aleh Режим доступа до ресурсу: <https://cyberleninka.ru/article/n/itil-framework-as-a-standard-of-information-security/viewer>

- 28 IT Security Management [Электронный ресурс] / Режим доступа до ресурсу: https://wiki.en.it-processmaps.com/index.php/ITIL_Processes
- 29 ITIL security management [Электронный ресурс] / Режим доступа до ресурсу: https://en.wikipedia.org/wiki/ITIL_security_management
- 30 Security Management and ITIL [Электронный ресурс] / C2 Enterprise Режим доступа до ресурсу: https://www.c2enterprise.com/sites/default/files/resources_files/itil_and_security_management.pdf
- 31 ITIL and Information Security [Текст] / Roman Jasek, Lukas Kralik, Miroslav Popelka, Tomas Bata University in Zlin, Faculty of Appied Informatics
- 32 Метрики по ITIL [Электронный ресурс] / Режим доступа до ресурсу: <http://80na20.blogspot.com/2016/01/itil.html>
- 33 ITIL information security management [Электронный ресурс] / Режим доступа до ресурсу: <https://www.bmc.com/blogs/itil-information-security-management/>
- 34 An overview of ITIL CSI and the 7-Step Improvement Process [Электронный ресурс] / Режим доступа до ресурсу: <https://www.invensislearning.com/resources/itil/overview-of-itil-csi-and-the-7-step-improvement-process>
- 35 ITIL [Электронный ресурс] / Режим доступа до ресурсу: <https://www.academia.edu/37070813/>
- 36 ITIL KPIs Continual Service Improvement [Электронный ресурс] / Режим доступа до ресурсу: https://wiki.en.it-processmaps.com/index.php/ITIL_KPIs_Continual_Service_Improvement
- 37 The Use of Six Sigma in Security [Электронный ресурс] / Rudy Neefs Режим доступа до ресурсу: <https://www.linkedin.com/pulse/use-six-sigma-security-rudy-neefs/>

- 38 Six Sigma and Information Security [Электронный ресурс] / Vishant Pai Режим доступа до ресурсу: <https://www.linkedin.com/pulse/six-sigma-information-security-vishant-pai/>
- 39 Six Sigma and CMM models offer security best practices [Электронный ресурс] / Erik Sherman Режим доступа до ресурсу: <https://searchsecurity.techtarget.com/Six-Sigma-and-CMM-models-offer-security-best-practices>
- 40 Security Policy Management Process within Six Sigma Framework [Текст] / Vijay Anand, Jafar Saniie, Erdal Oruklu, Department of Electrical and Computer Engineering, Illinois Institute of Technology, Chicago, USA // Journal of Information Security – 2012. – с. 49-58