Міністерство освіти і науки України
Державний вищий навчальний заклад
«Національний гірничий університет»

Інститут електроенергетики
Факультет інформаційних технологій
Кафедра безпеки інформації та телекомунікацій

ПОЯСНЮВАЛЬНА ЗАПИСКА
дипломної роботи

магістра
(ступінь підготовки)

галузь знань *12 Інформаційні технології*
(шифр і назва галузі знань)

напрям підготовки (спеціальність) *125 Кібербезпека*
(код і назва напряму підготовки)

спеціалізація (освітня програма) *Кібербезпека*
(код і назва спеціальності)

ступінь підготовки *магістр*
(назва освітнього рівня)

кваліфікація *професіонал із організації інформаційної безпеки*
(код і назва кваліфікації)

на тему: ***Підходи до створення центрів оперативного управління кібербезпекою на підприємствах***

Виконавець: студент ***6*** **курсу, групи** ***125м-16-1***

_____ ***Стародубець Олександр Васильович***
(підпис) (прізвище ім'я по-батькові)

Керівники	Прізвище, ініціали	Оцінка	Підпис
роботи	проф. Кагадій Т.С.		
розділів:			
спеціальний	ст.викл. Тимофеєв Д.С.		
економічний	к.е.н., доц. Волотковська Ю.О.		

Рецензент			

Нормоконтроль	к.ф.-м.н., доц. Гусєв О.Ю.		

Дніпро
2018

Міністерство освіти і науки України
Державний вищий навчальний заклад
«Національний гірничий університет»

Інститут електроенергетики
Факультет інформаційних технологій
Кафедра безпеки інформації та телекомунікацій

ЗАТВЕРДЖЕНО:
завідувач кафедри
безпеки інформації та телекомунікацій
_____ д.т.н., проф. Корнієнко В.І.

«_____»_____20___року

ЗАВДАННЯ
на виконання кваліфікаційної роботи магістра

напряму підготовки (спеціальності) *125 Кібербезпека*
(код і назва спеціальності)

студенту ***125м-16-1*** ***Стародубцю Олександру Васильовичу***
(група) (прізвище ім'я по-батькові)

Тема дипломної роботи ***Підходи до створення центрів оперативного управління управління центрів кібербезпекою на підприємствах***

1 ПІДСТАВИ ДЛЯ ПРОВЕДЕННЯ РОБОТИ

Наказ ректора Державного ВНЗ «НГУ» від «26» грудня 2017 р. № 2127-л

2 МЕТА ТА ВИХІДНІ ДАНІ ДЛЯ ПРОВЕДЕННЯ РОБІТ

Об'єкт досліджень *центри оперативного управління кібербезпекою*

Предмет досліджень *рекомендації щодо вибору моделі центру оперативного управління кібербезпекою*

Мета НДР *дослідження методів та моделей побудови центрів оперативного управління кібербезпекою*

Вихідні дані для проведення роботи *законодавство України та міжнародні стандарти у сфері інформаційної безпеки, наукові публікації вітчизняних та іноземних авторів, офіційні статистичні дані з інцидентів інформаційної безпеки, показники діяльності підприємства.*

3 ОЧІКУВАНІ НАУКОВІ РЕЗУЛЬТАТИ

Наукова новизна *у розробці факторів що впливають на вибір типу та архітектури центрів оперативного управляння кібербезпекою*

Практична цінність *у розробці рекомендацій для підприємства щодо побудови центрів оперативного управляння кібербезпекою та порядку їх розгортання*

4 ВИМОГИ ДО РЕЗУЛЬТАТІВ ВИКОНАННЯ РОБОТИ

Результати роботи мають відповідати вимогам чинного законодавства України та бути поданим у вигляді, що дозволяє безпосереднє використання при прийнятті рішення по створенню центру оперативного управління кібербезпекою на підприємстві

5 ЕТАПИ ВИКОНАННЯ РОБІТ

Найменування етапів робіт	**Строки виконання робіт (початок-кінець)**
Огляд джерел за темою та напрям досліджень	1 вересня 2017 р. – 25 вересня 2017 р.
Методи досліджень	26 вересня 2017 р. – 15 жовтня 2017 р.
Результати досліджень	16 жовтня 2017 р. – 20 грудня 2017 р.
Виконання економічного розділу	21 грудня 2017 р. – 1 січня 2018 р.
Оформлення пояснювальної записки	2 січня 2018 р. – 15 січня 2018 р.

6 РЕАЛІЗАЦІЯ РЕЗУЛЬТАТІВ ТА ЕФЕКТИВНІСТЬ

Економічний ефект *зменшення збитків пов'язаних з нештатною роботою основних та допоміжних сервісів підприємства*

Соціальний ефект *дипломної роботи, як наслідок зменшення критичних ризиків, полягає у підвищенні впевненості партнерів, клієнтів та працівників підприємства у його надійності.*

7 ДОДАТКОВІ ВИМОГИ

Відповідність оформлення пояснювальної записки:

ДСТУ 3008-95. «Документація. Звіти у сфері науки і техніки. Структура і правила оформлення».

Бабенко Т.В. Методичні вимоги до підготовки та захисту дипломної роботи (проекту) для студентів галузей знань 1701 «Інформаційна безпека» та спеціальності 125 «Кібербезпека» / Бабенко Т.В., Корнєєв М.В., Кручінін О.В., Тимофєєв Д.С.; Нац. гірн. ун-т. – Д: НГУ, 2016. – 45 с.

Бабенко Т.В. Методичні вимоги до підготовки та захисту дипломної роботи

Завдання видав _____ д.ф.-м.н., проф. Т.С. Кагадій
(підпис) (прізвище, ініціали)

Завдання прийняв до виконання _____ О.В. Стародубець
(підпис) (прізвище, ініціали)

Дата видачі завдання: 01.09.17р.

Термін подання дипломної роботи до ДЕК_____

РЕФЕРАТ

Пояснювальна записка: 79 с., 4 рис., 8 табл., 3 додатки, 20 джерел.

Об’єкт дослідження: центри оперативного управління кібербезпекою.

Мета дипломної роботи: дослідження методів та моделей побудови центрів оперативного управління кібербезпекою.

У спеціальній частині проаналізовані основні фактори які впливають на вибір рішення побудови різних моделей та характеристик центрів оперативного управління кібербезпекою. Розроблені рекомендації щодо вибору моделі, архітектури та побудови центру оперативного управління кібербезпекою для підприємства. Запропонований порядок розгортання такого центру.

У роботі проаналізовані моделі центрів оперативного управління кібербезпекою, надана їх порівняльна характеристика. Розглянуті основні складові, задачі, процеси та порядок їх розгортання.

В економічному розділі проведено розрахунок вартості розгортання центру оперативного управління кібербезпекою та його підтримки, обґрунтована його економічна доцільність.

Практична цінність полягає у розробці рекомендацій для підприємства щодо побудови центрів оперативного управляння кібербезпекою та порядку їх розгортання. Результати досліджень можуть бути застосовані на підприємствах України.

Наукова новизна полягає у визначені факторів що впливають на вибір моделі та архітектури центрів оперативного управляння кібербезпекою.

Ключові слова: ЦЕНТР ОПЕРАТИВНОГО УПРАВЛІННЯ КІБЕРБЕЗПЕКОЮ, ІНЦИДЕНТИ, ІНФОРМАЦІЙНА БЕЗПЕКА, КІБЕРБЕЗПЕКА, МОНІТОРИГ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ

РЕФЕРАТ

Пояснительная записка: 79 с., 4 рис., 8 табл., 3 приложения, 20 источников.

Объект исследования: центры оперативного управления кибербезопасностью.

Цель дипломной работы: исследования методов и моделей построения центров оперативного управления кибербезопасностью.

В специальной части проанализированы основные факторы, которые влияют на выбор решения построения различных моделей и характеристик центров оперативного управления. Разработаны рекомендации по выбору модели, архитектуры и построению центра оперативного управления кибербезопасностью для предприятия. Предложен порядок развертывания такого центра.

В работе проанализированы модели центров оперативного управления кибербезопасностью, представлена их сравнительная характеристика, рассмотрены основные составляющие, задачи, процессы и порядок их развертывания.

В экономическом разделе проведен расчет стоимости развертывания центра оперативного управления кибербезопасностью и его поддержания, обоснована его экономическая целесообразность.

Практическая ценность заключается в разработке рекомендаций для предприятия по построению центров оперативного Управления кибербезопасностью и порядка их развертывания. Результаты исследований могут быть применены на предприятиях Украины.

Научная новизна заключается в определении факторов, влияющих на выбор модели и архитектуры центров оперативного управления кибербезопасностью.

Ключевые слова: ЦЕНТР ОПЕРАТИВНОГО УПРАВЛЕНИЯ КИБЕРБЕЗОПАСНОСТЬЮ, ИНЦИДЕНТ, ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ, КИБЕРБЕЗОПАСНОСТЬ, МОНИТОРИНГ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

ABSTRACT

Explanatory note: 79 p., 4 fig., 8 tab., 3 application, 20 sources.

Object of study: security operation center.

The aim of research paper: research methods and models for the establishment of cybersecurity operational management centers

In a special part, the main factors that influence the choice of the solution for constructing various models of security operation center are analyzed. Recommendations for the selection of a model, architecture and the construction of a cybersecurity operational management center for the enterprise were developed.

This paper analyze the models of security operation center, their comparative characteristics are presented, the main tasks, processes and the order of their deployment are considered.

In the economic section, the value of the deployment and maintenance of the security operation center was calculated and proved its economic feasibility.

Practical value consists in development of recommendations for the enterprise on construction of the security operation center and the order of their deployment. Research results can be applied at enterprises of Ukraine.

The scientific novelty lies in the determination of factors that influence the choice of the model and architecture of the security operation center.

Keywords: SECURITY OPERATION CENTER, INCIDENT, INFORMATION SECURITY, CYBERSECURITY, MONITORING INFORMATION SECURITY

СПИСОК УМОВНИХ СКОРОЧЕНЬ

CERT – computer emergency response team;

DLP – Data loss prevention;

IDS – Intrusion detection system;

NOC – Network operations center

SIEM – Security information and event management;

SOC – Security operations center;

АС – автоматизована система;

ІБ – інформаційна безпека;

ІС – інформаційна система;

ІТ – інформаційні технології;

КС – комп’ютерна система;

НД – нормативний документ;

НСД – несанкціонований доступ;

ПЗ – програмне забезпечення;

ЗМІСТ

с.

ВСТУП

Останнім часом кількість кіберзагроз в корпоративному секторі зросло в десятки разів, а кібер злочинці вже не є хакерами одинаками, як 10-15 років тому, а являють собою потужні угруповання добре організованого і технічно оснащеного криміналу з величезними багатомільйонними оборотами коштів. Дуже тривожною виглядає статистика інцидентів інформаційної та кібербезпеки (І та КБ). І це незважаючи на те, що в корпоративному секторі працюють служби ІБ, які озброєні програмно-технічними засобами в області захисту інформації (SIEM, DLP, антивірусним ПЗ і т.п.).Та незважаючи на таку пристойну організацію захисту інформаційних активів в компаніях, все одно відбуваються інциденти ІБ з великим збитком. Фахівці з інформаційної безпеки давно усвідомили, що необхідний комплексний підхід в сфері реагування та розслідування інцидентів І та КБ і єдине централізоване рішення.

Таким рішенням є побудова на підприємстві центру моніторингу та управління безпекою, який допоможе захистити мережі і інформаційний трафік від загроз. Це інструмент для забезпечення цілісного і комплексного підходу в питанні моніторингу і реагування на інциденти, згідно з нормативними документами, які регулюють ІБ (ISO / IEC 27035, ISO / IEC 27001 і ін.)

SOC об'єднує технології, процеси та людські ресурси, формуючи комплексну систему захисту. Високий ступінь готовності і дотримання систематичного процесу реакції на інциденти в сфері безпеки, допоможе уникнути або згладити наслідки потенційно руйнівних атак, що спрямовані на вашу мережу.

РОЗДІЛ 1

АНАЛІЗ ТИПОВИХ АРХІТЕКТУР І ОСНОВНИХ ФУНКЦІЙ ЦЕНТРІВ ОПЕРАТИВНОГО УПРАВЛІННЯ КІБЕРБЕЗПЕКОЮ

1.1 Аналіз особливостей реалізації центрів оперативного управління кібербезпекою

SOC - Security Operations Center, або Центр оперативного управління, основними завданнями якого є консолідація подій з безлічі джерел, проведення певної аналітики і оповіщення уповноважених співробітників про інциденти інформаційної безпеки чи інших подіях. На основі отриманих даних співробітники центру проводять розслідування, вживають заходів, щоб виключити можливість повторення події, мінімізують втрати. SOC є еволюцію поняття CERT (Computer Emergency Response Team) - групу реагування на надзвичайних ситуації в області IT технологій[1].

Однією з ключових відмінностей від CERT є використання аналітичних технологій для створення єдиного оперативного бачення поточної ситуації в компанії з точки зору ІБ.

Традиційно під англомовним поняттям Security Operation Center (SOC) розуміється система, побудована на базі продуктів класу SIEM (Security Information and Event Management), призначених для збору і зберігання лог-файлів пристроїв і додатків з метою їх подальшого аналізу і виявлення інцидентів.

Зараз SOC на основі SIEM-продуктів допомагає компаніям вирішувати ряд ключових завдань:

- збирати і зберігати лог-файли в єдиному централізованому сховищі;
- надавати спеціалізовані звіти аудиторів для відповідності вимогам законодавства і галузевим стандартам;
- визначити якусь "базову лінію" мережевої активності організації, перевищення якої може свідчити про різного роду атаках;

- виконувати кореляцію подій між різними джерелами отримуваної інформації.

Однак загрози і атаки з кожним роком стають все більш складними і часто спрямованими проти певної групи організацій (наприклад, ЗМІ) або ж конкретної компанії. Очевидно, що подібні цілеспрямовані протиправні дії відбуваються підготовленими людьми, що мають певну кваліфікацію, і тому їх надзвичайно складно виявити за допомогою звичайних засобами захисту (антивірус, IPS). Для виявлення подібних дій потрібен максимально можливий обсяг даних для аналізу і в ідеальному варіанті необхідно аналізувати не тільки логи, але і весь трафік з метою виявлення аномальної активності і визначення ступеня шкоди. Тобто для отримання достовірної картини того, що відбувається в мережі в даний час вже недостатньо одних тільки лог-файлів з пристроїв і додатків.

Розглянемо одну з ключових частин центрів оперативного управління кібербезпекою SIEM – систему.

SIEM (Security information and event management) - об'єднання двох термінів, що позначають область застосування ПО: SIM (Security information management) - управління інформаційною безпекою та SEM (Security event management) - управління подіями безпеки. Технологія SIEM забезпечує аналіз в реальному часі подій (тривог) безпеки, що виходять від мережевих пристроїв і додатків. SIEM представлено додатками, приладами або послугами, і використовується також для журналирования даних і генерації звітів з метою сумісності з іншими бізнес-даними[2].

SIEM-системи, як і багато інших продуктів з'явилися в результаті еволюційного розвитку і подальшого злиття систем SEM і SIM[3]. SEM (Security Event Management) - системи діють в режимі наближеному до реального часу. Для цього їм потрібно: автоматичний моніторинг подій, їх збір, кореляція, генерація попереджувальних повідомлень. SIM (Security Information Management) - системи, в свою чергу, аналізують накопичену інформацію з боку

статистики, різних відхилень від «нормального поведінки» і т.д. Коли ж можливості SIM і SEM об'єднуються в рамках одного продукту, говорять про SIEM-системах. Виходячи з цього, можна дати «літературний» переклад абревіатури SIEM - система збору та кореляції подій. Важливо розуміти, що SIEM-системи в якості самостійного (standalone) рішення не призначені і не здатні запобігати інцидентам порушення інформаційної безпеки. Їх сутність закладена в їх назві: аналіз інформації, що надходить з різних джерел (DLP, IDS, антивіруси, міжмережеві екрани і т.д.), і подальше виявлення відхилень від норм за заданими критеріями. Перед системою SIEM ставляться такі завдання.

- Консолідація та зберігання журналів подій від різних джерел.
- Надання інструментів для аналізу подій і розбору інцидентів
- Кореляція і обробка подій за правилами.
- Автоматичне сповіщення і інцидент-менеджмент.

Розглянемо принцип роботи SIEM

Система збирає інформацію, аналізує (і генерує попередження), складає в бази даних, аналізує поведінку на підставі попередніх спостережень (і генерує попередження). На практиці схема реалізується за допомогою відповідних компонентів:

- Агенти (збір даних з різних джерел);
- Сервери-колектори (акумуляція інформації, що надійшла від агентів);
- Сервер баз даних (зберігання інформації);
- Сервер кореляції (аналіз інформації).

Вхідною інформацією для SIEM-систем може служити практично будь-яка інформація. Головне - правильно її подати. Як вже було сказано вище, збір даних може здійснюватися за допомогою спеціальних агентів, які представляють собою програму, яка локально збирає журнали подій і по можливості передає їх на сервер. Для «вичитки» того чи іншого джерела даних агент використовує колектори - бібліотеки для розуміння конкретного журналу подій або системи.

Колектори грають важливу роль, так як різні джерела можуть назвати однакові подія по-своєму. Наприклад, Firewall одного виробника може записувати в звіт deny, іншого discard, третього drop, хоча події однакові. Колектори допомагають привести всі ці події до спільного знаменника. Якщо ж для джерела немає відповідного колектора, події можна спробувати відправляти як SYSLOG (за умови, що джерело вміє це робити). Однак і тут можна зіткнутися з «проблемою синонімів» і необхідністю писати додатковий обробник для приведення даних в єдиний формат. Також інформацію можна збирати віддалено за допомогою з'єднання за протоколами NetBIOS, RPC, TFTP, FTP. Однак в цьому випадку може виникнути проблема з навантаженням на мережу, так як частина систем дозволяє передавати тільки журнал цілком, а не «свіжі» записи.

SIEM-системи можуть використовувати такі джерела інформації:

- Access Control, Authentication. Застосовуються для моніторингу контролю доступу до інформаційних систем і використання привілеїв.
- DLP-системи. Відомості про спроби інсайдерських витоків, порушення прав доступу.
- IDS / IPS-системи. Несуть дані про мережеві атаках, зміни конфігурації і доступу до пристроїв.
- Антивірусні програми. Генерують події про працездатність ПО, базах даних, зміні конфігурацій і політик, шкідливий код.
- Журнали подій серверів і робочих станцій. Застосовуються для контролю доступу, забезпечення безперервності, дотримання політик інформаційної безпеки.
- Міжмережеві екрани. Відомості про атаки, шкідливі програми та інше. Мережеве активне обладнання. Використовується для контролю доступу, обліку мережевого трафіку.
- Сканери вразливостей. Дані про інвентаризацію активів, сервісів, програмного забезпечення, вразливостей, поставка інвентаризаційних даних і топологічної структури.

- Системи інвентаризації та asset-management. Поставляють дані для контролю активів в інфраструктурі і виявлення нових.
- Системи веб-фільтрації. Надають дані про відвідування співробітниками підозрілих або заборонених веб-сайтів.

Основні протоколи і інтерфейси для збору подій[4]:

- Syslog and Syslog-ng
- SNMPv2 and SNMPv3
- Opsec
- HTTP, HTTPS
- SQL, ODBC
- WMI, WBEM (CIM)
- FTP, SFTP
- Socket Unix
- Plain log
- SSH
- Rsync
- Samba
- NFS
- SDEE, RDEP
- OPSEC, CPMI

Отримавши інформацію, система може її проаналізувати. В основі аналізу лежать математичні та статистичні засоби обробки інформації. Але відправною точкою служать задаються вручну правила. Наприклад, одноразове подія «login failed» нічого не означає, в той час як три і більше таких події від одного облікового запису вже можуть свідчити про спроби підбору пароля. У найпростішому випадку в SIEM-системах правила представлені в форматі RBR (Rule Based Reasoning) і містять набір умов, тригери, лічильники, сценарій дій. Наприклад, враховувати параметри віддаленості двох останніх точок

використання банківської карти за невеликий інтервал часу: якщо о 17:00 її використовували для оплати кави в Москві, а через 10 хвилин намагаються зняти денний ліміт в Гонконзі, то на обличчя – спроба шахрайства. SIEM-системи здатні виявляти:

- мережеві атаки у внутрішньому і зовнішньому периметрах;
- вірусні епідемії або окремі вірусні зараження;
- спроби несанкціонованого доступу до конфіденційної інформації; шахрайство;
- помилки і збої в роботі інформаційних систем;
- уразливості;
- помилки конфігурацій в засобах захисту та інформаційних системах;
- цільові атаки (APT).

Розглянемо основні етапи впровадження SIEM:

- Обстеження інфраструктури і вибір способу впровадження (всі події обробляються в одному місці, або буде розпаралелювання).
- Формування і ствердження ТЗ.
- Розробка керівництва адміністраторів і керівництво користувача.
- Встановлення серверу SIEM (інтеграція апаратних засобів, їх прописка в мережі).
- Налаштування джерел подій. (Налаштовуємо джерела на відправку подій SIEM).
- Розроблюємо правила реагування на події. (На даному етапі себе покажуть погано налаштовані джерела)
- Тестова експлуатація та накопичення статистики. (Один з найважливіших етапів)
- Коригування і написання додаткових правил. (Навчання SIEM)
- Завершення тестування.

Впровадження SIEM займає від 6 місяців.

Можна виділити основних представників SIEM – рішень[5]:

- HP (ArcSight)
- IBM (Qradar)
- McAfee (NitroSecurity)
- RSA, EMC (envision, NetWitness)
- LogRhythm
- Novell (NetIQ)
- CorreLog
- SolarWinds (Log and Event Manager)
- Splunk
- Symantec (SSIM, SEP)
- Trustwave SIEM OE

Розглянемо подібність і відмінності SOC та CERT

Абревіатура CERT розшифровується як Computer Emergency Response Team. Іноді вона приймає значення Комп'ютерної команди безпеки по реагуванню на інциденти - CSIRT (Computer Security Incident Response Team). Слово «команда» в даному випадку часто замінюється словом «центр»[6].

CERT - це централізована функція управління інцидентами інформаційної безпеки та реагування на них в організації. Вона може бути частиною SOC, або як окрема команда у великих організаціях.

Основна відмінність CERT від SOC полягає в тому, що зазвичай це конгломерат ролей на підприємстві, які беруть участь у всіх типах функцій відповіді на інциденти. Хоча відповідачі за інциденти, звичайно, керують самим процесом реагування на інцидент, інші функції, включаючи зв'язки з громадськістю (PR), маркетинг, підтримка клієнтів та управління, часто співпрацюють із CERT.

Кінцевою метою CERT є мінімізація та контроль пошкоджень, отриманих внаслідок інциденту, тому в такий спосіб може бути задіяне так багато різних

функцій. Потрібно не тільки вирішувати саму загрозу, але й проінформувати клієнтів, членів правління та громадськість про інцидент.

Розглянемо обов'язки команди CERT:

- Запобігання, виявлення та реагування на поточні загрози безпеці
- Оцінка ризиків
- Дослідження, аналіз та проведення більш глибокої експертизи за інцидентами
- Розробка планів комунікації (для громадських зв'язків, клієнтів, членів правління тощо)
- Координація та реалізація стратегій реагування
- Підтримка сховища даних журналу подій, пов'язаних з подіями для подальшого використання, а також юридичних цілей

CERT може бути створений формальною чи неформальною організацією залежно від унікальних потреб вашої компанії. Якщо на регулярній основі ви не стикаєтесь із загрозами, команда CERT може збиратися лише на необхідній основі. Але якщо ви працюєте в галузі високого ризику (наприклад, державне управління, охорона здоров'я, фінанси), де реагування на погрози є регулярною та важливою частиною вашої бізнес-стратегії, може знадобитися формальний та повний робочий день команди CERT.

CERT може розвиватися з часом. Хоча це може розпочатися як неформальна команда, яка збирається на необхідній основі, вона може розвинутися в повнофункціональну команду, якщо потреба у відповідних випадках вимагає цього.

Ролі CERT:

- Аналітики безпеки
- Фахівці з реагування на інциденти
- Мережеві та системні адміністратори
- Менеджери рівня C (наприклад, CIO, CISO, CTO, CRO)

1.2 Основні задачі центрів оперативного управління кібербезпекою

Щоб зрозуміти необхідність побудови такої систем, розглянемо основні вимоги до інформаційної безпеки від бізнесу:

- Зниження ризиків і часу простою
- Контроль і запобігання загрозам
- Захист від перевантаження адміністратора / оператора
- Відповідальність за процес
- ескалація проблем
- Аудит і перевірка відповідності
- Реагування на інциденти
- Збір доказів
- Відповідність законодавчим вимогам

Ситуаційний центр являє собою комплексне організаційно-технічне рішення, що дозволяє:

- автоматизовано виявляти події, що представляють потенційну загрозу для організації, її інформаційних систем або інформаційних активів (інциденти ІБ);
- забезпечити тривале зберігання всього обсягу зібраних подій і зафіксованих інцидентів ІБ для можливості проведення постінцідентного розслідування;
- реалізувати процес обробки виявлених інцидентів, який би дозволив в гарантований час (залежне від рівня критичності інциденту) оповіщати відповідальні підрозділи організації про те, що сталося, і рекомендувати необхідні заходи для запобігання впливу інциденту інформаційної безпеки на бізнес.

Зібрана в ході комплексного моніторингу інформація надходить в єдиний центр, де вона обробляється і представляється в наочному і зручному вигляді. Тут же здійснюється реагування та вирішення інцидентів ІБ, усунення виявлених

відхилень. Побудова такого центру оперативного управління ІБ (Security Operations Center, SOC (Рисунок 1.1)) є непростим завданням.

Центр оперативного управління ІБ дозволяє контролювати і оперативно управляти інформаційною безпекою компанії в режимі реального часу, бути впевненим в тому, що необхідний рівень забезпечення ІБ досягнутий і підтримується, відстежувати виконання заданих цільових показників ефективності (KPI) забезпечення ІБ.

Центр оперативного управління ІБ дозволяє відслідковувати в інформаційній системі події, пов'язані з ІБ, аналізувати і зіставляти їх з іншими даними, представляти зібрану інформацію в наочному і зручному вигляді, контролювати наявні уразливості, здійснювати контроль конфігурацій, відстежувати ступінь виконання вимог законодавства, нормативних актів і корпоративних політик, а також оперативно реагувати на виявлені інциденти ІБ. Тобто надає повну картину поточного стану інформаційної безпеки компанії, що дозволяє оперативно усувати виявляються відхилення і забезпечувати заданий рівень ІБ.

Ключовими факторами, що забезпечують ефективність подібних центрів, є: впровадження процесів моніторингу, управління уразливими і інцидентами, правильне розмежування відповідальності між співробітниками всередині компанії, розробка і впровадження регламентів реагування на інциденти ІБ і їх подальшого розбору.

У компаніях з великою кількістю філій, розвиненою IT-інфраструктурою та великою кількістю різноманітних засобів захисту без спеціалізованих технічних засобів реалізувати повноцінний комплексний моніторинг ІБ вельми проблематично.

Рисунок 1.1 Основні процесі центру оперативного управління ІБ

Також багато що залежить від якості налаштувань технічних засобів і кваліфікованих дій обслуговуючого персоналу.

Впроваджуючи Центр оперативного управління ІБ, компанії одночасно реалізують частину процесів системи управління ІБ (СУІБ) відповідно до стандарту ISO 27001[7] (процес управління інцидентами ІБ, управління уразливостями, управління змінами, контроль відповідності законодавчим та галузевим вимогам), та ISO 27037[8] (методи забезпечення безпеки, настанови щодо ідентифікації, збору, придбання і збереження цифрових даних»)

Таким чином, центр оперативного управління ІБ являє собою набір пов'язаних і працюючих разом процесів управління ІБ (моніторинг, управління інцидентами, управління уразливостями, інвентаризація активів, управління змінами, контроль політик безпеки) і автоматизуючих їх технічних систем:

- Моніторинг стану ІБ:
- Моніторинг подій ІБ;
- Аудит дій користувачів;
- Управління уразливостями / контроль конфігурацій;
- Управління інцидентами ІБ;
- Контролю відповідності вимогам законодавства, міжнародних і галузевих стандартів, внутрішніх корпоративних політик.
- Інвентаризація та контроль інфраструктури;
- Консолідація інформації про інциденти ІБ;
- Координація та автоматизація реагування на інциденти ІБ;
- Інтеграція та отримання даних із зовнішніх джерел;
- Збір показників ефективності системи захисту (метрик).

Моніторинг ІБ - це ключовий елемент управління ризиками ІБ в змінюється інформаційному середовищі організації.

Основними цілями моніторингу ІБ є оперативне і постійне спостереження, збір, аналіз і обробка даних для кожного з напрямків діяльності СУІБ відповідно до заданих цілей, а також забезпечення повної, своєчасної, достовірної інформацією для прийняття обґрунтованих рішень в області ІБ. Такими цілями аналізу можуть бути наступні:

- контроль за реалізацією положень внутрішніх і зовнішніх документів по ОІБ в організації для виявлення відхилень від прийнятих вимог бізнесу і вимог по ОІБ (наприклад, зафіксованих в політиці щодо логічного доступу (ПЛД) до інформаційних активів);
- контроль якості (результативності та ефективності) використовуваних захисних заходів;
- виявлення нештатних, в тому числі злочинних, дій з інформаційними активами і бізнес-процесами організації;

- виявлення подій ІБ, частина з яких в подальшому класифікується як інциденти ІБ;
- виявлення вразливостей активів, якими можуть скористатися зловмисники для реалізації атак на системи, мережі і сервіси як самої організації, так і її бізнес-партнерів або користувачів загальнодоступних мереж типу Інтернету;
- забезпечення доказової бази на випадок розслідування комп'ютерних злочинів.

Процеси моніторингу ІБ в рамках процесу управління ІБ включають таке:

- пошук, відстеження, спостереження, накопичення, систематизація, оцінювання відомостей, що відносяться до області ІБ;
- прогнозування стану та якості всіх об'єктів і процесів в інформаційному середовищі організації.

Моніторинг ІБ забезпечує прозорість автоматизованих бізнес-процесів (основних, допоміжних і управлінських) та гарантує їх спостережність протягом всього часу їх функціонування, що, як наслідок, підвищує рівень довіри бізнесу до них. Також моніторинг ІБ сприяє підвищенню почуття відповідальності працівників організації за свої дії, що впливають на ІБ, допомагає у виявленні неправильного використання ресурсів і діє як стримуючий чинник для осіб, здатних спробувати нанести шкоду організації. І, нарешті, під час моніторингу виявляються помилки в самій обробці інформації та її результати, пов'язані як зі збоями в функціонуванні СВТ, так і з людським фактором, що дозволяють в подальшому оптимізувати процес експлуатації (з точки зору дотримання встановлених регламентів) і функціонування систем, мереж і сервісів.

Моніторинг ІБ реалізується на основі безперервного спостереження за зареєстрованими подіями, що впливають на ІБ, в конкретному середовищі (системі, мережі, сервісі) і контролю за дотриманням базових вимог по ОІБ і запропонованих регламентів (контроль штатності режиму функціонування цього середовища). У процесі моніторингу події ІБ піддаються ретельному і

регулярному аналізу, на основі якого робиться висновок про наявність чи відсутність, а також можливості настання інциденту ІБ. На основі отриманих під час моніторингу ІБ результатів складаються відповідні звіти і далі виконуються заздалегідь запрограмовані дії, спрямовані на усунення виявлених вразливостей, переривання неприпустимих видів подій і т. П.

Отже, можна зробити висновок, що моніторинг ІБ і управління інцидентами ІБ дуже тісто взаємопов'язані.

Система управління (моніторингу) подіями ІБ (Security Information Management System, SIMS) - реалізує комплексний підхід до вирішення завдань збору, аналізу (кореляції) і контролю подій ІБ від різних засобів захисту, що дозволяє в режимі реального часу ефективно ідентифікувати інциденти інформаційної безпеки (з подальшою їх передачею в систему управління інцидентами), отримувати реальні дані для аналізу та оцінки ризиків, для прийняття обґрунтованих і адекватних наявним ризикам рішень щодо забезпечення ІБ.

Система управління подіями ІБ допомагає вирішити такі завдання:

- управління великим обсягом подій ІБ;
- отримання повної картини того, що відбувається в ІС;
- моніторинг поточного рівня забезпечення безпеки (контроль досягнення заданих показників ефективності (KPI) забезпечення ІБ);
- своєчасне виявлення інцидентів ІБ;
- отримання реальних даних для аналізу та оцінки ризиків; прийняття обґрунтованих рішень з управління ІБ;
- виконання вимог законодавства та нормативних актів з моніторингу подій, пов'язаних з ІБ (ISO / IEC 27001: 2013, SOX).

На ринку систем управління подіями інформаційної безпеки представлені технічні рішення різних виробників, вони відрізняються по функціоналу, спектру вирішуваних завдань, сфері застосування:

- Symantec Security Information Manager (SSIM);
- nFX SIM One (netForensics);
- ArcSight Enterprise Security Management (ArcSight ESM);
- Cisco Security Monitoring, Analysis and Response System (CS-MARS).

Система аудиту дій користувачів забезпечує реєстрацію і аналіз дій користувачів (перш за все на рівні БД), розсилку повідомлень в режимі реального часу і підготовку звітів про те, хто отримує доступ, до якої саме інформації, і як ці дії можуть порушити вимоги зовнішніх регулюючих органів або внутрішні правила з інформаційної безпеки компанії.

Система аудиту дій користувачів допомагає вирішити такі завдання:

- контроль зловмисних дій користувачів;
- захист від витоку конфіденційної інформації;
- отримання відповіді на питання: «Хто? Що зробив? Коли? Де? Звідки? Куди? За допомогою яких засобів? »;
- підготовка звітів різного рівня (від керівника компанії до адміністратора інформаційної безпеки).

Для контролю дій користувачів можуть бути використані рішення компанії Imperva, а також відмінно зарекомендували себе продукти nFX Data One (netForensics) і Oracle Audit Vault, перший з яких легко інтегрується з іншими продуктами компанії netForensics, а другий - розроблений спеціально для однієї з найбільш поширених СУБД - Oracle.

Система управління уразливостями / контролю конфігурацій дозволяє отримувати дані за наявними уразливостями в режимі реального часу, відстежувати динаміку їх усунення, контролювати вироблені зміни, а також забезпечує автоматизацію таких завдань, як: інвентаризація ресурсів і контроль конфігурацій.

Пошук вразливостей критичних ресурсів проводиться на постійній основі різними способами:

- мережеве сканування;
- тест на проникнення;
- системні перевірки;
- аналіз захищеності СУБД;
- аналіз захищеності Web-додатків.

Інвентаризація та контроль інфраструктури:

На базі центрів SOC досить часто забезпечується вирішення актуальних для кожної компанії завдання з управління інформаційними активами компанії, таких як:

- моніторинг IT-інфраструктури, збір даних про обладнання і його характеристиках (інвентаризація), контроль складу IT-систем, побудова зв'язків взаємодії між компонентами;
- складання переліку критичних активів і проведення оцінки їх цінності;
- контроль облікових записів користувачів, управління доступами і привілеями;
- управління уразливостями.

За рахунок відповідних інструментів SOC виявляються найбільш критичні активи компанії і визначаються відповідальні за ці активи фахівці. Все це здійснюється в тісній взаємодії з іншими інфраструктурними системами (антивірусами, сканерами вразливостей і т.д.). Також, як правило, в рамках контролю інфраструктури здійснюється контроль за знову встановленими програмами, виявляється ПО, яке не дозволено використовувати, фіксується підключення нового обладнання та інші потенційно небезпечні активності. Візуалізація даних за активами представляється у вигляді графів, схем, карт мереж, що дозволяють підвищити ефективність аналізу захищається інфраструктури.

Управління уразливостями в рамках контролю інфраструктури, в свою чергу, полягає не тільки в їх виявленні, а й в реєстрації відповідно до типу і рівнем критичності, з подальшим автоматичним призначенням відповідальних і термінів усунення, а також винятком тих вразливостей, які в ході вивчення визнаються помилкові спрацьовування.

Коли в організації немає єдиного центру моніторингу, інформація про інциденти розрізнена и не систематизована, ця обставина ускладнює, як оперативне реагування на інцидент, так и швидке и якісне його розслідування. Тому потрібна єдина база для збору інформації про всі інциденті ІБ, що відбулися в организаціх.

Розглянемо поетапно, як відбувається робота з обробки інцидентів:

- Виявлення інцидентів. На цьому етапі інформація про інциденти збирається централізовано з різних джерел, класифікується, аналізується.
- Реагування. Призначення відповідальних осіб і групи реагування, контроль термінів і дій.
- Розслідування інциденту. На даному етапі збирається доказова база, свідоцтва, виявляються причини і обставини інциденту.
- Аналіз і статистика. Формуються статистичні дані по відділах, філіях, по типам. Виявляються основні зв'язки і залежності.
- Звітність. Формування і висновок різного виду звітів (для керівництва, для регуляторів і т.д.).

Інформація про інциденти при цьому може надходити в централізовану базу даних різними способами (по e-mail, через програмний інтерфейс API або вводиться вручну через веб-форму). В рамках фіксації інцидентів, як правило, реєструються такі параметри інцидентів як: рівні критичності, рівні збитку, джерело інциденту, ступінь навмисності, статус реалізації, ймовірність повторного виникнення, пріоритет і т.д.

Координація та автоматизація реагування на інциденти ІБ:

У сфері ІБ вкрай важлива автоматизація процесів реагування на інциденти, щоб кожен раз групі реагування не доводилося вигадувати якісь «відповідні заходи» заново. У SOC, як правило, закладена «адаптивна логіка», це означає, що існують певні конструктори, за допомогою яких, з огляду на конкретні бізнес-процеси в компанії можна задати ряд правил, за допомогою яких збирається інформація про інциденти за заданими критеріями, налаштовуються доступи до ній, а також автоматично призначаються відповідальні особи з розслідування даного інциденту.

Група реагування на інциденти ІБ організовується на базі SOC, функції всіх членів групи заздалегідь строго прописані процедурами SOC, формується автоматична звітність на всіх стадіях реагування та розслідування інцидентів ІБ.

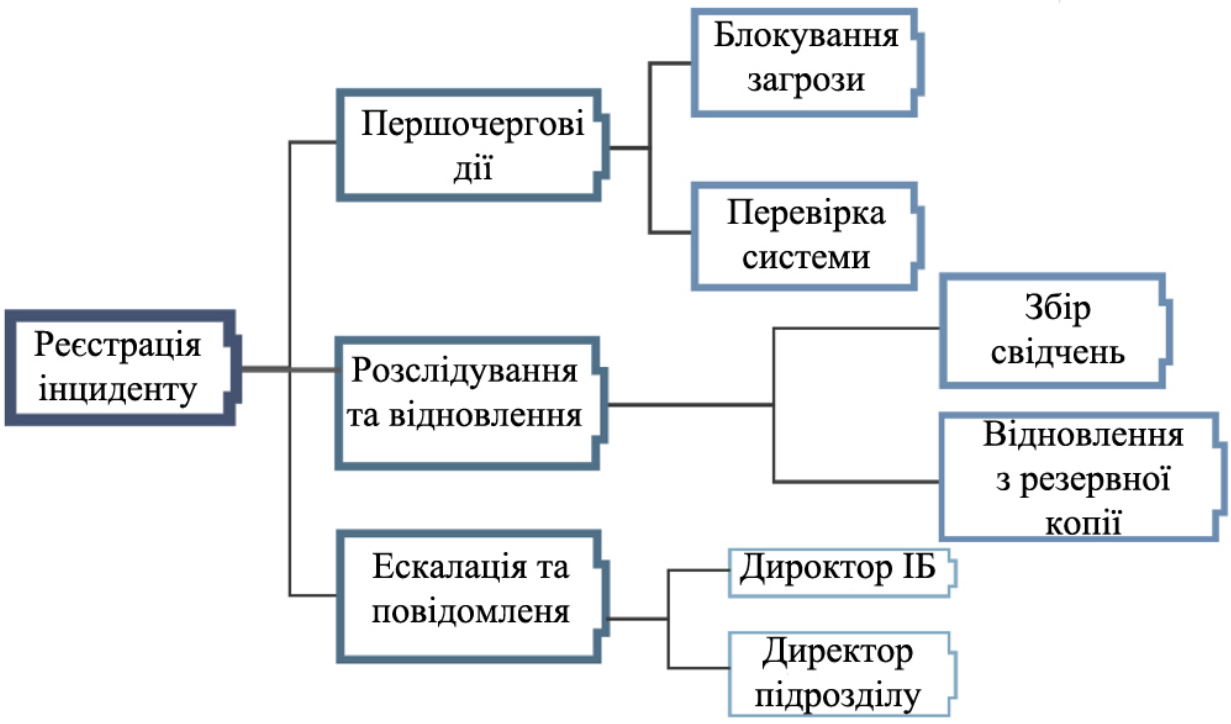

Рисунок 1.2. Автоматизація реагування на інциденти

Інтеграція з зовнішніми джерелами і обмін інформацією по інцидентах, які підключені до SOC. Це можуть бути повідомлення, що надходять з систем збору і кореляції подій безпеки - SIEM, DLP - систем, антивірусних пакетів, сканерів уразливості і т.д. (Див. Рис. 3). Повідомлення можуть надходити і з зовнішніх

джерел через прикладний програмний інтерфейс API або навіть по електронній пошті. Головне, щоб вони оброблялися за певними правилами, заснованим, наприклад, на регулярних виразах або тегах. Пояснимо на прикладі інтеграції з SIEM: інцидент передається в SOC, далі проводиться його обробка відповідно до встановлених регламентів, а після завершення роботи над інцидентом він автоматично закривається і в системі SIEM, тобто працює двостороння синхронізація стану інцидентів. Хороший SOC повинен забезпечувати обмін даними і з іншими учасниками галузі ІБ (із зовнішніми експертами, іншими компаніями, громадськими структурами центрами реагування SERT / SOC і.т.д.)

Ще один важливий блок SOC - це «метрики», тут подано звітність за типами інцидентів, термінів реагування і по величині матеріальних збитків від них. У хорошій системі повинні бути налаштовані як мінімум наступні метрики:

- середній час реагування на інцидент,
- кількість інцидентів в роботі,
- середній час закриття інциденту,
- ставлення закритих інцидентів до зареєстрованих інцидентів.

Крім вище зазначених параметрів, можуть бути представлені і інші показники, такі як «збиток від реалізації інцидентів» і ін. Всі метрики представляються візуально у вигляді графіків і схем.

1.3 Аналіз моделей центрів оперативного управління кібербезпекою

Існують три моделі центрів оперативного управління:

1. Власний SOC
2. SOC як сервіс
3. Гібридний SOC

Їх можна порівняти за такими показниками:

1. Розміщення технічного обладнання
2. Розміщення персоналу

3. Рівень зрілості ІБ
4. Структура витрат

У табл. 1.1. порівнюється місце розміщення технічного оснащення.

Таблиця 1.1 – Порівняння місця розміщення технічного оснащення

	Власний SOC	SOC як сервіс	Гібридний SOC
Обладнання для системи SIEM	O	I	O
Технічна підтримка	O	I	I
Сервери для збору даних	O	O	O
Сервери для зберігання даних	O	I	I
Сервери резервного копіювання	O	I	I
Ліцензування (SIEM, Servise Desk,	O	I	O

O – розташовані в організації

I – розташовані у інтегратора

Персонал та ролі

Адміністратор Системи (інженер), що здійснює функції з підтримки працездатності СЗІ і SIEM-системи, по створенню нових ресурсів і коригуванні існуючих (в тому числі правил кореляції);

- мінімальна кількість: 2

Оператори моніторингу та первинного реагування, які виконують регламентні операції, обробку потоку подій ІБ, пріоритезацію, реагування на інциденти і їх ескалацію;

- мінімальна кількість 24x7: 5

Експерт(и) з розслідування (аналітик) інцидентів ІБ, який проводить розслідування по інцидентах ІБ.

- мінімальна кількість: 1

Керівник SOC

Таблиця 1.2 – Порівняння розміщення персоналу

	Власний SOC	SOC як сервіс	Гібридний SOC
Керівник SOC	O	I	м
Адміністратор системи	O	O	O
Група моніторингу	O	O	O
Експерт, аналітик ІБ	O	O/ I	O/ I

O – розташовані в організації

I – розташовані у інтегратора

Порівняння зрілості інформаційної безпеки

За стандартом COBIT[9] можна виділити такі рівні зрілості:

5 - оптимізований рівень

- Характеризує рівень опрацювання менеджменту ІБ до рівня кращої практики, заснованої на результатах безперервного вдосконалення і порівняння рівня зрілості щодо інших організацій.
- Захисні заходи в організації використовуються комплексно, забезпечуючи основу вдосконалення процесів менеджменту ІБ.
- Організація здатна до швидкої адаптації при змінах в оточенні та бізнесі.

4 - керований рівень

- Характеризує те, що забезпечуються моніторинг і оцінка відповідності використовуваних в організації процесів.
- При виявленні низької ефективності реалізованих процесів менеджменту ІБ забезпечується їх оптимізація.
- Процеси менеджменту ІБ знаходяться в стадії безперервного вдосконалення і ґрунтуються на хорошій практиці.
- Засоби автоматизації і менеджменту ІБ використовуються частково і в обмеженому обсязі.

3 - певний рівень

- Характеризує те, що процеси стандартизовані, документовані і доведені до персоналу за допомогою навчання.
- Однак порядок використання даних процесів залишений на розсуд самого персоналу.
- Це визначає ймовірність відхилень від стандартних процедур, які можуть бути не виявлені.

- Застосовувані процедури не оптимальні і недостатньо сучасні, але є відображенням практики, використовуваної в організації.

2 - повторюваний рівень

- Характеризує рівень опрацювання процесів менеджменту ІБ до рівня, коли їх виконання забезпечується різними людьми, вирішальними одну і ту ж задачу.
- Однак відсутні регулярне навчання і тренування по стандартних процедурах, а відповідальність покладена на виконавця.
- Керівництво організації в значній мірі покладається на знання виконавців, що тягне за собою високу ймовірність можливих помилок.

1 - початковий рівень

- Характеризує наявність документально зафіксованих свідчень усвідомлення організацією існування проблем забезпечення ІБ.
- Однак використовувані процеси менеджменту ІБ не стандартизовані, застосовуються епізодично і безсистемно
- Загальний підхід до менеджменту ІБ не вироблений.

0 - рівень

- Характеризує повна відсутність будь-яких процесів менеджменту ІБ в рамках діяльності організації.
- Організація не усвідомлює існування проблем ІБ.

Для власного SOC необхідний найвищий рівень зрілості ІБ. SOC виділяється в окремий бізнес-процес, його робота не суміщається з іншими задачами. Вводиться база інцидентів та KPI.

Для SOC як сервісу та гібридного достатньо третього рівня зрілості ІБ, тому що на інтеграторі лежить часткова чи повна організація процесу побудови і підтримки процесу.

Розглянемо структуру витрат для побудови центру оперативного управління кібербезпекою.

Для власного SOC необхідні великі кошти, тому що потрібно самостійно закуповувати обладнання, програмне забезпечення, також велика вартість впровадження та підтримки власної системи, необхідно тримати штат висококооплачуваних спеціалістів та витрачати кошти на електроенергію та амортизацію обладнання.

Для SOC як сервіс потрібно платити лише за підписку на послугу, яка значно менша від повного розгортання власного центру.

Для гібридного SOC також потрібні кошти на обладнання та програмні засоби, але менші ніж для повного розгортання центру, також потрібно сплачувати кошти за підписку, але менші, тому що частина функцій та обладнання розташовується на підприємстві.

Порівнюючи ці типи можна виділити такі переваги та недоліки кожної з систем, які наведені у порівняльній таблиці 1.3.

Таблиця 1.3 – Недоліки та переваги різних типів SOC

	Власний SOC	SOC як сервіс	Гібридний SOC
Переваги	Власний процес який контролюється самою організацією	Готовий процес як послуга Порівняно невелика вартість	Порівняно невелика вартість Готовий процес як послуга Можливість розгорнути власний SOC
Недоліки	Висока вартість і складність організації, побудови та підтримки	Вихід інформації за рамки організації	Вихід інформації за рамки організації

1.4 Узагальнена архітектура типового центру оперативного управління кібербезпекою

Розглянемо побудову типової архітектури SOC, та стадії прийняття заходів у відповідь у разі виникнення інцидентів. Виконавши ці дії і пройшовши ці стадії, ми матимемо найважливіші процедури для ідентифікації і нейтралізації інцидентів в сфері інформаційної безпеки.

Типова архітектура SOC демонструє, яку інформацію про безпеку слід збирати, і визначає правила аналізу, обробки і поширення цієї інформації. Відповідні етапи перераховані на стрілках у верхній частині рисунка 1.3.

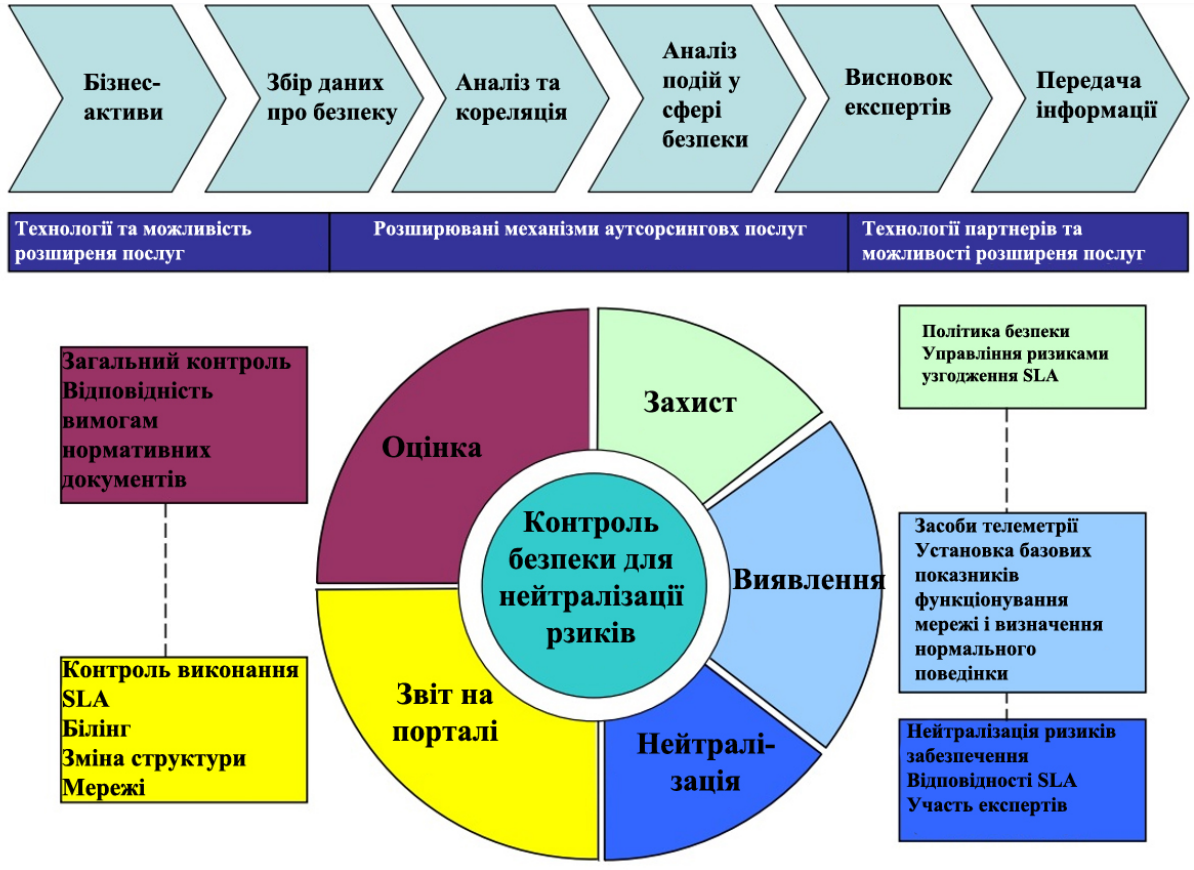

Рисунок 1.3 Типова архітектура SOC

1) Визначення, для яких бізнес-активів необхідні моніторинг і захист.

Для початку потрібно визначитися захист яких маршрутизаторів, комутаторів, серверів, комп'ютерів, баз даних та інших бізнес-активів є необхідним.

У разі підключення аутсорсингово SOC, визначивши на які бізнес-активи буде поширюватися моніторинг, потрібно відповісти на два питання:

- Яка політика безпеки потрібно для захисту цих активів?
- Який договір про рівень обслуговування (SLA) необхідний?

SLA – Угода про рівень обслуговування визначається як офіційне зобов'язання, яке переважає між постачальником послуг і клієнтом. Особливі аспекти послуги - якість, наявність, відповідальність - узгоджуються між постачальником послуг та користувачем служби.[10] Найбільш поширеним компонентом SLA є те, що послуги повинні надаватися клієнту, як це узгоджено в договорі. Наприклад, Інтернет-провайдери та телекомунікаційні компанії, як правило, включають угоди про рівень сервісу в рамках своїх контрактів з клієнтами, щоб визначити рівень послуги, що продаються на простому рівні. У цьому випадку, як правило, SLA має технічне визначення середнього часу між відмовами (MTBF), середнім часом для відновлення або середнім часом до відновлення (MTTR), визначення того, яка сторона несе відповідальність за повідомлення про несправності, відповідальність за різні швидкості передачі даних, пропускна здатність або подібні вимірювані деталі.

Відповівши на нього можна перейти визначити які дані про безпеку слід збирати.

Відповідно до політики безпеки і умовам договорів SLA необхідно отримувати від ваших клієнтів певні дані. Як правило, чим ширше масштаби моніторингу безпеки, тим більше докладніші дані потрібно збирати. Іншими словами, можливі суттєві відмінності в характері і обсязі зібраних даних, що залежать від конкретного підприємства

2) Визначити, за якими даними слід проводити аналіз і визначати кореляцію. Аналізувати весь трафік, недоцільно. Навіть малі та середні підприємства можуть видавати воістину колосальні обсяги даних. Можна, можливо спростити цей процес, проводячи аналіз і кореляцію тільки тих даних,

які створені в результаті аналізу результатів опитувань по протоколу SNMP, повідомлень SNMP-trap, syslog-повідомлень і даних NetFlow. Засоби аналізу і механізми кореляції миттєво ідентифікують потенційні інциденти в сфері безпеки, і ці функції виключно важливі для забезпечення належної якості сервісів.

Якщо ми використовуємо аутсорсинговий SOC, то аналіз і визначення кореляції можуть виконуватися як в центрі інтегратора, так і на самому підприємстві. Більшість провайдерів вибирають перший варіант, але через обмеженості смуги пропускання більш привабливим може стати другою. В будь-якому випадку підприємство буде проінформоване, якими даними користуєтеся інтегратор для збору інформації про інциденти в сфері інноваційної та кібербезпеки. Інтегратор повинен гарантувати підприємству, що ніяка конфіденційна інформація, тобто інформація, пов'язана з їх поточною діловою активністю, не потрапляє в центр SOC. Це послужить додатковим аргументом для представників керівництва організацій.

3) Аналіз відповідних подій в сфері безпеки.

Виконавши аналіз і визначивши кореляцію інформаційного трафіку клієнта потрібно виділити інциденти в сфері безпеки з коректного трафіку і сконцентрувати свою увагу на них. Важливо виділяти тільки ті інциденти, які є фактичним порушенням політики безпеки. Наприклад, неможливо виконати перевірку кожної рядки з двох мільйонів syslog-повідомлень, створених фаєрволом. Виділивши тільки ті рядки, які відповідають загрозу безпеці можливо ефективно використовувати дефіцитні ресурси в сфері інформаційних технологій.

4) Залучення експертів з безпеки.

Після того як SOC виділить потенційний інцидент в сфері безпеки, до роботи приступають експерти з безпеки. Ці люди мають професійні навички і

досвідом для аналізу потенційного порушення безпеки і швидкого і ефективного усунення наслідків порушення безпеки.

Останній етап в побудові архітектури SOC як сервісу та гібридного - формування процесу, за допомогою якого підприємство отримуватиме інформацію про кожен інцидент в сфері безпеки і контролювати процес його усунення. При виникненні інциденту генерується облікова картка (так званий Trouble Ticket) і надається підприємству, якого торкнувся цей інцидент, доступ до цієї картці відповідно до умов договору SLA або політикою безпеки. Крім цього, можуть складатися докладні щотижневі, щомісячні та річні звіти, що дозволяє додатково зміцнити взаємини з підприємствами.

Розглянемо шість етапів прийняття заходів у відповідь у разі виникнення інцидентів.

Отже, архітектура центру SOC сформована, але як і раніше необхідні ефективні і результативні заходи у відповідь на випадок виявлення загрози безпеці.

Для цього служать шість етапів прийняття заходів у відповідь у разі виникнення інцидентів (див. Рисунок 1.4), докладний опис яких наведено нижче.

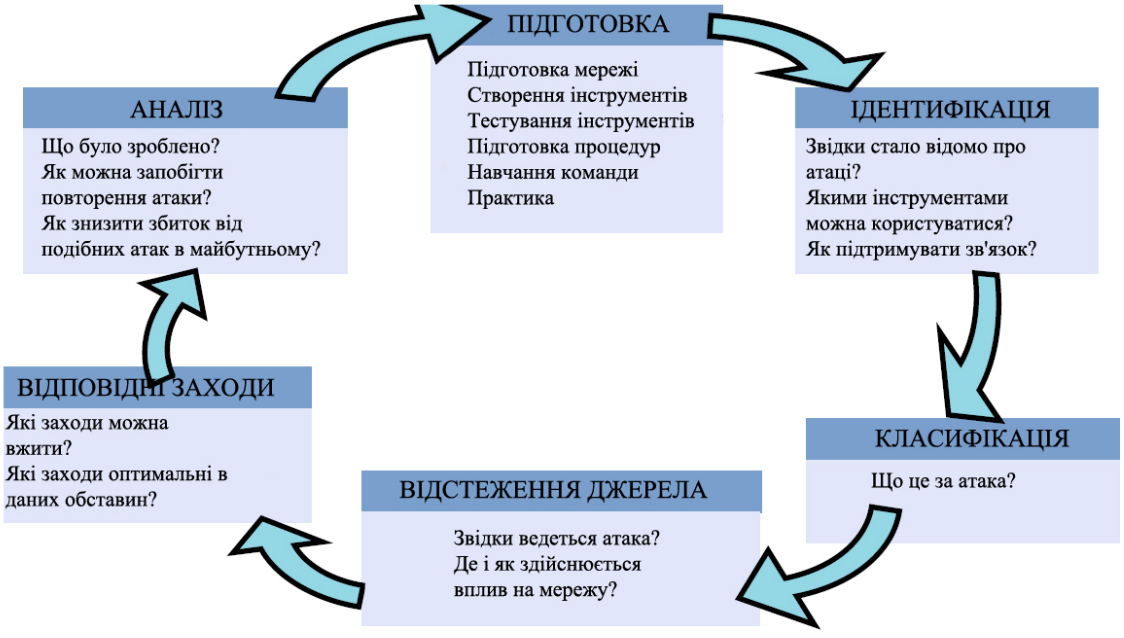

Рисунок 1.4 Шість етапів реакції на інцидент

1) Підготовка

Продумана підготовка - важливий елемент продуманої реакції на інциденти. Якщо ви добре підготовлені, ви знаєте, що і як робити, якщо виникне інцидент в сфері безпеки. Хороша підготовка - це:

- Залучення досвідчених дипломованих фахівців.
- Розробка та оформлення плану забезпечення безпеки.
- Придбання необхідних інструментів.
- Впровадження процедур забезпечення безпеки.
- Навчання персоналу центру SOC роботі з інструментами і процедурами.
- Регулярна перевірка безперервності експлуатації.
- Наявність постійно діючих договорів про супроводі з виробниками / постачальниками.
- Експертна оцінка і кількісний вимір ступеня поліпшення процесу.

Коли ці дії будуть виконані, центр SOC зможе швидко і ефективно реагувати на виникаючі мережеві загрози. Необхідно переконатись в тому, що весь персонал добре знайомий з завданнями центру і з передбаченими процедурами. Ретельне планування, що забезпечує готовність, і впровадження надійних базових параметрів для прийняття відповідних заходів позбавлять від помилок і пропусків, які можуть відчутно знизити ефективність дій в критичних ситуаціях.

2) Ідентифікація

Виявляти інциденти в сфері безпеку необхідно безумовно до того, як вони торкнуться мережі. Для того щоб отримати таку цінну можливість, використовуйте аналітичні інструменти і дані моніторингу, одержувані за допомогою NetFlow, опитувань по протоколу SNMP, повідомлень SNMP-trap і syslog-повідомлень[11].

3) Класифікація

Після того як атака ідентифікована, необхідно оцінити ступінь її серйозності і масштаб: чи зачіпає атака один вузол, або всю інфраструктуру?

4) Відстеження джерела

У атаки є жертва і джерело. Після того як загроза класифікована фахівці повинні знайти точку її проникнення: це може бути мережу організації-партнера, сервер в мережі більш високого рівня, сервер в мережі нижчого рівня або зламані мережеве пристрій в центрі обробки даних.

5) Відповідні заходи

Класифікувавши атаку і виявивши її джерело, фахівці центру SOC застосовують інструменти та процедури придушення атаки. Для того щоб ця робота була успішною, необхідна наочна картина стану мережі і добре прописані стандартні операційні процедури. Дотримуючись цих процедур, немає ризику в погіршені проблеми.

6) Аналіз

Фахівці з безпеки повинні аналізувати вихідні причини кожного інциденту і вносити знайдені нові рішення в робочі інструкції по вирішенню інцидентів, щоб використовувати їх для довідки при виникненні чергового інциденту.

Навіть бездоганні процедури реакції на інциденти принесуть мало користі, якщо у фахівців немає достатніх професійних навичок або досвіду правильного застосування таких процедур. Тому необхідно зібрати команду фахівців центру SOC і створити оперативну групу для вирішення інцидентів.

Розглянемо вимоги до професійних навичок команди фахівців SOC.

Працівники центру SOC повинні бути фахівцями одночасно і по магістральних мереж провайдерів послуг, і по забезпеченню безпеки. Фактично, фахівці центру SOC повинні бути знайомі з наступними аспектами функціонування мереж провайдерів:

- Функціонування ядра і магістральної мережі.
- Підключення клієнтської мережі до ядра або магістральної мережі.
- Управління мережею, включаючи системи підтримки функціонування (OSS).
- Системи хостингу і зберігання контенту.
- Діяльність спільнот, наприклад, з безпеки провайдерів мережевих сервісів (NSP-SEC).
- Система доменних імен (DNS), протокол DHCP, схеми адресації і процедури забезпечення безпеки.
- Функціонування групи реагування на надзвичайні ситуації (CERT).

Фахівці центру SOC також повинні володіти знаннями, які необхідні звичайному технічному фахівцеві з безпеки. Спираючись на належні інструменти і процедури, можливо оптимізувати і масштабувати професійні навички таких працівників.

Створення оперативної групи для вирішення інцидентів у випадку гібридної, або моделі SOC як ервіс.

Фахівці центру SOC забезпечують його повсякденну роботу, але на випадок реальних атак, можливо, слід створити спеціальну оперативну групу для вирішення інцидентів. Така спеціальна оперативна група буде потрібно, якщо центр SOC діє незалежно від центру NOC. Якщо ці два центри працюють як єдиний підрозділ, фахівці центру SOC формують оперативну групу, при цьому до них приєднується ряд нетехнічних фахівців, згаданих нижче. В будь-якому випадку, розмір такої оперативної групи, як правило, буде змінюватися в залежності від кількості і розміру контрольованих мереж.

Якщо центри SOC і NOC працюють окремо, в оперативну групу по вирішенню інцидентів повинні входити представники і SOC, і NOC. Це надає можливість оперативно визначити, що є джерелом інциденту мережу або міжмережевий екран - і чи можна віднести інцидент до сфери інформаційної

безпеки. Наприклад, якщо оформляється облікова картка, можливо, в першу чергу її слід направити в центр NOC. Якщо центр NOC встановить, що з мережею все в порядку, картка буде перенаправлено в центр SOC. Якщо фахівці SOC підтвердять що міжмережевий екран функціонує справно, облікова картка буде передана в оперативну групу дозволу інцидентів. Завдяки залученню фахівців з центру SOC і NOC, ця команда має концептуальне бачення і професійними навички, які необхідні для системного підходу до вирішення проблеми, для застосування інструментів, прийомів і процесів ідентифікації інцидентів, відстеження їх джерел і прийняття належних заходів у відповідь.

Також слід включити в оперативну групу по вирішенню інцидентів ведучого фахівця з інформаційної безпеки, провідного спеціаліста з інформаційних технологіям, головного юрисконсульта, менеджера зі зв'язків з громадськістю та, можливо, інших працівників.

Атестація готовності працівників і мереж.

Якщо обидві команди фахівців і мережу підготовлені, ви можете дати відповіді на наступні питання:

- Нормальні ці шаблони трафіку для нашої мережі?
- Що займає всю нашу смугу пропускання?
- Дзвонять розсерджені клієнти. Що трапилось?
- Чому сервер, мережа або автономна система недоступні?
- Чи не стався Чи незаконне захоплення наших маршрутизаторів іншим провайдером?
- Чи необхідно нам змінити атрибути або політику BGP?

У центрі SOC повинні існувати встановлені процедури зв'язку з працівниками, підприємством і взаємодіючими провайдерами на випадок, якщо чиясь мережа піддається атаці. Фактично, необхідно застосовувати шестиетапний процес реакції на інциденти, описаний раніше. Точна контактна

інформація допоможе пройти ці шість етапів швидше і ефективніше. Тому необхідно зібрати і своєчасно оновлювати таку інформацію:

● Всі найважливіші адреси електронної пошти, номери телефонів і пейджерів, URLадреса Web-сторінок.

● Контактні особи всіх взаємопов'язаних провайдерів - одного рівня з вашої організацією і більш високого рівня - а також виробників, постачальників і клієнтів.

● Контактні особи ваших постачальників з оперативних груп забезпечення безпеки продуктів і особи, відповідальні за прийняття заходів у відповідь.

● Політики, які встановлюють рівень підтримки клієнтів, порядок класифікації та відстеження джерел атак, методи прийняття заходів у відповідь (Наприклад, чи буде застосовуватися у вашій інфраструктурі скидання пакетів, формують атаку?).

● Процедури відповідей на питання і процедури взаємодії.

В результаті функціонування центру SOC повинні з'являтися такі результати, багато з яких будуть видаватися у формі звітів:

● Моніторинг безпеки з метою управління ризиками.

● Аналіз ризиків для визначення стану безпеки.

● Надійний доступ до порталу моніторингу безпеки з використанням рольової моделі контролю доступу.

● Моніторинг в режимі реального часу; встановлення стану обробки інцидентів і ведення облікових карток.

● Звіти про політику безпеки.

● Звіти про інциденти в сфері безпеки.

● Експертиза інцидентів в режимі реального часу, а також оформлення щотижневих і щомісячних звітів.

● Інформація, необхідна для підготовки до аудиторської перевірки дотримання нормативних вимог.

● Звіти за договорами SLA.

● Звіт про підтвердження дотримання політики безпеки.

● Динаміка інцидентів і подій в сфері інформаційної безпеки.

Важлива роль звітності

Як можна зробити висновок на підставі перерахованих результатів, звітність грає винятково важливу роль в ефективній роботі центру SOC. В кінцевому підсумку, ви розробите власні стандарти звітності про інциденти, але, відповідно до накопиченим практичним досвідом, в цих звітах повинні бути присутніми деякі загальні складові, зокрема, час і дата реакції на інцидент, ідентифікаційні дані і результати класифікації атаки, основна причина, метод виявлення, метод відображення і результати аналізу ризиків (тобто як можна уникнути виникнення цієї проблеми в майбутньому).

Крім цього, не слід оприлюднювати інформацію, яка може негативно відбитися на функціонуванні центру SOC або зробити вас вразливою мішенню для хакерів.

Іншими словами, проявити належну увагу на етапі остаточного оформлення звітів. На додаток до цього, якщо звіти про інциденти можуть бути віддані гласності, перед публікацією зміст цих звітів повинен оцінити фахівець зі зв'язків з громадськістю або юрисконсульт.

Для того щоб підвищити цінність звітів про інциденти, по можливості вказуйте час в стандарті UTC (за Гринвічем) стосовно до всієї інфраструктури маршрутизації і комутації, інструментів забезпечення безпеки і критично важливим серверів. Стандартизація по UTC надасть можливість сформувати загальний тимчасової базис для простої консолідації та об'єднання даних, що

надходять від сенсорів. Звівши до мінімуму перерахунок часу, ви усунете ризик випадкового спотворення зібраних відомостей.

Необхідно простежити за тим, щоб в списки контактних осіб були включені всі люди, які брали участь в обробці з інцидентом, і вказані їх ролі. Ця інформація виключно важлива для аналізу інцидентів і боротьби з інцидентами подібного характеру. І наостанок, необхідно надати доступ до ваших звітів через портал моніторингу безпеки. На цьому порталі повинна бути відображена послідовна картина стану безпеки в масштабах всієї мережі.

1.5 Висновок

У розділі розглянуті основні задачі, процеси центрів оперативного управління кібербезпекою та їх описання. Були проаналізовані їх моделі та надана порівняльна характеристика.

Центр реагування на критичні інциденти ІБ може бути власним або аутсорсинговим. У будь-якому випадку, впроваджуючи SOC, організація одночасно реалізує частину процесів системи управління ІБ (СУІБ) відповідно до стандарту ISO 27001 (процес управління інцидентами ІБ, управління уразливостями і змінами, контроль відповідності законодавчим та галузевим вимогам), а також виконує частину вимог стандарту PCI DSS.

Проаналізовано та запропоновано типову архітектуру та визначені етапи її розгортання на підприємстві.

1.6 Постановка задачі

На основі приведених типових архітектур центрів оперативного управління кібезбезпекою проаналізувати фактори які впливають на вибір архітектури та розробити рекомендації щодо її вибору. Запропонувати порядок розвертання SOC на установі.

РОЗДІЛ 2

РЕКОМЕНДАЦІЇ ДЛЯ ПІДПРИЄМСТВА ЩОДО ПОБУДОВИ ЦЕНТРУ ОПЕРАТИВНОГО УПРАВЛІННЯ КІБЕРБЕЗПЕКОЮ

2.1 Аналіз факторів які впливають на вибір рішення

Можна виділити такі основні фактори які будуть впливати на вибір архітектури впроваджуваної SOC:

1) Складність архітектури ІС

Масштаб системи служить основою для подальшого планування, розгортання, впровадження та дозрівання SOC і пов'язаних з ним можливостей. Він впливає на вибір рішення, архітектурні вимоги, необхідний штат співробітників, а також процеси і процедури.

Наявність філіалів, можливість співробітників працювати віддалено.

Кількість користувачів в системі. Чим більша кількість користувачів, тим більше транзакцій проводиться в системі і тим більше джерел інцидентів може бути.

Сфера застосування. Можна виділити такі класи комп'ютерних інформаційних систем:

- системи для наукових досліджень;
- системи автоматизованого проектування;
- системи організаційного управління;
- системи управління технологічними процесами.

З названих класів детальніше виділимо два:

Інформаційні системи організаційного управління призначені для автоматизації функцій адміністративного (управлінського) персоналу. До цього класу належать системи управління як промисловими (підприємства), так і

непромисловими об'єктами (банки, біржі, стра-хові компанії, готелі тощо) й окремими офісами (офісні системи).

Інформаційні системи управління технологічними процесами призначені для автоматизації технологічних процесів (гнучкі виробничі процеси, металургія, енергетика тощо)[12].

Де та як обробляється інформація:

- Локальна мережа без виходу в інтернет
- Локальна мережа з виходом в інтернет
- Локальна мережа з використанням хмарних сховищ
- Вся інформація зберігається і обробляється в хмарних сховищах

Процеси в організації, прикладом може бути:

- управління розробками;
- управління фінансами;
- управління виробництвом (планування і виготовлення)
- управління складами;
- управління основними фондами;
- управління замовленнями (договорами);

2) Кваліфікація персоналу IT та ІБ

SOC повноцінно працює лише в руках професіоналів і, будучи встановленої у великій організації, може зажадати команду з 8 виділених співробітників. SOC є інструментом, що вимагає висококваліфікованих фахівців, для досягнення значущих результатів.

Необхідно переконатись, що організація здатна використовувати SOC. Чи є необхідні ресурси і персонал? Чи зможете вона найняти і навчити нових співробітників.

3) Наслідки від порушення КБ

Критерії, які можуть використовуватися, щоб оцінити можливі наслідки, що випливають із втрати спостережливості, автентичності або надійності активів[13]:

- порушення законодавства та / або регулювання;
- погіршення продуктивності бізнесу;
- втрата доброзичливості / негатив на репутації;
- порушення, пов'язане з особистою інформацією;
- загроза персональної безпеки;
- негативні впливи на приведення законів у життя;
- порушення конфіденційності;
- фінансова втрата;
- перерву бізнес діяльності;

Інший підхід, щоб оцінити наслідки, може бути в:

- Переривання сервісу:
    - Нездатність надати послугу.
- Втрата довіри клієнта:
    - Втрата довіри у внутрішній інформаційній системі;
    - Шкода репутації.
- Руйнування внутрішньої працездатності:
    - Руйнування безпосередньо в організації;
    - Додаткової внутрішньої вартості.
- Руйнування працездатності третьої особи:
    - Руйнування у третіх осіб, які проводять операції з організацією;
    - Різного типи пошкодження.
- Порушенні законів / інструкції:
    - Нездатність виконати юридичні зобов'язання.
- Порушенні умов контракту:

    - Нездатність виконати договірні зобов'язання.
- Небезпека для персоналу / користувальницької безпеки:
    - Небезпека для персоналу організації та / або користувачів.
- Атака на приватне життя користувачів.
- Фінансових втрати.
- Фінансовою вартості для надзвичайної ситуації або відновлення в термінах:
- Персоналу;
- Обладнання;
- Досліджень, звітів експертів.
- Втрата товарів / грошових коштів / активів.
- Втрата клієнтів, втрати постачальників.
- Судових позовах і штрафах.
- Втрата переваг конкурентоспроможності.
- Втрата технологічної / технічної головній ролі.
- Втрата ефективності / довіри.
- Втрата технічної репутації.
- Зниженні ролі у веденні переговорів.
- Індустріальних кризах (ударах).
- Урядових кризах.
- Звільнення.
- Матеріальні збитки.

Ці критерії - приклади проблем, які розглядаються для оцінки активу. Для того щоб виконати оцінки, організація повинна вибрати критерії, які стосуються її типу вимог безпеки і бізнесу. Це могло б означати, що деякі із згаданих вище критеріїв не застосовні і що інші, можливо, повинні бути додані в список.

4) Дуже важливою складовою є бюджет підприємства, та те, які кошти підприємство готово витрачати на забезпечення І та КБ.

2.2 Рекомендації щодо вибору типу та архітектури центру оперативного управління кібербезпекою

Розглянемо в яких випадках взагалі необхідно будувати центр оперативного управління кібезбезпекою:

- Компанії потрібно підвищення стійкості бізнес-процесів і бізнес-інфраструктури. Ключова теза для бізнесу. Власники бізнес-процесів і бізнес-інфраструктури, повинні бути поінформовані про операційні ризики, пов'язані з погрозами І та КБ, і їх вплив на бізнес. Якщо керівництво компанії звертає увагу на необхідність підвищення стійкості бізнес-процесів і бізнес-інфраструктури, то варто замислитися над створенням SOC як відповідь на існуючі виклики І та КБ.
- Компанія володіє розвиненим ландшафтом І та КБ. Істотні капітальні витрати в ІБ призводять до того, що бізнес вимагає обґрунтування інвестицій і підвищення ефективності як самих підсистем, так і процесів супроводу.
- Процеси ІБ формалізовані, потрібно їх уніфікація та оптимізація, необхідне впровадження нових складних процесів (наприклад, threat hunting). Зростання операційних витрат також може вказувати і підштовхувати компанію до рішення про створення SOC. В рамках проекту по його створенню зазвичай проводиться реінжиніринг процесів та їх оптимізація, що може «перезавантажити» існуючі процеси і операції і підвищити їх ефективність.
- Необхідна уніфікація процесів в ІС. Уніфікація і SOC можуть дозволити компанії вибудувати спільні процеси з ІС.

1) Побудова власного центру оперативного управління кібербезпекою

Побудова локального центру оперативного управління кібербезпекою буде актуальна для компаній і корпорацій сегмента Enterprise. Компаній з великою кількістю співробітників загальна сума яких може перевищувати тисячу чоловік. Це компанії в яких є філіали в різних містах або інших країнах світу. Саме в цьому сегменті департамент інформаційної безпеки має значний штатний склад, власні бюджети і чітко окреслене коло вирішуваних завдань.

Висока цінність інформації, що захищається, велика кількість різних засобів її захисту, територіально розподілена структура, кількість працівників в кілька тисяч чоловік - якщо ці критерії відносяться до профілю компанії, напевно створення власного SOC - питання часу.

Основою будь-якого центру моніторингу і реагування на інциденти інформаційної безпеки є такі компоненти[14]:

- персонал - інженери, аналітики, архітектори, адміністратори;
- контент - набори кореляційних правил, регламенти аналізу інцидентів, шаблони оповіщення, бази знань по різним загрозам і векторах атак;
- процеси - процедури розбору інциденту, реагування, звітності, ескалації та протидії інцидентів;
- потужності і ліцензії - розміщення платформи SOC, SIEM-системи, засобів моніторингу працездатності, сховища подій, інцидентів, ліцензії SIEM-системи і додаткових модулів.

Якщо питання з потужностями та ліцензіями можна вирішити за допомогою прямих фінансових вливань, то перші три пункти вимагають величезних тимчасових і трудовитрат. Давайте розглянемо докладніше саме ці пункти.

На українському ринку існує дефіцит фахівців і інженерів. Пошук одного аналітика часто займає кілька місяців, в залежності від пропонованих умов. Далі необхідно ще до півроку, в залежності від кваліфікації працівника, для повноцінного включення його в роботу. Якщо ж у компанії існують вимоги до організації моніторингу 24x7, то ситуація ускладнюється ще більше.

Наповнення SIEM-системи контентом є найважливішим завданням, тому що базовий набір правил не здатний закрити всі потенційні вектори загроз для компанії, особливо класу Enterprise. Для вирішення даного завдання необхідний архітектор SIEM-системи, який буде вибудовувати контент в залежності від поставлених перед SOC цілей, адаптувати його під інфраструктуру,

реалізовувати сценарії виявлення інцидентів в бізнес-додатках. Також необхідні інженери для підключення джерел і написання конекторів до додатків, адміністратор, що забезпечує працездатність і займається "залізної" архітектурою.

Крім персоналу і контенту, не менш важливою задачею є строга регламентація процесів виявлення, аналізу інцидентів, сповіщення відповідальних осіб, вибудовування схем взаємодії між підрозділами. Необхідно не тільки забезпечити процедуру повідомлення та розслідування кожного типу інциденту, а й передбачити SLA, ескалацію і звітність. За інцидентів високою критичності варто заздалегідь передбачити можливість втручання в бізнес-процеси аж до зупинки останніх, оцінивши ризики наслідків інциденту і порівнявши їх з втратами від тимчасового простою окремих підрозділів.

2) Використання центру оперативного управління кібезбезпекою як сервісу

Для великої компанії, яка бажає побудувати власний SOC з нуля, спроба реалізації може зайняти роки і не увінчатися успіхом. Виникнення проблем в будь-якому з пунктів(персонал, контент, процеси, потужності), може занапастити ідею SOC-будівництва. Найчастіше це може статися не з вини відповідальних за SOC департаментів, а через внутрішні взаємодії всередині структури компанії, конфліктів з бізнес-підрозділами.

Іншим важливим аспектом, який варто враховувати при побудові власного центру моніторингу, є бажання бізнесу виділяти гроші на забезпечення безпеки тут і зараз. Він часто не готовий чекати 1-2 роки, поки внутрішній SOC почне працювати .

Тут і допоможе сервіс-провайдер, "закривши" перехідний період до запуску власного Security Operations Center, вмонтувавши свої процеси в поточну модель інформаційної безпеки компанії.

SOC як сервіс значно знижує ризики невдачі, дозволяючи запустити моніторинг в найкоротші терміни, надаючи експертизу, команду і контент. При цьому капітальні витрати відсутні, що дозволяє відключитися від хмарного SOC в будь-який момент.

Якщо ви використовуєте SOC як сервіс, то відразу вирішуєте проблему персоналу (як інженерів, так і аналітиків), наповнення контентом SIEM-системи, розробки регламентів і процесів взаємодії при виявленні, аналізі та протидію інцидентів - всі завдання лягають на плечі аутсорсера. При цьому сервіс-провайдер враховує специфіку компанії і внутрішні вимоги до організації процесу. У регламенті відбивається чіткий поділ відповідальностей між замовником і підрядником.

Але якщо компанія налаштована на будівництво власного SOC, в рамках перехідного періоду найбільш цікавим варіантом до розгляду є використання гібридної моделі Security Operations Center, що має на увазі під собою використання власної SIEM-системи, яку сервіс-провайдер забирає на адміністрування і опирається на неї контент, оптимізуючи під замовника. Гібридний варіант також вирішує завдання швидкого пошуку команди моніторингу, що дає додатковий час компанії на пошук власної команди.

3) Використання гібридного центру оперативного управління кібезбезпекою

У разі гібридної моделі SIEM-система купується на кошти компанії і розташовується в її інфраструктурі. Вибір потрібного рішення є складним питанням, і при вирішенні використовувати гібридний SOC необхідно враховувати тенденції ринку і думка компанії, яка надає аутсорсингові послуги.

Первісна установка і настройка рішення може реалізовуватися як інтегратором, організуючим поставку, так і сервіс-провайдером, що забезпечує моніторинг. Причому другий варіант кращий, так як при підключенні компанії до сервісу з виявлення інцидентів підрядник найчастіше використовує свої

коннектори, парсери, настройки SIEM-системи, і його залучення дозволить виключити подвійну роботу.

На період надання сервісу адмініструванням системи збору подій і серверів конекторів зазвичай займається аутсорсер, а замовнику надається обмежений доступ до консолі SIEM-системи. Такий підхід пов'язаний як з політикою конфіденційності та захисту авторського контенту, так і з поділом відповідальностей - сервіс-провайдер відповідає за працездатність системи, в тому числі і грошима, тому намагається мінімізувати ризики, пов'язані з людським фактором і нештатним втручанням в роботу ПО.

Паралельно з технічними роботами на SIEM-системі відбувається обстеження інфраструктури, спілкування з власниками систем, службою ІБ, ІТ і вибудовування процедури взаємодії при розборі різних типів інцидентів. Документ, що розробляється в процесі обстеження, представляє собою готовий регламент, який в подальшому може використовуватися замовником при запуску власного SOC.

Крім регламенту реєстрації та оповіщення по інцидентах ІБ, важливим процесом є процедура взаємодії з ключовими підрозділами при розборі інцидентів і протидії загрозам. Період надання сервісу дозволить створити уявлення про те, як вибудовувати взаємодію з ІТ-відділом, службою сервіс-деск, бізнес-підрозділами до моменту запуску внутрішнього SOC.

При використанні гібридного варіанту вирішуються в тому числі ті деякі проблеми використання хмарного SOC, які турбують деякі компанії:

- Події інформаційної безпеки з систем-джерел компанії залишаються в її інфраструктурі.
- Після відключення від послуги сервіс-провайдера у компанії залишається система збору подій, яку можна використовувати далі.
- Завантаження інтернет-каналу при гібридному варіанті значно нижче, ніж при хмарному варіанті підключення.

Навіть при відключенні від послуг сервіс-провайдера регламенти, процедури, відпрацьовані з сервіс-провайдером, можна використовувати в рамках внутрішнього центру оперативного управління кібезбезпекою, зібравши власну команду аналітиків, адміністраторів та інженерів моніторингу. Також більшість аутсорсеров дозволяють "викупити" контент і допомагають в ньому розібратися. Таким чином, коли команда буде готова, набереться досвіду в розборі і розслідуванні інцидентів, необхідно буде лише перевести SIEM-систему під свій контроль і продовжити моніторинг інцидентів.

Даний спосіб нівелює ризики невдалого злету, забезпечує моніторинг і розбір інцидентів тут і зараз і дозволяє зібрати команду і ввести її в процес плавно, не порушуючи процеси інформаційної безпеки компанії.

2.3 Порядок розгортання SOC на установі

Базові етапи впровадження SOC:

1) Обстеження підприємства

На цьому етапі досліджується вся ІС підприємства, проводиться аналіз архітектури, виділяють основні функції цієї системи, бізнес-процеси, масштаб системи, визначається для яких бізнес активів необхідний моніторинг і захист.

Спроба розгорнути SOC без попередньої оцінки масштабу безнадійна. Масштаб системи служить основою для подальшого планування, розгортання, впровадження та дозрівання центру оперативного управління кібербезпекою. Він впливає на вибір рішення, архітектурні вимоги, необхідний штат співробітників, а також процеси і процедури.

Потрібно бути готовим до того, що проекти з впровадження SOC тривалі. Знадобиться близько року, щоб накопичити бібліотеку відпрацьованих сценаріїв і навичок, які дозволять ефективно реалізувати і розширювати ваш SOC. Рекомендується застосовувати багатоступінчастий підхід, що охоплює не тільки початкова розгортання, а й наступні етапи, в рамках яких будуть охоплені додаткові сценарії і підключені нові джерела даних для їх підтримки.

Після цього етапу у нас є вся інформація про систему, яка необхідна для вибору програмних продуктів, кількості персоналу, яке апаратне оснащення нам необхідно, тому наступним етапом є проектування.

2) Проектування SIEM – системи

На цьому етапі необхідно:

- Сформувати проектну групу, в основні обов'язки якої увійде визначення цілей, масштабів та етапів проекту, а також виявлення кінцевих споживачів.
- Визначити цілі моніторингу подій безпеки і початкову область розгортання проекту.
- Визначити вихідні сценарії використання, які охоплюються SIEM.
- Визначити вимоги до збору даних, зберігання, звітності і моніторингу подій безпеки.
- Оцінити, скільки і які джерела даних будуть необхідні для обраних сценаріїв (з точки зору кількості подій в секунду, внутрішнього сховища або обчислювальної потужності), а потім перевірити, чи можна отримати доступ до цих джерел даних.

Після цього зібрана інформація використовується для:

- Оцінки середовища і ресурсів.
- Оцінки вимог до архітектури та методів збору даних, щоб відповісти на наступні питання: які зусилля будуть потрібні для інтеграції джерел даних, та чи підтримують ці джерела ведення журналів безпеки без шкоди для продуктивності,
- Визначення здатності джерел даних генерувати очікувані події. На деякі джерела логів можуть бути накладені обмеження через продуктивності, версій програмного забезпечення і т. Д.

- Опрацювання процесу моніторингу подій і реагування на інциденти. Приділіть особливу увагу деталізації сценаріїв реагування (playbooks), після того як ваш SIEM почне генерувати інциденти.
- Створення відповідних процесів і політик з метою оцінки необхідних ресурсів для SIEM.

Після зібраної інформації проводять вибір необхідного технічного обладнання і програмних засобів.

З основних джерел даних можна виділити:

- Access Control, Authentication (контроль доступу, аутентифікація користувачів)
- Журнали подій серверів і робочих станцій
- Мережеве активне обладнання
- IDS \ IPS
- Антивірусний захист
- Сканери вразливостей
- GRC-системи для обліку ризиків
- Інші системи захисту і контролю політик ІБ: DLP, контроль пристроїв.
- Системи інвентаризації, asset-management
- Netflow, системи обліку трафіку

3) Закупівля технічного оснащення та ліцензії на програмні продукти.

Згідно з проектом системи SIEM закуповується необхідне технічне обладнання, та ліцензії на програмне забезпечення, яке необхідне для працездатності системи.

Технічне обладнання являє собою комп'ютери для моніторингу, сервери-колектори, призначені для попередньої акумуляції подій від безлічі джерел, сервер-корелятор, що відповідає за збір інформації від колекторів і агентів і

обробку за правилами і алгоритмами кореляції, сервер баз даних і сховища, який відповідає за зберігання журналів подій, та мережеві пристрої.

4) Пошук та найм спеціалістів.

Наразі в Україні немає висококваліфікованих спеціалістів з досвідом роботи у центрах SOC, тому необхідно залучити фахівців із-за кордону чи провести перекваліфікацію наявних кадрів у відділі ІБ.

Мінімально необхідний штат команди SOC виглядає так:

- Керівник SOC - 1 спеціаліст;
- Аналітик SOC - 1 спеціаліст;
- Технічний експерт -1 спеціаліст;
- Адміністратор SIEM -1 спеціаліст;
- Група моніторингу та реагування - 4 спеціалісти.

5) Розгортання, підключення джерел подій до SIEM

Встановлюються всі технічні пристрої, програмні засоби, та підключаються джерела подій.

6) Налаштування SIEM, впровадження сценаріїв подій, розробка правил кореляції, звітність.

Налаштовуємо фільтри для входу даних в SIEM, обладнання, панелі візуалізації та ін.

За сценарії подій вважаємо конкретний набір правил, скриптів і/або механізмів візуалізації. Наприклад, для виявлення сканування портів, звірки IP адреси з зовнішньої репутаційної базою і т.д. Сценарії подій можна писати самому, брати готові з сайту виробника або замовляти у підрядників.

Зараз всього 4 виробника організували власні майданчики для публікації сценаріїв подій. Також у більшості виробників є внутрішній форум для обміну інформацією та пошуку рішень виникаючих проблем.

- HPE ArcSight Marketplace – в наявності платні і безкоштовні. Якщо не застосовувати додаткову фільтрацію, то на сайті сумарно 170 сценаріїв подій[15].
- IBM Security App Exchange - завантаження безкоштовно. Усього доступно 73 сценаріїв подій, розробленим як самим IBM, так і партнерами[16].
- LogRhythm - поки всього 19 сценаріїв подій[17].
- Splunk - підрозділ "Security, Fraud and Compliance" містить 487 додатків. Але якщо відфільтрувати тільки додатки (а не аддони, хоча вони теж важливі) і вказати версію продукту 6.0 і вище - то сумарна кількість зменшується до 236 сценаріїв подій[18].

Для розробки правил кореляції збираємо всю інформацію яку нам може дати SIEM система, і починаємо фільтрувати. З основних методів кореляції можна виділити[19]:

- Заснований на правилах (rule based) - взаємозв'язку між подіями визначаються аналітиками в заздалегідь заданих специфічні правила.
- Заснований на графах (graph based) - пошук залежностей між системними компонентами в поданні у вигляді графа.

Інструменти SIEM повинні бути налаштовані під ваші індивідуальні вимоги для розпізнавання специфічних для вас подій.

Щоб цілеспрямовано збирати й аналізувати тільки релевантні дані, SIEM повинна орієнтуватися на результат. Це означає, що дані про події повинні збиратися, тільки якщо вони необхідні для кінцевого результату. Джерела логів і подій повинні прийматися тільки для конкретних сценаріїв, правил кореляції, звітів і панелей моніторингу. Наприклад, для типового сценарію моніторингу підозрілих вихідних підключень і передачі даних, потрібні тільки логи брандмауера, проксі-сервера і дані мережевого потоку. Підключення журналів DHCP або доступу до веб-додатків буде вже зайвим.

7) Тестування системи

За допомогою тестових даних оцінюється можливість і зручність обробки подій з урахуванням процесів і технологій, розроблених в рамках проекту.

Завершивши ці етапи можна впроваджувати SOC.

Після запуску проводиться підтримка діяльності та перевірка ефективності SOC.

В ході роботи оптимізуються існуючи процеси, наймthemся нові спеціалісти та підключатися нові джерела подій.

2.4 Висновок

У цьому розділі були проаналізовані основні фактори, які можуть впливати на вибір тієї чи іншої моделі SOC, розроблені рекомендації, що на основі приведених факторів може допомогти вибрати архітектуру необхідну для різних типів підприємств. Представлений порядок розгортання SOC на установі.

РОЗДІЛ 3

ВИЗНАЧЕННЯ ВИТРАТ НА ПРОЕКТУВАННЯ ТА ЕКСПЛУАТАЦІЮ ЦЕНТРА ОПЕРАТИВНОГО УПРАВЛІННЯ КІБЕРБЕЗПЕКОЮ

3.1 Загальні відомості про підприємство

Діяльність приватного підприємства “NewSoft” полягає у розробці і продажі програмного забезпечення.

Офіс підприємства займає перший і другий поверхи офісної п’ятиповерхової будівлі. Об’єктом інформаційної діяльності будуть виступати усі приміщення, де циркулює інформація з обмеженим доступом. Офісна будівля підприємства, знаходиться за адресою: Україна, м. Дніпропетровськ, пр. Дмитра Яворницького, 5.

До активів підприємства відносяться:

- офісне приміщення розташоване за адресою Україна, м. Дніпропетровськ, пр. Дмитра Яворницького, 5, вартість якого складає 10 000 000 грн.;

- річний прибуток підприємства складає 20 600 000 грн.

Загальний кількість персоналу складає 500 чоловік.

Кількість персоналу у відділі інформаційної безпеки 10 чоловік, а саме:

- Аналітики ІБ - 2 чоловіки, заробітна плата яких складає 25 000;

- Інженери ІБ – 8 чоловік, заробітна плата яких складає 8000.

3.2 Розрахунок витрат підприємства на розгортання центу оперативного управління кібербезпекою

Найдорожча складова капітальних витрат - це ліцензії SIEM. Схема ліцензування основних виробників SIEM визначається потоком EPS (кількість подій в секунду, яке надходить в SIEM від інформаційних систем і засобів захисту), який в свою чергу залежить від кількості і типів підключаються джерел.

Вартість розгортання SOC можна визначити по формулі:

$$В_{SOC} = В_{SIEM} + В_{пп} , \text{ грн,} \quad (3.1)$$

де $В_{SIEM}$ – вартість розгортання SIEM;

$В_{пп}$ – вартість перекваліфікації персоналу;

Вартість розгортання SIEM можна визначити по формулі:

$$В_{SIEM} = В_{ТО} + В_{ТР} + С_е, \text{ грн,} \quad (3.2)$$

де $В_{ТО}$ – вартість технічного оснащення;

$В_{ТР}$ – вартість технічних робіт;

$С_е$ - вартість електроенергії, що споживається апаратурою протягом року.

Вартість технічного оснащення можна визначити по формулі:

$$В_{ТО} = В_{аз} + В_{рк} + В_{мо} , \text{ грн,} \quad (3.3)$$

де $В_{аз}$ – вартість апаратних засобів;

$В_{рк}$ – вартість систем резервного копіювання;

$В_{мо}$ – вартість мережевого обладнання;

Вартість технічних робіт можна визначити по формулі:

$$В_{ТР} = В_о + В_п + В_л + В_н + В_{пд} + В_{рпк} + В_{рр} + В_{рі}, \text{ грн,} \quad (3.4)$$

де $В_о$ – вартість обстеження підприємства;

$В_п$ – вартість проектування;

$В_л$ – вартість ліцензії програмних засобів SIEM;

$В_н$ – вартість налаштування SIEM;

$В_{пд}$ – вартість підключення джерел подій;

$В_{рпк}$ – розробка правил кореляції для сценаріїв виявлення інцедентів;

$В_{рр}$ – розробка регламенту реагування на інциденти ІБ;

$B_{рі}$ – розробка інструкцій оператора / аналітика / користувача.

Таблиця 3.1 – Характеристики та вартість мереженого обладнання

Найменування	Характеристика	Кіл-ть	Вартість, грн	Загальна вартість, грн
Комутатор Cisco SB SRW224G4-K9-EU	24-портовий Gigabit Ethernet настільний керований комутатор з доповненими 4 GE Combo mini-GBIC/SFP портами.	3	6 000	18 000
Загальна сума ($B_{мо}$), грн				18 000

Таблиця 3.2 – Характеристики та вартість апаратних засобів

Найменування	Характеристики	Кіл-ть	Вартість, грн	Загальна вартість, грн
Сервери для моніторингу	Intel B85/ Intel Core i5-4570 (3.2 ГГц)/ RAM 16 Gb / HDD 1Tb/ Intel HD Graphics/DVD±RW/ 500W	4	15 000	60 000
Монітор Samsung C24F390F	Діагональ 24 " / 1920x1080 / 60 Гц	4	5 000	20 000
Комп’ютерна мишка Genius Xscroll G5 USB Black	1000 dpi / оптична	4	100	400
Клавіатура Genius KB-110X USB Black	USB / мембранна	4	200	800
Загальна сума ($B_{аз}$), грн				81 200

Таблиця 3.3 – Характеристики та вартість програмних засобів

Вид ПЗ	Назва та версія ПЗ	Тип ліцензії, номер, дійсна до	Вартість, грн
Операційна система	Windows 10 Pro	Комерційна	7 000
	Браузери Opera 38, Google Chrome 51, Safari 5.1,Internet Explorer 8	Індивідуальні публічні ліцензії	-
	Антивірус ESET NOD32 Antivirus Business Edition (3.0.695.0)	Комерційна, до 01.01.19	1 200
Загальна сума, грн			8 200

Таблиця 3.4 – Характеристики та вартість систем резервного копіювання

Найменування	Характеристики	Кіл-ть	Вартість	Загальна вартість
Storage (сервер резервного копіювання)	Intel Xeon E5-2650 (6 ядер)/2.0 ГГц Ram: 16 Гб/ LAN: 1 Гбіт/с (RJ-45) - 2 шт. HDD: Seagate 2x1Tb -SATA Hot Plug/500W	2	10 000	20 000
Загальна сума ($B_{рк}$), грн				20 000

Обстеження підприємства проводитиме стороння організація ПАТ «Security Solution», $B_о$ = 15 000 грн.;

Проектування SIEM проводитиме стороння організація ПАТ «Security Solution», $B_п$ = 15 000 грн.;

Вартість річної ліцензії SIEM ($B_л$) HP ArcSight складає 150 000 грн.

Таблиця 3.4 – Програмні продукти HP ArcSight

№	Найменування
1	HP ArcSight Lgr 30GB/d 200Dev SW E-LTU
2	P ArcSight CONAPP 50 Con SW E-LTU
3	HP ArcSight SC 5.14 Eng SW E-Media
4	RTS Charge

Налаштування SIEM проводитиме стороння організація ПАТ «Security Solution», $В_н$ = 25 000 грн.;

Підключення джерел подій до SIEM проводитиме стороння організація ПАТ «Security Solution», $В_{пд}$ = 15 000 грн.;

Розробку правил кореляції для сценаріїв виявлення інцедентів проводитиме стороння організація ПАТ «Security Solution», $В_{рпк}$ = 15 000 грн.;

Розробку регламенту реагування на інциденти ІБ проводитиме стороння організація ПАТ «Security Solution», $В_{рр}$ = 10 000 грн.;

Розробку розробка інструкцій оператора / аналітика / користувача проводитиме стороння організація ПАТ «Security Solution», $В_{рі}$ = 10 000 грн.;

$$В_{ТО} = 81\ 200 + 20\ 000 + 18\ 000 = 119\ 200 \text{ грн.}$$

$$В_{ТР} = 15\ 000 + 15\ 000 + 150\ 000 + 25\ 000 + 15\ 000 + 15\ 000 + 10\ 000 + 10\ 000 = 255\ 000 \text{ тис. грн.}$$

Для розрахунку машинного часу ми використаємо середню потужність серверу, яка складає 1,2 кВт і вартість електроенергії для приватних підприємств 1,67 грн.

$$Змч = 1{,}2*1{,}67 = 2 \text{ грн.} \qquad (3.4)$$

Вартість 1 години машинного часу ПК визначається за формулою:

$$C_{мч} = P \cdot t \cdot C_e + \frac{Ф_{зал} \cdot Н_а}{F_р} + \frac{К_{лпз} \cdot Н_{апз}}{F_р}, \text{ грн/год,} \qquad (3.5)$$

де Р – встановлена потужність ПК, кВт;

$С_е$ – тариф на електричну енергію, грн/кВт·година;

$Ф_{перв}$– первісна вартість ПК на початок року, грн.;

$Н_а$ – річна норма амортизації на ПК, частки одиниці;

$Н_{апз}$ – річна норма амортизації на ліцензійне програмне забезпечення, частки одиниці;

$К_{лпз}$ – вартість ліцензійного програмного забезпечення, грн.;

$F_р$ – річний фонд робочого часу (система повинна працювати постійно, тому $F_р = 8760$ год).

$$C_{\text{мч}} = 1.2 \cdot 1 \cdot 1.67_e + \frac{15000 \cdot 0.25}{8760} + \frac{8200 \cdot 0.25}{8760} = 2.66 \text{ грн./год}$$

Вартість електроенергії, що споживається апаратурою SOC протягом року ($С_е$), визначається за формулою:

$$С_е = С_{мч} \cdot F_р \text{ , грн,} \qquad (3.6)$$

$F_р$ – річний фонд робочого часу системи інформаційної безпеки (визначається виходячи з режиму роботи системи інформаційної безпеки, складає 8760);

$$С_е = 2{,}66*8760 = 23\ 336 \text{ грн.}$$

Загалом вартість розгортання SIEM становитиме:

$$В_{SIEM} = 119\ 200 + 255\ 000 + 23\ 336 = 397\ 536 \text{ грн.}$$

Перекваліфікацією персоналу займатиметься сторонння організація ПАТ «Security Solution».

Таблиця 3.5 – Вартість перекваліфікації персоналу

Минула посада	Цільова посада	Вартість перекваліфікації	Необхідна кількість, чол	Загальна вартість, грн
Аналітик ІБ	Керівник SOC	50 000	1	50 000
	Аналітик SOC	40 000	1	40 000
Інженер ІБ	Фахівець з моніторингу та реагування	10 000	4	40 000
Загальна сума ($В_{мо}$), грн				140 000

Загалом вартість розгортання SOC становитиме:

$$В_{SOC} = 397\,536 + 140\,000 = 537\,536 \text{ грн.}$$

3.3 Оцінка можливого збитку від атаки на вузол або сегмент корпоративної мережі

Для розрахунку вартості такого збитку можна застосувати наступну спрощену модель оцінки.

Необхідні вихідні дані для розрахунку:

$t_{п\ до}$ – час простою вузла або сегмента корпоративної мережі внаслідок атаки до впровадження SOC, годин, даний показник складає приблизно $t_п = 4$ години;

$t_{п\ після}$ – час простою вузла або сегмента корпоративної мережі внаслідок атаки після впровадження SOC, годин, даний показник складає приблизно $t_п = 1$ годину;

$t_{в\ до}$ – час відновлення після атаки персоналом, що обслуговує корпоративну мережу до впровадження SOC, годин, даний показник складає $t_в$ = 4 години;

$t_{в\ після}$ – час відновлення після атаки персоналом, що обслуговує корпоративну мережу після впровадження SOC, годин, даний показник складає $t_в$ = 1 годину;

$t_{ви}$ – час повторного введення загубленої інформації співробітниками атакованого вузла або сегмента корпоративної мережі до впровадження SOC, годин $t_{ви}$= 5 годин;

$t_{ви}$ – час повторного введення загубленої інформації співробітниками атакованого вузла або сегмента корпоративної мережі після впровадження SOC, годин $t_{ви}$= 1 годину;

$З_{о\ до}$ – місячна заробітна плата обслуговуючого персоналу (інженери ІБ) з нарахуванням єдиного соціального внеску, грн на місяць, складає 8000грн;

$З_{о\ після}$ – місячна заробітна плата обслуговуючого персоналу (фахівці з моніторингу та реагування) з нарахуванням єдиного соціального внеску, грн на місяць, складає 8000грн;

$З_с$ – місячна заробітна плата співробітника атакованого вузла або сегмента корпоративної мережі з нарахуванням єдиного соціального внеску, грн на місяць, складає 25000 грн;

$Ч_{о\ до}$ – чисельність обслуговуючого персоналу (інженери ІБ), осіб,

$Ч_{о\ після}$ = 8 осіб;

$Ч_{о\ після}$ – чисельність обслуговуючого персоналу (фахівці з моніторингу та реагування), осіб,

$Ч_{о\ після}$ = 4 особи;

$Ч_с$ – чисельність співробітників атакованого вузла або сегмента корпоративної мережі, осіб, $Ч_с$ = 20 осіб;

За вузол вважаємо команду розробників та тестувальників ПО, яка складається з 20 чоловік.

О – обсяг чистого прибутку/дохід від реалізації/ атакованого вузла або сегмента корпоративної мережі, грн у рік, або оподаткований прибуток атакованого вузла або сегмента корпоративної мережі, складає 1 000 000 грн.;

I – число атакованих вузлів або сегментів корпоративної мережі;

I=5

N – середнє число можливих атак на рік.

N=10

Упущена вигода від простою атакованого вузла або сегмента корпоративної мережі становить:

$$U = П_п + П_в + V, \qquad (3.7)$$

де $П_п$ – оплачувані втрати робочого часу та простої співробітників атакованого вузла або сегмента корпоративної мережі, грн;

$П_в$ – вартість відновлення працездатності вузла або сегмента корпоративної мережі (переустановлення системи, зміна конфігурації та ін.), грн;

V – втрати від зниження обсягу продажів за час простою атакованого вузла або сегмента корпоративної мережі, грн.

Втрати від зниження продуктивності співробітників атакованого вузла або сегмента корпоративної мережі являють собою втрати їхньої заробітної плати (оплата непродуктивної праці) за час простою внаслідок атаки:

$$П_{п\_до} = \frac{\sum З_с * Ч_с}{F} \cdot t_п \ , \qquad (3.8)$$

До впровадження SOC:

$$П_{п\_до} = \frac{25000 \cdot 20}{160} \cdot 4 = 15625 \quad \text{грн.}$$

Після впровадження SOC:

$$П_{п\_після} = \frac{25000 \cdot 20}{160} \cdot 1 = 3125 \quad \text{грн.}$$

де F – місячний фонд робочого часу (при 40-а годинному робочому тижні становить 160-176 ч).

Витрати на відновлення працездатності вузла або сегмента корпоративної мережі включають кілька складових:

$$П_в = П_{ви} + П_{пв} + П_{зч}, \qquad (3.9)$$

де $П_{ви}$ – витрати на повторне уведення інформації, грн;

$П_{пв}$ – витрати на відновлення вузла або сегмента корпоративної мережі, грн;

Витрати на повторне введення інформації $П_{ви}$ розраховуються виходячи з розміру заробітної плати співробітників атакованого вузла або сегмента корпоративної мережі $З_с$, які зайняті повторним введенням втраченої інформації, з урахуванням необхідного для цього часу $t_{ви}$:

$$П_{ви} = \frac{\sum З_с * Ч_с}{F} \cdot t_{ви} \quad . \qquad (3.10)$$

До впровадження SOC:

$$П_{ви\_до} = \frac{25000 \cdot 20}{160} \cdot 5 = 23437 \quad \text{грн.}$$

Після впровадження SOC:

$$П_{ви\_після} = \frac{25000 \cdot 20}{160} \cdot 1 = 3125 \quad \text{грн.}$$

Витрати на відновлення вузла або сегмента корпоративної мережі $П_{пв}$ визначаються часом відновлення після атаки $t_в$ і розміром середньогодинної заробітної плати обслуговуючого персоналу (адміністраторів):

$$П_{пв} = \frac{\sum З_о * Ч_о}{F} \cdot t_в \quad . \qquad (3.11)$$

До впровадження SOC:

$$П_{пв\_до} = \frac{8000 \cdot 8}{160} \cdot 4 = 1600 \quad \text{грн.}$$

Після впровадження SOC:

$$П_{пв\_після} = \frac{8000 \cdot 4}{160} \cdot 1 = 200 \quad \text{грн.}$$

Втрати від простою атакованого вузла або сегмента корпоративної мережі визначаються виходячи із середньо-годинного прибутку і сумарного часу простою атакованого вузла або сегмента корпоративної мережі:

$$V = \frac{O}{F_г} \cdot (t_п + t_в + t_{ви}) \quad , \qquad (3.12)$$

$$V_{до} = 1000000*(4+ 4+5) /1920 = 6\ 770 \text{ грн.}$$

$$V_{після} = 1000000*(1+ 1+1) /1920 = 1\ 562 \text{ грн.}$$

де $F_г$ – річний фонд часу роботи організації (52 робочих тижні, 5-ти денний робочий тиждень, 8-ми годинний робочий день)

До впровадження SOC:

$$U_{до} = 15625 + 23437 + 6\ 770 = 45\ 832 \text{ грн.}$$

Після впровадження SOC:

$$U_{після} = 3125 + 3125 + 1562 = 7\ 812 \text{ грн.}$$

Таким чином, загальний збиток від атаки на вузол або сегмент корпоративної мережі організації складе

$$B = \sum\sum U \cdot N \cdot I . \qquad (3.13)$$

До впровадження SOC:

$$В_{до} = 45\,832 \cdot 10 \cdot 5 = 2\,291\,600 \text{ грн.}$$

Після впровадження SOC:

$$В_{після} = 7\,812 \cdot 10 \cdot 5 = 390\,600 \text{ грн.}$$

3.4 Економічне обґрунтування впровадження центру оперативного управління кібербезпекою

Різницю від втрат до впровадження SOC на установі та після вирахуємо по формулі:

$$\Delta В = В_{до} - В_{після} \qquad (3.14)$$

$$\Delta В = 2\,291\,600 – 390\,600 = 1\,901\,000 \text{ грн.}$$

Вирахуємо термін протягом якого окупиться впровадження центру оперативного управління кібербезпекою за формулою:

$$T = \frac{Bsoc}{\Delta B} \qquad (3.15)$$

$$T = \frac{537\,536}{1901000} = 0{,}28 \text{ років.}$$

3.5 Висновки

В економічному розділі були розраховані витрати на впровадження SOC та можливі збитки від реалізації інцидентів. Було доведено, що впровадження запропонованого центру оперативного управління кібербезпекою окупиться протягом 4 місяців.

ВИСНОВКИ

Підчас виконання дипломної роботи проаналізовано моделі та архітектури центрів оперативного управління кібербезпекою та фактори які впливають на їх вибір. В результаті були розроблені рекомендації щодо вибору моделі та архітектури центру оперативного управління для підприємства.

Впровадження центру оперативного управління на підприємство дозволяє зменшити збитки пов’язані з реалізацією можливих загроз і вирішує такі питання І та КБ:

- Моніторинг стану ІБ:
- Моніторинг подій ІБ;
- Аудит дій користувачів;
- Управління уразливостями / контроль конфігурацій;
- Управління інцидентами ІБ;
- Контролю відповідності вимогам законодавства, міжнародних і галузевих стандартів, внутрішніх корпоративних політик.

Результати дослідження можуть бути застосовані на підприємствах під час побудови центрів оперативного управління кібербезпекою.

СПИСОК ЛІТЕРАТУРИ

1 What is a SOC (Security Operations Center) [Електронний ресурс]. – Режим доступу: http://securityaffairs.co/wordpress/47631/breaking-news/soc-security-operations-center.html – Загол. з екрану.

2 Security Information and Event Management [Електронний ресурс]. – Режим доступу: https://www.gartner.com/it-glossary/security-information-and-event-management-siem/ – Загол. з екрану.

3 S. David. A Practical Application of SIM/SEM/SIEM / Automating Threat Identification. SANS Institute, 2006. p.3. [Електронний ресурс]. – Режим доступу: https://www.sans.org/reading-room/whitepapers/logging/practical-application-sim-sem-siem-automating-threat-identification-1781.pdf

4 Types of Log Collection Methods (Електрон. ресурс)/Спосіб доступу: URL: https://support.symantec.com/en_US/article.INFO4456.html – Загол. з екрану.

5 SIEM – Security Information and Event Management [Електронний ресурс]. – Режим доступу: https://amica.ua/siem-security-information-and-event-management – Загол. з екрану.

6 CERT-UA [Електронний ресурс]. – Режим доступу: https://cert.gov.ua/– Загол. з екрану.

7 Міжнародний стандарт ISO/IEC 27001:2013 «Система управління інформаційною безпекою. Вимоги» [Електронний ресурс]. – Режим доступу: http://www.iso.org/iso/ru/catalogue_detail?csnumber=56742.;

8 Міжнародний стандарт ISO/IEC 27037:2012 «Інформаційні технології. Методи забезпечення безпеки. Настанови щодо ідентифікації, збору, придбання і збереження цифрових даних» [Електронний ресурс]. – Режим доступу: http://www.iso.org/iso/catalogue_detail?csnumber=44381.

9 COBIT - Цілі контролю за інформаційними та суміжними технологіями, 2012 р.;

10 Kearney, K.T.; Torelli, F. (2011). "The SLA Model". [text] / Wieder, P.; Butler, J.M.; Theilmann, W.; Yahyapour, R. Service Level Agreements for Cloud Computing. Springer Science+Business Media, 2011. – pp. 43–68.

11 Configuring SNMP and using the NetFlow [Електронний ресурс]. – Режим доступу: https://www.cisco.com/c/en/us/td/docs/ios-xml/ios/netflow/configuration/12-4t/nf-12-4t-book/cfg-snmp-mib-mon-nf.html

12 ДСТУ 2226-93 Автоматизовані системи. Терміни та визначення. [Електронний ресурс]. – Режим доступу: http://online.budstandart.com/ru/catalog/doc-page?id_doc=61937

13 Міжнародний стандарт ISO/IEC 27005:2011 «Інформаційна технологія. Методи і засоби забезпечення безпеки. Менеджмент ризику інформаційної безпеки» [Електронний ресурс]. – Режим доступу: http://www.iso.org/iso/ru/catalogue_detail?csnumber=56742.

14 Nadel, Barbara A. Building Security: Handbook for Architectural Planning and Design/ McGraw-Hill,2011. – p. 2;

15 HPE ArcSight Marketplace [Електронний ресурс]. – Режим доступу: https://marketplace.microfocus.com/arcsight– Загол. з екрану

16 IBM Security App Exchange Marketplace [Електронний ресурс]. – Режим доступу: https://exchange.xforce.ibmcloud.com/hub – Загол. з екрану

17 Use Cases LogRhythm [Електронний ресурс]. – Режим доступу: https://logrhythm.com/tags/use-cases/– Загол. з екрану

18 Splunk [Електронний ресурс]. – Режим доступу: https://splunkbase.splunk.com/ – Загол. з екрану

19 Корреляция SIEM [Електронний ресурс]. – Режим доступу: https://www.securitylab.ru/analytics/431459.phphttps://www.securitylab.ru/analytics/431459.php – Загол. з екрану

20 Інтернет-магазин «Розетка.УА» [Електронний ресурс] – Режим доступу: http://soft.rozetka.com.ua.

ДОДАТОК А. Перелік матеріалів дипломної роботи

1 Титульна сторінка.doc

2 Завдання.doc

3 Реферат.doc

4 Список умовних скорочень.doc

5 Зміст.doc

6 Вступ.doc

7 Розділ 1.doc

8 Розділ 2.doc

9 Розділ 3.doc

10 Висновки.doc

11 Список використаної літератури.doc

12 Додаток А.doc

13 Додаток Б.doc

14 Додаток В.doc

Презентація.pptx

ДОДАТОК Б. Відгуки керівників розділів

Б.1 Відгук керівника економічного розділу

Керівник розділу _____ _____

(підпис) (ініціали, прізвище)

ДОДАТОК В

Відзив

на дипломну роботу магістра на тему:
“Підходи до створення центрів оперативного управління кібербезпекою на підприємствах”
студента групи 125м-16-1 Стародубця Олександра Васильовича

Дипломна робота за спеціальністю 125 – «Кібербезпека» студента Стародубця Олександра Васильовича надана у вигляді пояснювальної записки на ___ сторінок, додатками на ___ сторінок. Результати практичної реалізації надані на електронному носії.

Тема та зміст дипломної роботи повністю відповідає завданню для виконання дипломної роботи.

На сьогоднішній день дуже поширені випадки кібератак та порушення інформаційної безпеки. Тому обрана тема диплому є актуальною.

У спеціальній частині проаналізовані основні фактори які впливають на вибір рішення побудови різних моделей та характеристик центрів оперативного управління кібербезпекою. Розроблені рекомендації щодо вибору моделі, архітектури та побудови центру оперативного управління кібербезпекою для підприємства. Запропонований порядок розгортання такого центру.

У роботі проаналізовані моделі центрів оперативного управління кібербезпекою, надана їх порівняльна характеристика. Розглянуті основні складові, задачі, процеси та порядок їх розгортання.

В економічному розділі визначена величина капітальних витрат на впровадження центру оперативного управління кібербезпекою розрахований можливий збиток від кібератак, обгрунтована економічна ефективність впровадження центру.

Повнота і глибина вирішення завдань є достатньою.

Оформлення пояснювальної записки дипломної роботи виконано, в основному, у відповідність до чинних стандартів і нормативних вимог.

Практичне значення роботи полягає в рекомендаціях щодо вибору моделі центру оперативного управління кібербезпекою для підприємства.

До недоліків роботи можна віднести деякі неточності в оформленні пояснювальної записки.

В цілому дипломна робота виконана у відповідності з вимогами, які були представленні до дипломних робіт магістрів, заслуговує оцінки «відмінно», а студент Стародубець Олександр Васильович заслуговує на присвоєння кваліфікації професіонала з організації інформаційної безпеки.

Керівник дипломної роботи,
д.ф.-м.н., проф. Т.С. Кагадій

Керівник спец. част.,
ст. викл. Д.С. Тимофеєв