МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
НАЦІОНАЛЬНИЙ АВІАЦІЙНИЙ УНІВЕРСИТЕТ
КАФЕДРА КОМП'ЮТЕРИЗОВАНИХ СИСТЕМ ЗАХИСТУ ІНФОРМАЦІЇ

ДОПУСТИТИ ДО ЗАХИСТУ
Завідувач кафедри Комп'ютеризованих систем захисту інформації

_____ Михайло СТЕПАНОВ
«____»_____ 2023 р.

На правах рукопису
УДК
004.056:056.53(079.2)

КВАЛІФІКАЦІЙНА РОБОТА

ЗДОБУВАЧА ВИЩОЇ ОСВІТИ

ОСВІТНЬОГО СТУПЕНЯ «МАГІСТР»

Тема: Удосконалені засоби захисту інформації в політиці безпеки банку

Виконавець: Мирослав БУЯР

Керівник: к.т.н., доцент Андрій ПЕТРЕНКО

Консультант розділу «Охорона навколишнього середовища»: к.т.н., доцент Тетяна ДМИТРУХА

Нормоконтролер: к.т.н., доцент Андрій ПЕТРЕНКО

Київ 2023

НАЦІОНАЛЬНИЙ АВІАЦІЙНИЙ УНІВЕРСИТЕТ

Факультет: Кібербезпеки та програмної інженерії

Кафедра: Комп'ютеризованих систем захисту інформації

Освітній ступінь: Магістр

Спеціальність: 125 «Кібербезпека»

Освітньо-професійна програма: «Безпека інформаційних і комунікаційних систем»

ЗАТВЕРДЖУЮ
Завідувач кафедри Комп'ютеризованих систем захисту інформації

_____ Михайло СТЕПАНОВ
«___» _____ 2023 р.

ЗАВДАННЯ
на виконання кваліфікаційної роботи
здобувача вищої освіти Буяра Мирослава Петровича

1. Тема: Удосконалені засоби захисту інформації в політиці безпеки банку затверджена наказом ректора від «15» вересня 2023 № 1814/ст.
2. Термін виконання з 16.10.2023 р. по 31.12.2023 р.
3. Вихідні дані: проаналізувати існуючі методи кібератак,SIEM системи, вдосконалити SIEM систему та інтегруємо сервіс X-Force exchange через API Проведення експериментальної атаки для перевірки спрацювання SIEM системи .
4. Зміст пояснювальної записки: теоретичні аспекти кібератак на банк, захист інформації, вдосконалення SEIM системи та інтеграція сервісу X-Force exchange через API.

КАЛЕНДАРНИЙ ПЛАН

виконання кваліфікаційної роботи

№ з/п	Етапи виконання кваліфікаційної роботи	Термін виконання етапів	Примітка
1.	Уточнення постановки задачі	16.10.2023	*Виконано*
2.	Аналіз літературних джерел	18.10.2023	*Виконано*
3.	Обґрунтування вибору рішення	25.10.2023	*Виконано*
4.	Збір інформації	26.10.2023	*Виконано*
5.	Аналіз нормативно-правової бази, актуальні загрози та атаки в автоматизованих системах	1.11.2023	*Виконано*
6.	Аналіз управління інформаційною безпекою банку	5.11.2023	*Виконано*
7.	Вдосконалення SIEM системи та інтегрування x-force exchange за допомогою API	15.11.2023	*Виконано*
8.	Перевірка на антиплагіат	15.12.2023	*Виконано*
9.	Оформлення і друк пояснювальної записки	18.12.2023	*Виконано*
10.	Оформлення презентації	20.12.2023	*Виконано*
11.	Отримання рецензій	22.12.2023	*Виконано*

6. Консультанти з окремих розділів

Розділ	Консультант (посада, П.І.Б.)	Дата, підпис	
		Завдання видав	Завдання прийняв
Охорона навколишнього середовища	Дмитруха Т.І.		

7. Дата видачі завдання: «16» жовтня 2023 р.

Здобувач вищої освіти Мирослав БУЯР

(підпис, дата)

Керівник кваліфікаційної роботи Андрій ПЕТРЕНКО

(підпис, дата)

РЕФЕРАТ

Кваліфікаційна робота складається зі вступу, 4-х розділів, загальних висновків, списку використаних джерел. Загальним обсягом робота складає 73 сторінку, має 10 рисунків, 2 таблиці. Список використаних джерел містить 35 найменування і займає 3 сторінки.

Мета кваліфікаційної роботи полягає в удосконалені програмного засобу Siem системи за допомогою API

В кваліфікаційній роботі розглянуті проблеми та питання захисту від загроз, як зовнішніх, так і внутрішніх, для загальної інформаційної безпеки банків.

Розглянули нормативно –правову політику банку моделі загроз та порушників і провели аналіз загроз. Вдосконалили SIEM систему захисту інформації банку інтегрувавши X-Force exchange

Запропонована система може використовуватися у реальному часі та атматично обновлятися і захищати банківську систему від різних атак та вторгнень в реальному часі .

Ключові слова: політки безпеки, ISO, захист системи, підвищення загального рівня безпеки банку, вдосконалення SIEM системи

ЗМІСТ

ВСТУП

Актуальність. В сучасному світі питання кібербезпеки в банківській сфері стає дедалі більш актуальним і значущим. Збільшення обсягів та різноманітність кіберзагроз, а також швидкий розвиток інформаційних технологій вимагають від банків системного та ефективного захисту від кібератак.

У зв'язку з інтенсивним використанням онлайн-сервісів та цифрових технологій у фінансовому секторі, банки стають привабливою мішенню для кіберзлочинців. Здатність виявляти, запобігати та відновлювати наслідки кібератак стає критично важливою для забезпечення стабільності та довіри в банківському галузі.

Використання різноманітних заходів безпеки, розробка та впровадження політик і стандартів, а також постійне вдосконалення інфраструктури та процесів стають невід'ємною частиною стратегії банківської кібербезпеки. Такі заходи дозволяють забезпечити високий рівень захищеності банківської інформації та зберегти довіру клієнтів, що є ключовим чинником успіху в умовах сучасного цифрового середовища.

Мета кваліфікаційної роботи полягає в удосконаленні програмного засобу SIEM системи за допомогою API

Об’єкт дослідження: Управління подіями та інцидентами кібербезпеки банку

Предмет дослідження:Засоби захисту що використовуються в політиці безпеки банку

Галузь застосування. Дану методику можна примінити до SIEM систем задля вдосконалення захищеності банку

Новизна.Удосконалення SIEM системи за рахунок інтегрування сервісу e exchange, що дозволяє виявити невідомі атаки та невиявленні вразливості.

РОЗДІЛ 1. МЕТОДИ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ

1.1 Поняття кібербезпеки

Кібербезпека - це набір заходів і процесів, спрямованих на захист комп'ютерів, мереж, електронних систем і даних, а також забезпечення безпеки програмного забезпечення від потенційних кіберзагроз. У сучасну цифрову епоху це надзвичайно важливий аспект, оскільки він відіграє ключову роль у різних сферах нашого життя. Кібербезпека використовується різними підприємствами та організаціями для захисту від несанкціонованого доступу до баз даних та інших систем.

Тема безпеки постійно змінюється, оскільки постійно змінюються ризики безпеки та заходи безпеки. Важливо приділяти цьому достатньо уваги, адже наслідки кібератак можуть критично вплинути не лише на великі компанії, а й на всіх нас.[13]

1.2 Найпоширеніші недоліки у формуванні інформаційної безпеки в організаціях

Проблеми безпеки в цифровому просторі становлять серйозну загрозу для організацій, що може призвести до витоку (компрометації) даних, фінансових втрат і втрати клієнтів.

Давайте розглянемо найпоширеніші проблеми кібербезпеки, на думку експертів з кібербезпеки.

- Неакуальне оновлення наявного ПЗ.

Експерти звертають увагу на важливість моніторингу та оновлення програм в операційних системах, щоб запобігти використанню вразливостей. Кожне оновлення виявляє та усуває потенційні загрози, які можуть бути використані для атак. Відсутність актуальних оновлень у системі відкриває двері для використання вже відомих вразливостей.

- Відсутність політик корпоративної інформаційної безпеки.

Кожна компанія, неважливо який вона має розмір, повинна мати корпоративну політику безпеки та процедури для захисту даних співробітників. Наявність такої політики робить загальний процес побудови захисту даних логічнішим та простішим.

- Загроза зсередини компанії.

Робота зі своїми співробітниками вимагає обережності, оскільки вони можуть бути вразливою ланкою у вашій програмі кібербезпеки. Недостатня

інформація про безпеку може зробити співробітників джерелом загроз.

•Використання "слабких" паролів.

Використання слабких паролів і неефективна автентифікація є серйозною загрозою. Важливо встановити надійні паролі, які мають належну довжину, щоб бути менше схильними до перебору брутфорсом, та використовувати мультифакторну автентифікацію (2FA), щоб запобігти несанкціонованому доступу.

•Порушення конфіденційності даних через дистанційну роботу.

Зараз дистанційна робота є джерелом нових загроз, і для зменшення ризиків важливо, щоб працівники використовували безпечні засоби для встановлення захищенного з'єднання. Наприклад, використання VPN робить можливість отримання доступу до внутрішнії сервісів компанії юезпечнішим шляхом шифрування трафіку та розмежування доступу.

•Атаки програм-вимагачів(Ransomware).

Атаки програм-вимагачів є серйозною загрозою, оскільки зловмисники шифрують дані та вимагають грошових виплат за можливість дешифрування. Іноді, навідь після того, як гроші були переведені на рахунки зловмисників, розшифрування даних не було Плани готовності та реагування можуть допомогти уникнути серйозних наслідків.

•Можливість відовлення данихх після кібератаки.

Важливо мати ефективні плани аварійного відновлення, наприклад, наявність RAID - масивів або бекапів, щоб уникнути серйозних збитків у разі кіберінциденту. Інвестування в розробку, тестування та оновлення планів може значно полегшити відновлення даних після кібератаки.[9,12]

1.2 Захист і управління безпекою для систем автоматизації

Підприємства використовують низку різних способів для попередження отримання несанкціонованому фізичного доступу до критичних компонентів системи. Від стандартного входу в будівлю до захисту особливих зон, доступ до яких отримується виключно з використанням особистих карток-ключів. Індивідуальні послуги промислової безпеки включають комплексні процеси захисту даних та рекомендації. Вони знаїодяться в діапазоні від аналізу ризиків, впровадження відповідних заходів кіберзбезпеки до спостеріганням за наявністю актуальних оновлень ПЗ.

Одним із головних завдань забезпечення скоординованої комунікації є подальше забезпечення відповідного захисту систем, до яких легко можна отримати доступ. Окрім доступності, головна увага віддається захисту мереж,

які є автоматизованими від отримання несанкціонованого доступу до них.[7]

Системний захист поділяється на декілька частин, координація яких всередині організації має включове значення для успішної системи кібербезпеки.

Розділи мають наступне:

• безпека програмних рішень;

• безпека даних;

• безпека мережі;

•планування аварійного відновлення відмовостійкості роботи підприємства;

• безпека експлуатації;

• безпека хмарних рішень;

• робудова безпеки інфраструктури, яка носить критичний характер;

• фізична охорона;

• навчання співробітників компанії.

Безпека мережі полягає в захисті комп'ютерних мереж від зловмисників. І не має значення були ці атаки цілеспрямованими, чи масове шкідливе програмне забезпечення.

Метою безпеки програмних рішень є захист програмного забезпечення. Через зламану програму зловмисники можеть отримати доступ будь-куди.

Система інформаційної безпеки має захищати конфіденційність даних, їх цілісність та доступність на усіх етапах їх обробки. Починаючи від збереження цих даних у мережі компанії і закінчуючи передачею цих даних як у локальніх мережі, так і назовні.

Підвищення рівня обізнанності співробітників компанії щодо інформаційної безпеки направлене на найважливішу ланку у безпеці - людей. Без належних заходів безпеки будь-хто може випадково завантажити вірус у безпечну систему. Тренування користувачів у визначенні фішингових листів, процедурі, як потрібно діяти у цьому випадку, виикористання лише безпечний зовнішніх носіїв інформації та іншим уроками є вкрай необхідним для забезпечення загального рвіня безпеки кожної компанії.

1.3 Види атак на системи інформаційного захисту

Кібератаки - це різні види нападів або зловживань в цифровому просторі з метою завдання шкоди, отримання несанкціонованого доступу чи крадіжки конфіденційної інформації. Існує безліч різних видів кібератак, і їх розмаїття постійно зростає відповідно до технологічного розвитку. Ось деякі з найпоширеніших видів кібератак:

Фішинг**:**

•Соціальний фішинг: Атаки, спрямовані на отримання конфіденційної інформації, такої як паролі або особисті дані, шляхом використання маніпуляцій і соціальної інженерії.

•Підробка сайтів: Використання подібних до офіційних веб-сайтів або служб для викрадення авторизаційних даних.

Malware(шкідливе програмне забезпечення):

•Віруси: Програми, які можуть самореплікуватися та поширюватися на інші файли.

•Троянські коні: Шкідливі програми, які приховані під корисними, але фактично виконують зловмисні функції.

•Шпигунське програмне забезпечення: Засоби для незаконного збору інформації з комп'ютера чи користувача.

•Ransomware:

Тип малвари, який шифрує файли на комп'ютері користувача і вимагає викуп за їхнє відновлення. Наприклад, віруси WannaCry або NotPetya.

•Spyware:

Програмне забезпечення, яке приховано встановлюється на комп'ютері для збору конфіденційної інформації, такої як паролі, дані банківських карток або інша особиста інформація.

•Adware:

Програмне забезпечення, яке відображає рекламу на комп'ютері користувача, часто нав'язливу, з метою генерації прибутку для злоумисника.

•Trojan Horse (Trojan):

Програма, яка приховується як корисна, але насправді виконує шкідливі функції. Наприклад, програма, яка стверджує, що вона антивірус, але фактично викрадає особисті дані.

•Botnets:

Збірник комп'ютерів, які були заражені зловмисним кодом і використовуються для виконання команд зловмисника. Botnets можуть бути використані для виконання DDoS-атак, розсилання спаму чи витоку конфіденційної інформації.

•Keyloggers:

Програми, які ведуть журнал всіх натискань клавіш на комп'ютері, з метою вивчення паролів або іншої конфіденційної інформації.

•Worms:

Саморозповсюджувана малвара, яка може розповсюджуватися через мережу без участі користувача, інфікуючи інші комп'ютери.

•Rootkits:

Засоби, які намагаються приховати наявність шкідливої програми, змінюючи або приховуючи системні файли та процеси.

•Fileless Malware:

Malware, яка не залишає слідів на жорсткому диску і використовує інші методи, такі як використання резидентної пам'яті, щоб уникнути виявлення та блокування.

•Polymorphic Malware:

Малвара, яка може змінювати свій код або вигляд, ускладнюючи виявлення за допомогою сигнатур антивірусних програм.

DDoS-атаки (атаки на відмову в обслуговуванні):

•Переповнення каналу: Спроби заблокувати доступ до ресурсу, перевищивши його оброблювальну здатність.

•Синфлуд: Надмірне відправлення запитів для перевантаження системи.

DoS-атаки (відмова в обслуговуванні):

•Атаки на порти: Використання програм для перевантаження мережевих портів.

Атаки на веб-додатки:

•Перехоплення сесій: Зловживання або крадіжка ідентифікаторів сесій користувачів.

•Cross-Site Scripting (XSS):

Злоумисник вбудовує скрипти в веб-сайт, які виконуються на браузері користувача. Це може призвести до викрадення сесій, перенаправлення на інші сторінки або введення фальшивого вмісту.

•Cross-Site Request Forgery (CSRF):

Злоумисник використовує авторизований сеанс користувача для виконання несанкціонованих дій без його згоди. Це може включати зміну паролів, відправлення коментарів або виконання інших дій від імені

користувача.

•SQL Injection:

Злоумисник вводить SQL-код у вхідні поля веб-сайту з метою викликання змін у базі даних. Це може призвести до витоку чутливої інформації або знищення даних.

•Security Misconfigurations:

Злоумисники використовують вразливості в налаштуваннях безпеки, які можуть включати в себе неправильні налаштування прав доступу, виток інформації чи використання застарілих версій програмного забезпечення.

•File Upload Vulnerabilities:

Злоумисники завантажують шкідливі файли через механізми завантаження файлів на веб-сайті, намагаючись використати це для виконання коду або розповсюдження шкідливого програмного забезпечення.

•XML External Entity (XXE) Attacks:

Злоумисники використовують слабкості у обробці XML-даних для виклику змін у системі чи отримання конфіденційної інформації.

•Server-Side Request Forgery (SSRF):

Злоумисники викликають сервер для виконання запитів на віддалені сервери з метою отримання конфіденційної інформації або виконання несанкціонованих дій.

•Remote Code Execution (RCE):

Злоумисники викликають виконання віддаленого коду на сервері, що може призвести до незаконного доступу, зміни конфігурацій або витоку даних.

Атаки на безпеку мережі:

•Man-in-the-Middle (MitM) Attack:

Злоумисник встає між двома взаємодіючими сторонами і перехоплює або маніпулює передачею даних між ними. Це може включати атаки, такі як атака ARP-отрути, DNS-отрути, або використання відомостей про віддалену ідентифікацію (Remote Identity Spoofing).

•Packet Sniffing:

Злоумисник використовує програми для перехоплення та аналізування мережевого трафіку, що може призвести до витоку конфіденційної інформації, такої як паролі або дані користувачів.

•DNS Spoofing (DNS Cache Poisoning):

Злоумисник намагається вводити хибні записи в кеш DNS, перенаправляючи користувачів на фейкові веб-сайти або інші небезпечні домени.

•Session Hijacking:

Злоумисник викрадає сесійні ідентифікатори користувача для несанкціонованого доступу до облікових записів. Це може включати атаки на безпеку сесій (Session Fixation) або перехоплення сесійних файлів cookie.

•Eavesdropping (Packet Sniffing):

Незаконне прослуховування мережевого трафіку для перехоплення конфіденційної інформації.

•Brute Force Attack:

Злоумисник намагається отримати доступ до системи шляхом послідовного спробування всіх можливих паролів чи ідентифікаторів до вдалого зламу.

•Zero-Day Exploit:

Використання вразливостей у програмному забезпеченні або операційних системах, які не мають виправлення або відомі виробником, для отримання несанкціонованого доступу.

•Port Scanning:

Злоумисник сканує мережеві порти системи з метою виявлення вразливостей або служб, які можуть бути атаковані.

•Smurf Attack:

Атака на мережевий пристрій, при якій велика кількість ICMP Echo Request повідомлень (ping) надсилаються широкомовно, переповнюючи і витрачаючи ресурси системи.

Соціальна інженерія:

•Маніпуляція користувачів: Використання психологічних та соціальних технік для залучення користувачів до зловмисних дій.

•Фізичний доступ: Зловмисники можуть використовувати соціальну інженерію, щоб отримати фізичний доступ до комп'ютерних систем, отримати паролі або інші конфіденційні дані.

Атаки на інтернет-протоколи:

•DNS-атаки: Маніпуляція DNS-запитів для перенаправлення трафіку або зловживання ідентифікацією домену.

•BGP-атаки: Маніпуляція маршрутами для перенаправлення трафіку через зловмисний вузол.

•ARP-отрута (ARP Poisoning):

Ця атака полягає в тому, що зловмисник відправляє фальшиві ARP-відповіді для того, щоб перенаправити мережевий трафік через свій власний комп'ютер. Це може призвести до перехоплення і аналізу пакетів або подальшої маніпуляції трафіком.

•DNS-серверне отруєння (DNS Spoofing):

Атака, при якій зловмисник вносить зміни в DNS-відповіді для перенаправлення користувачів на фейкові веб-сайти або інші неправомірні домени.

•ICMP-атаки (Ping of Death):

Здійснюється надсилання великої кількості ICMP-пакетів або створення особливого ICMP-пакета, який перевищує допустимий розмір. Це може викликати перевантаження та відмову в обслуговуванні віддаленого комп'ютера.

•IP-серверне отруєння (IP Spoofing):

Зловмисник намагається відправляти пакети, приховуючи свій справжній IP-адресу за адресою іншого джерела. Це може бути використано для обходу систем фільтрації та отримання несанкціонованого доступу.

•Синтаксичні атаки на SMTP (SMTP Injection):

Зловмисник вбудовує команди або зловживає синтаксисом Simple Mail Transfer Protocol (SMTP) для внесення змін у електронних листах або викликання інших проблем у системі обробки електронної пошти.

•Використання слабкостей BGP (BGP Hijacking):

Атака, при якій зловмисник маніпулює інформацією маршрутизації BGP, щоб перенаправити мережевий трафік через свій контрольований вузол, дозволяючи перехоплення чи зміну даних.

•SNMP-атаки (Simple Network Management Protocol):

Зловмисники можуть використовувати SNMP для отримання доступу до інформації про мережеві пристрої або вносити зміни у конфігурації пристроїв, якщо вони не налаштовані належним чином.

•Сміттєвий трафік (Traffic Interception):

Атака, при якій зловмисник перехоплює та аналізує мережевий трафік між двома точками для отримання конфіденційної інформації або виявлення вразливостей у системах.

Найвідоміші шкілдиві програми типу "Троян".

Троянські коні (Trojan Horses або трояни) - це вид шкідливого програмного забезпечення, яке приховується під корисним або легітимним зовнішнім виглядом, але насправді має зловмисний вміст. Названі на честь античного міфу про Троянського кінного шахрая, ці програми дозволяють

зловмисникам отримувати несанкціонований доступ до комп'ютера чи інших пристроїв, викрадати конфіденційні дані, запускати атаки або виконувати інші шкідливі дії. Ось декілька найвідоміших троянських коней:

Zeus (Zbot):

Відомий також як Zbot, цей троянець був спроектований для крадіжки фінансової інформації, зокрема, банківських облікових записів та паролів. Зловмисники використовують Zeus для створення ботнетів і ведення атак на банківські та фінансові установи.

SpyEye:

Схожий на Zeus, SpyEye також спрямований на крадіжку фінансової інформації. Він включає в себе деякі функції, які дозволяють зловмисникам віддалено контролювати заражені системи та виконувати різноманітні атаки.

Emotet:

Спочатку використовувався для вивчення чутливої інформації, такої як логіни та паролі, Emotet став більш загальною загрозою, розповсюджуючи інші види малвари. Він може використовуватися для створення ботнетів та ведення різноманітних атак.

CryptoLocker:

Цей троянець входить до категорії розширюючої шкідливої програми. Він шифрує файли на жорсткому диску користувача, а зловмисники вимагають викуп за розшифрування файлів. Це один із видів вірусів-викупників.

Banker Trojan (Banload):

Зорієнтований на фінансовий сектор, цей троянець спроектований для крадіжки фінансової інформації, зокрема, банківських даних та інших фінансових реквізитів.

DarkTequila:

Орієнтований на користувачів в Латинській Америці, DarkTequila використовує соціальний інженеринг і спрямований на крадіжку банківської інформації, особистих даних та інших конфіденційних відомостей.

RAT (Remote Access Trojan):

Рат-троянці призначені для забезпечення віддаленого доступу до заражених систем, дозволяючи зловмисникам виконувати різноманітні дії, включаючи крадіжку інформації, встановлення інших шкідливих програм і ведення рейдерських атак.

Dridex:

Відомий також як Cridex або Bugat, Dridex використовується для крадіжки банківської інформації, включаючи логіни та паролі. Він може розповсюджуватися через електронну пошту та експлойти.

Найвідоміші кібератаки:

Є багато визначних кібератак, які відбулися в різний час. Нижче представлено огляд деяких найвідоміших кібератак:

- Stuxnet (2010):

Став однією з перших відомих кібератак на об'єкти критичної інфраструктури. Вірус Stuxnet призначений для атаки систем керування промисловими об'єктами, зокрема, ядерними установками в Ірані.

•Sony Pictures Hack (2014):

Злом систем Sony Pictures спричинив витік конфіденційної інформації, включаючи електронну пошту, фільми та інші документи. Атаку було пов'язано з невідомою групою, яка протестувала проти випуску фільму "The Interview".

•WannaCry (2017):

Розповсюджувався за допомогою вразливостей у операційних системах Windows, WannaCry був розроблений для шифрування файлів на комп'ютерах та вимагав викуп для їхнього відновлення. Атака поширилася глобально та зачепила тисячі організацій, включаючи багатонаціональні корпорації та органи влади.

•NotPetya (2017):

Вважається однією з найбільш руйнівних кібератак у світі, NotPetya використовував вразливості в Україні, але швидко поширився глобально, зачепивши тисячі компаній та організацій. Багато експертів вважають, що за атакою стояла держава.

•Equifax Data Breach (2017):

Кібератака на американську компанію Equifax призвела до витоку особистих даних більше 147 мільйонів людей. Зловмисники використали вразливість в програмному забезпеченні Apache Struts для отримання доступу до сховища інформації.

•SolarWinds Cyberattack (2020):

Ця атака вплинула на понад 18 000 клієнтів популярної платформи SolarWinds. Зловмисники внедрили злоумисне програмне забезпечення в оновлення програми, що призвело до доступу до конфіденційної інформації великих корпорацій та установ.

•Colonial Pipeline Ransomware Attack (2021):

Розраховуючи на розбещення транспортної системи США, хакери використали атаку вірусів-викупників на Colonial Pipeline. Атака призвела до призупинення роботи магістрального трубопроводу для перевезення пального, що викликало проблеми з постачанням палива в південних штатах США.

Ці атаки відображають різні аспекти кіберзагроз та показують, наскільки важливо захищати інформацію та критичну інфраструктуру від кібератак. Компанії та організації в усьому світі вдосконалюють свої заходи кіберзахисту, щоб запобігти подібним інцидентам у майбутньому.[16,17,19,26]

1.5 Управління ризиками в кіберпросторі та засоби кіберзахисту.

Кібербезпека, безперечно, стоїть перед постійними викликами, зокрема від хакерів, що завдають втрати даних, порушують конфіденційність і вимушують перегляд стратегій управління кібербезпекою. Прогнози, які передбачають збільшення числа кібератак у найближчому майбутньому, залишаються дуже актуальними. Варто враховувати, що з появою нових технологій, таких як Інтернет речей (IoT), розширюється поверхня для потенційних атак, підкреслюючи необхідність посилення захисту мереж та пристроїв.

Один із ключових викликів у сфері кібербезпеки - це постійна зміна ризиків безпеки. Нові технології та їх різноманітне використання ведуть до розробки нових методів атак. Слід постійно відслідковувати ці зміни та адаптувати заходи захисту, але це може бути непросто, особливо для малих організацій з обмеженими ресурсами.

Зазначу, що навчання кінцевих користувачів - важлива складова програм кібербезпеки. Застосування навчання допомагає співробітникам стати більш відповідальними та активними у захисті від кіберзагроз. Важливо також враховувати чинники, що впливають на навчання, такі як регулярність та доступність, для максимальної ефективності.

Управління кіберризиками - це процес, який вимагає уваги до деталей і систематичного підходу. Визначення ризиків навколо бізнес-активів і процесів важливе для ефективного вирішення проблем. Однак варто також враховувати, що аналіз ризиків, заснований на фактах, може допомогти визначити пріоритети інвестицій в безпеку та адаптувати заходи захисту до реальних загроз.

І найголовніше - в умовах постійної еволюції кіберзагроз і технологій, зберігайте актуальність і готовність до швидкої реакції на зміни. Використовуйте аналіз ризиків, щоб забезпечити реальний захист і зберігайте свої системи безпеки високими якостями.[24]

1.6 Чому варто розвивати кібербезпеку в банках

Розвиток кібербезпеки в банках має велике значення з огляду на постійне зростання кількості та складності кіберзагроз. Банки здійснюють обробку величезного обсягу конфіденційної інформації, такої як особисті дані клієнтів та фінансові транзакції.

Забезпечення кібербезпеки є необхідністю для ефективного функціонування банківських систем та збереження довіри клієнтів. Кібератаки можуть призвести до витоку конфіденційної інформації, фінансових втрат та порушень репутації, що негативно впливає на бізнес та відносини з громадськістю.

Розвиток ефективної системи кіберзахисту дозволяє банкам уникнути суттєвих фінансових втрат, забезпечити безпеку клієнтів та підтримувати стабільність в сучасному цифровому середовищі. Також це сприяє виконанню законодавчих вимог щодо захисту конфіденційної інформації та підвищенню рівня впевненості в технологічній безпеці в цілому.

Додатково, розвиток кібербезпеки в банках дозволяє:

1. Захистити Клієнтські Ресурси: Забезпечення безпеки інформаційних ресурсів клієнтів є важливою частиною діяльності банку. Клієнти віддають перевагу банкам, які забезпечують надійний захист їхніх фінансових та особистих даних.

2. Збереження Репутації: Кіберінциденти можуть суттєво вплинути на репутацію банку. Розвиток кібербезпеки допомагає уникнути ситуацій, коли виток чи порушення безпеки може призвести до втрати довіри клієнтів та інвесторів.

3. Виконання Регуляторних Вимог: Банки повинні відповідати високим стандартам безпеки, встановленим регуляторами. Розвиток системи кібербезпеки дозволяє банкам ефективно виконувати регуляторні вимоги та уникати штрафів за порушення правил.

4. Запобігання Фінансовим Збиткам: Кібератаки можуть призвести до серйозних фінансових втрат. Заходи кібербезпеки направлені на зменшення ризиків та швидке виявлення та врегулювання інцидентів.

5. Створення Устійкої Системи: Забезпечення устійкості та швидкого відновлення після кіберінцидентів є ключовим елементом ефективної кібербезпеки. Це дозволяє банку мінімізувати час простою та негативний вплив на клієнтів.

Таким чином, інвестиції в розвиток кібербезпеки є стратегічно важливими для забезпечення стабільності та успішності банку в умовах сучасного цифрового середовища.

1.7 Міжнародні аспекти

Міжнародні аспекти захисту інформації в банках включають у себе вивчення та впровадження міжнародних стандартів і практик, спрямованих на забезпечення найвищого рівня безпеки в галузі фінансів. Банки співпрацюють на міжнародному рівні з метою обміну досвідом та інформацією з іншими установами, враховуючи транскордонні аспекти кібербезпеки. Створення єдиних стандартів та взаємодія в цьому напрямку допомагають банкам ефективно протистояти глобальним кіберзагрозам та узгоджувати свої підходи до захисту інформації на міжнародному рівні.

Додатково, міжнародні аспекти включають участь банків у міжнародних ініціативах та організаціях, спрямованих на зміцнення кібербезпеки в

фінансовому секторі. Банки можуть брати участь у спільних проектах і програмах, спрямованих на виявлення та протидію новим кіберзагрозам.

Деякі міжнародні аспекти включають розробку стандартів для захисту глобальних фінансових операцій, встановлення механізмів обміну інформацією та практиками взаємодії для негайного реагування на інциденти. Забезпечення взаємодії та співпраці між різними країнами та банками важливо для створення єдиної міжнародної системи захисту інформації, яка могла б високоефективно протистояти кіберзагрозам у фінансовому секторі.

1.8 Правові аспекти

В контексті захисту інформації в банку правові аспекти грають важливу роль у забезпеченні конфіденційності та цілісності даних. Основні аспекти включають:

- Законодавче регулювання:

Визначення та вивчення основних законів та нормативно-правових актів, що визначають порядок збереження, обробки та передачі банківської інформації. Зокрема, це може стосуватися законодавства про конфіденційність, захист персональних даних, кібербезпеку тощо.

- Комерційна таємниця:

Дослідження правового регулювання в сфері комерційної таємниці, яке визначає, які дані банку вважаються конфіденційною інформацією, а також як вони повинні бути захищені.

- Ліцензії та сертифікація:

Розгляд вимог до ліцензування та сертифікації в галузі банківської діяльності та інформаційної безпеки.

- Відповідальність та кримінальні санкції:

Вивчення правової відповідальності за порушення заходів безпеки інформації в банку, включаючи штрафи, судові справи та кримінальні переслідування.

- Правила та стандарти:

Аналіз правил і стандартів, рекомендованих та обов'язкових для банківського сектора щодо захисту інформації.

- Внутрішні політики та процедури:

Розгляд правил та політик, які встановлюються самим банком для забезпечення внутрішньої безпеки та відповідності законодавству.

Взаємодія з цими правовими аспектами дозволяє банку створити ефективну систему захисту інформації, яка відповідає сучасним стандартам та вимогам.

1.9 Висновок до розділу

В першому розділі ми розглянули основні недоліки у формуванні безпеки банку також захист і управління безпекою. Зясували що в наш час дуже багато банків попадають під еібер атаку і без висого рівня пз і кваліфікованих співробітників банк втратить всю інформацію і своїх клієнтів

Вияснили роль нормативно-правових аспектів банку, що визначають порядок збереження, обробки та передачі банківської інформації. Міжнародних стандартів і практик, спрямованих на забезпечення найвищого рівня безпеки в галузі фінансів.

РОЗДІЛ 2. Аналіз політик та методик інформаційної безпеки.

2.1 Сфера регулювання Інформаційної безпекив в банку

Нормативна сфера процесів інформаційної безпеки охоплює всі сфери діяльності Банку та враховується в рамках заходів, спрямованих на захист інформації, систем і мереж. Забезпечення безпеки та інформаційної безпеки є ключовою передумовою для досягнення очікуваної ефективності бізнесу, сталого розвитку та стійкості до зовнішніх і внутрішніх загроз інформаційній безпеці. Інформаційна безпека є невід'ємною частиною діяльності банку та охоплює всіх співробітників, технології, інфраструктуру, продукти та процеси. Політика інформаційної безпеки банку регламентує функціонування системи управління інформаційною безпекою відповідно до законодавства України з урахуванням вимог міжнародних і вітчизняних платіжних систем і систем переказу грошей, а також нормативних документів.

Сфери регулювання:

1. Законодавство:

- кіберзахист: закони спрямовані на захист інформації та забезпечення безпеки в мережі
- Кіберкримінал: законодавство, що стосується криминільних правопорушень

2.Міжнародні стандарти:

- ISO 270001: стандарт для систем управління інформаційною безпекою
- NIST cybersecurity framework: фрейморк розроблений інтститутом стандартів і технологій США

3. Національні стратегії:

Кібербезпека країни: сукупність заходів та стратегій , спрямованих на захист кіберпростору держави

4. Аудит та ревізія:

- Внутрішній аудит проведення внутрішніх аудитів з метою перевірки ефективності захоідв інформаційної безпеки
- Зовнішній – залучання зовнішніх аудиторів для оцінювання системи інформаційної безпеки

2.2 Система захисту та їх групи

Банк – це інформаційний об’єкт, що містить комплекс взаємопов’язаних компонентів, єдиним призначенням яких є обмін інформацією та захист за допомогою структурних зв’язків і технологій. У процесі роботи ці компоненти можуть змінюватися і піддаватися впливу різних зовнішніх і внутрішніх факторів. Основні з цих компонентів можна поділити на такі групи

1. Співробітники
2. Документація
3. ПЗ – сукупність програм та даних
4. Технічні засоби

Ці фактори взаємодіють один з одним, сприяючи інформаційній безпеці банку. Забезпечення інформаційної безпеки та її складових, таких як захист інформації, неможливо досягти лише організаційними, технічними, програмними чи криптографічними заходами. Заходи інформаційної безпеки мають бути системним процесом, заснованим на комплексному застосуванні всіх заходів та засобів безпеки в усіх сферах діяльності банку. Водночас ресурси, заходи та методи безпеки мають бути об’єднані в єдиний комплексний механізм, який захищає не лише від зловмисників, а й від некомпетентних, недобросовісних банківських працівників та непередбачених ситуацій. Іншими словами, забезпечення інформаційної безпеки, включаючи всі її складові, має бути системним і комплексним.

Системність заходів інформаційної безпеки має передбачати таке:

- найвищий рівень захищеності
- діяльність банкупо забезпеченню функціоналу повинна працювати безперервно
- Забезпечення інформаційної безпеки взаємодіє з поточною діяльністю банку в єдиному комплексі.

Системний підхід гарантує оптимізацію заходів та інструментів, що використовуються в системі, з метою досягнення балансу між вимогами та можливостями, необхідними для забезпечення безпеки банківської інформації. Такий комплексний підхід зумовлений тим, що загрози банківській інформації є багатоаспектними, а їх взаємодія потребує застосування різних заходів та інструментів. Врахування значної різноманітності банківських операцій, широке географічне розміщення банківських установ, а також

специфіка поведінки банківських службовців і клієнтів визначають специфіку функціонування банківських систем безпеки. Тому для ефективної відповіді на ці виклики необхідна злагоджена дія всіх ресурсів та інструментів, що можливо досягти лише системним підходом.

Крім того, в сучасних умовах безпека повинна реалізовуватися на технологічному та логічному рівні, який має враховувати всі фактори та характеристики, що впливають на захист інформації банківського сектору, а також усі етапи інформаційної діяльності: збір. , обробка, зберігання, передача та використання. За таких умов системність і комплексність забезпечення банківської безпеки, особливо у сфері захисту інформації, стає необхідною умовою високої ефективності.

Система захисту інформації банку - це організована сукупність об'єктів і суб'єктів захисту інформації, заходів, методів і засобів, що обслуговують безпеку. Основне призначення системи – гарантувати надійність зберігання та використання банківської інформації.

Враховуючи систему захисту інформації банку та необхідність її невизначеного функціонування, побудова такої системи має бути спроектована на відповідних принципах.

Принципу захисту інформації визначається до рівня захисту інформації,. Чим вищий рівень захисту тим краще захищена система від різних кібератак і тим самим більш надійна.

Вирішальну роль у забезпеченні інформаційної безпеки відіграє політика банку. Набір прийнятих правил, рекомендацій і стандартів, на основі яких створюється та керується система безпеки. Реалізація політики здійснюється за допомогою організаційних і програмно-технічних заходів, що визначають архітектуру системи захисту та засоби управління механізмами захисту.

Принцип повної участі та персональної відповідальності забезпечує розподіл відповідальності за захист інформації між усіма особами, які працюють з інформаційними продуктами банку (програмами, документами, функціями тощо), і вимагає, щоб усі працівники банку або інші особи брали відповідальність за дотримання. інформація про заходи безпеки

Принцип заделегіть підготовлених заходів передбачає планування та впровадження правил заходів безпеки задля забезпечення захисту інформації

Банки не захищають відкриту інформацію. Захист інформації здійснюється через облік і контроль доступу. Треба регулювати доступ до інформації.

Заходи інформаційної безпеки сприяють збереженню конфіденційності інформації третіх осіб і реалізуються за допомогою технічних, програмних і юридичних засобів.

Технічні заходи включають засоби кодування та засоби контролю доступу до інформації. Програмне забезпечення використовується для

контролю та обмеження доступу до інформації в банківській системі. Пізніше програмне забезпечення можна використовувати для визначення того, хто намагався відкрити або запустити певний файл у системі.

Відповідні положення про захист інформації та комерційної таємниці знаходяться встатуті банку. Статут банку включає в себе:

- Створювати спеціальних підрозділів для системи захисту та таємниці банку
- Відшкодування збитків та заист конфіденційної інформації
- Юридичне право на захист інформації
- Видання нормативнтх документів

Нормативним документом банку, що регулює захист інформації, є рішення про комерційну таємницю та конфіденційну інформацію. У цьому документі перераховані дані, що стосуються комерційної таємниці та конфіденційної інформації банку. Вони також визначають обов'язки співробітників щодо систем захисту інформації та визначають відповідальність за порушення правил.

Рішення визначає порядок захисту інформації та організації роботи з конфіденційною інформацією в банку.

. Постанова передбачає такі пункти як :

1.Обовязки посадових осіб та службовців банку щодо роботи

2. Право на співробітників банку на інформацію з обмеженим доступом

3. Порядок зберігання передачі та переміщення документів у установах банку

Нормативно-правова база банку зобов'язує співробітників зберігати таємницю, укладені домовленності з клієнтами в умовах конфіденційної інформації.

Створення нормативно-правової бази, є основою правового захисту його інтересів і діяльності.

Нормативні акти банку - це офіційні документи, які визначають правила та внутрішні процедури функціонування банку, його взаємодію з клієнтами, персоналом, а також зовнішніми сторонами. Ці акти є частиною нормативно-правового фреймворку, який регулює діяльність банку та гарантує відповідність його операцій вимогам законодавства.

До типових нормативних актів банку можуть входити:

1.Положення про організацію та функціонування банку: Цей документ може визначати структуру банку, повноваження внутрішніх підрозділів, порядок прийняття рішень тощо.

2.Правила надання банківських послуг: Описують умови та процедури, за якими банк надає свої послуги клієнтам.

3.Стандарти безпеки інформації: Визначають заходи та процедури для захисту конфіденційної інформації банку.

4.Положення про внутрішній аудит: Регулюють процес контролю та аудиту внутрішніх операцій та процедур банку.

5.Етичний кодекс: Встановлює стандарти етичної поведінки для співробітників та інших зацікавлених сторін.

6.Положення про взаємодію з регулюючими органами: Визначає правила та обов'язки банку у відносинах з регулюючими органами та наглядовими установами.

Ці акти можуть змінюватися та доповнюватися в залежності від змін у законодавстві, внутрішніх потреб банку та еволюції фінансового ринку.

У банкусуб'єктом захисту інформації є працівники, про яких може бути зібрана значна кількість інформації, особливо цінової. Банківські працівники відрізняються своїми позитивними і негативними якостями, які впливають на їх захист. Позитивно, що без історичної інформації банк не може залишитися в пам'яті співробітників з жодного питання, він може об'єктивно оцінити сучасну значимість цієї інформації і повернутися назад. Вони можуть скористатися перевагами інформації для споживачів, знаючи, кому і якій інформації можна довіряти.

Мінус у тому, що колеги можуть загубитися серед більшості таких користувачів, не будучи компетентними у актуальній значущості цієї інформації, їхні дії багато в чому залежать від їхнього емоційного стану, характеру та особистих потреб. У таких умовах системи захисту інформації для такого об'єкта захисту, як працівники банку, необхідно реалізувати заходи щодо регламентації роботи роботів-співробітників інформацією, створити відповідальні обмеження та захисту, що мотивують поведінку певним чином. працівники дотримання правил. Створено систему захисту інформації для організації роботи співробітників з інформацією про розвиток банку за допомогою:

1. установлення порядку
2. правила зберігання інформації
3. правила переселиння електронних і паперових документів
4. визначення осіб якімають доступ до всієї інформації як знаходиться в банку
5. розподілення конфіденційної інформації тільки яку потребує співробітник для виконання своїх обовязків

Основними методами є: банківське виховання патріотизму серед співробітників; належне ставлення до колективу, фінансові та професійні вигоди.

Важливе значення мають заходи, спрямовані на запобігання впливу осіб, зацікавлених у отриманні банківської інформації, оскільки безпека інформації в банківському секторі є ключовою для захисту клієнтських даних, фінансових операцій та репутації банку. Нижче подано ключові аспекти та принципи, які підкреслюють важливість заходів щодо захисту банківської інформації від небажаних впливів:

1. Конфіденційність: банківська інформація містить конфіденційні дані клієнтів, бізнес-операції та інші важливі деталі. Заходи мають на меті запобігти неправомірному доступу до цієї інформації, щоб уникнути витоку конфіденційних даних.

2. Захист від кіберзлочинців: зростання кіберзлочинності вимагає від банків ефективних заходів щодо кібербезпеки. Це включає в себе застосування передових технологій захисту мережі та інформаційних систем, а також навчання персоналу щодо розпізнавання фішингових атак та інших кіберзагроз.

3. Соціальна інженерія: заходи повинні бути спрямовані на запобігання атак, які використовують соціальну інженерію для отримання доступу до конфіденційної інформації. Це може включати навчання персоналу щодо виявлення та уникнення соціально-інженерних атак.

4. Відповідальність персоналу: працівники банку повинні бути свідомі важливості збереження конфіденційності та відповідальності за захист інформації. Заходи включають в себе проведення тренінгів, встановлення чітких правил користування інформацією та впровадження механізмів внутрішнього контролю.

5. Моніторинг та виявлення інцидентів: важливо мати системи моніторингу, які можуть вчасно виявляти незвичайну або підозрілу активність в мережі, щоб оперативно реагувати на потенційні загрози та інциденти.

6. Законодавча відповідність заходи повинні враховувати вимоги законодавства, щоб банк дотримувався стандартів безпеки та не порушував встановлені норми.

Всі ці аспекти допомагають банку створити ефективну систему захисту інформації, яка гарантує конфіденційність, цілісність та доступність банківської інформації.

Для забезпечення безпеки інформації банківські працівники повиннідотримуватисяправил. Ось деякі ключові аспекти, які вони повинні враховувати:

1. Дотримання стандартів безпеки: персонал повинен дотримуватися внутрішніх та зовнішніх стандартів безпеки, встановлених банком і відповідними регуляторами. Це включає в себе використання захищених паролів, шифрування інформації та інші стандарти безпеки даних.

2. Регулярне навчання та тренінги: банківський персонал повинен регулярно навчатися новим методам і технологіям забезпечення безпеки.

Тренінги допомагають зрозуміти поточні загрози та ефективні заходи для їх запобігання.

3. Використання безпечного програмного забезпечення: працівники повинні використовувати тільки ліцензійне та оновлюване програмне забезпечення, яке відповідає стандартам безпеки.

4. Фізична безпека: крім цифрових аспектів, працівники повинні дотримуватися фізичних заходів безпеки, таких як обмеження доступу до приміщень з серверами чи конфіденційними документами.

5. Управління доступом: забезпечення обмеженого доступу до конфіденційної інформації лише тим працівникам, які мають необхідність в ній, є важливим для запобігання неправомірному використанню даних.

6. Реагування на інциденти: працівники повинні бути навчені ефективно реагувати на можливі кіберінциденти або порушення безпеки та повідомляти про них відповідним відділам.

7. Вживання заходів проти соціальної інженерії профілактичні заходи від соціальної інженерії, такі як виявлення фішингових атак, грають важливу роль у забезпеченні безпеки.

Забезпечення безпеки інформації — це комплексний процес, і важливо, щоб працівники були добре підготовлені та дотримувались визначених процедур і стандартів безпеки.

Заходи безпеки при звільненні працівника, особливо того, який мав доступ до конфіденційної інформації, є критичними для забезпечення цілісності та безпеки даних. Ось кілька ключових заходів безпеки, які можуть бути вжиті:

1. Перегляд прав доступу: першим кроком є перегляд і відкликання всіх прав доступу працівника до інформаційних систем та конфіденційних даних. Це може включати доступ до серверів, баз даних, електронної пошти та інших інструментів.

2. Зміна паролів та ключів доступу: важливо змінити всі паролі та ключі доступу, які були використані працівником. Це допоможе уникнути неправомірного доступу після звільнення.

3. Фізичний доступ: в період звільнення, особливо якщо працівник має фізичний доступ до приміщень, важливо забезпечити заблокування йому доступу до офісних приміщень та інших фізичних ресурсів.

4. Нагляд за виїздом: в разі можливості, здійснюйте нагляд за працівником під час виїзду, переконуючись, що він не намагається вивезти чи викрасти конфіденційну інформацію чи обладнання.

5. Забирання робочих засобів: заберіть у працівника всі робочі засоби, такі як ноутбуки, смартфони, ключі USB тощо. Переконайтеся, що ніякі конфіденційні дані не залишаються на його особистих пристроях.

6. Звітність: підготуйте документ, що фіксує всі заходи безпеки, які були вжиті під час звільнення. Цей документ може стати частиною внутрішньої звітності та слугувати як інформаційна основа у випадках аудиту чи інциденту.

7. Повідомлення колег: сповістіть інших співробітників про звільнення працівника, особливо тих, які можуть взаємодіяти з ним або мати доступ до інформації, що стосується його робочих обов'язків.

Забезпечення безпеки під час звільнення вимагає завчасного планування та чіткої стратегії для мінімізації ризиків витоку конфіденційної інформації або інших безпекових проблем.

Заходи безпеки, вжиті під час звільнення працівника та спрямовані на контроль і захист інформації, сприяють декільком аспектам: Запобігання неправомірному доступу: Відключення або перегляд прав доступу працівника до інформаційних систем допомагає уникнути неправомірного доступу після припинення його трудових відносин з компанією. Захист конфіденційності та цілісності даних: Зміна паролів та ключів доступу, а також відкликання всіх доступів допомагає у збереженні конфіденційної інформації та уникненні її несанкціонованого використання.

Фізичний контроль заборона фізичного доступу звільненого працівника до офісних приміщень та інших фізичних ресурсів захищає від можливих фізичних загроз та несанкціонованого забирання інформації чи обладнання.Зменшення ризику витоку даних. Заборона вивезення робочих засобів і перевірка виходу працівника може зменшити ризик витоку конфіденційної інформації чи недозволеного вивезення даних. Збереження репутації компанії.Заходи безпеки допомагають зберегти репутацію компанії, оскільки вони демонструють відповідальний ставлення до управління інформаційною безпекою та уникнення можливих інцидентів.

Виконання нормативних вимог.Деякі заходи безпеки, такі як відключення доступів та зміна паролів, можуть відповідати вимогам законодавства щодо захисту даних та конфіденційної інформації.Збереження ефективності інформаційних систем: Заходи безпеки допомагають зберегти ефективність та безпеку інформаційних систем компанії, запобігаючи недозволеним діям та зберігаючи довіру клієнтів та партнерів.

Загалом, ці заходи спрямовані на максимальний захист конфіденційної інформації, запобігання ризикам та збереження інтегрітету систем безпеки компанії.

Захист інформації на банківських пристроях є надзвичайно важливим завданням для забезпечення інформаційної безпеки. Банки вживають ряд заходів для гарантування цього захисту Шифрування даних: Однією з основних стратегій є використання шифрування для захисту конфіденційної інформації. Важливі дані на пристроях шифруються, щоб унеможливити їх доступ для несанкціонованих осіб. Якщо пристрій потрапить в неправомірні руки,

інформація залишиться непридатною для використання без правильного розшифрування.

Системи аутентифікації: Системи вимоги до входу, такі як біометричні дані, одноразові паролі чи токени безпеки, гарантують, що лише авторизовані особи можуть отримати доступ до банківських пристроїв та інформаційних систем.

Фізичний захист: банки використовують фізичні заходи безпеки, такі як системи контролю доступу, відеоспостереження та інші, щоб унеможливити несанкціонований доступ до фізичних об'єктів та пристроїв.Спеціалізоване програмне забезпечення: Застосування антивірусів, антиспаму та файрволів допомагає виявляти та запобігати загрозам безпеки на рівні програмного забезпечення.

Оновлення та патчі: регулярні оновлення програмного та апаратного забезпечення, а також використання патчів безпеки, допомагають усувати вразливості та мінімізувати ризики. Політики безпеки: Банки встановлюють та виконують строгі політики безпеки, що регулюють доступ, збереження та обробку інформації на пристроях та системах.

Співробітництво зі сторонніми постачальниками: Банки вимагають від своїх постачальників відповідати високим стандартам безпеки та виконувати відповідні норми для захисту інформації. Навчання персоналу: Здійснення навчання персоналу щодо правил безпеки, розпізнавання фішингових атак та інших технік атак дозволяє ефективно реагувати на загрози та збільшує свідомість персоналу.

Ці комплексні заходи не тільки допомагають запобігти втратам та несанкціонованому доступу, але й створюють надійну систему захисту інформації на всіх рівнях банківської діяльності.

Спеціальний реєстр банку - це обов'язковий документ, який веде банк та містить важливі відомості про його фінансовий стан, операції та інші ключові аспекти діяльності. Такий реєстр є частиною регулюючого та наглядового механізму у банківській сфері та може бути обов'язковим вимогами від відповідних фінансових установ чи регуляторів.

Основні елементи спеціального реєстру банку можуть включати:

1. Фінансова інформація: Звіти про фінансовий стан банку, включаючи баланс, звіт про прибутки і збитки, розширені фінансові показники.

2. Інформація про операції: деталізація проведених операцій банку, таких як кредитування, інвестування, обслуговування клієнтів та інші банківські трансакції.

3. Структура власності: інформація про власників та ділові партнери банку, включаючи дочірні та пов'язані компанії.

4. Регуляторні вимоги: відомості про те, як банк відповідає регуляторним вимогам та нормативам, у тому числі в сфері капіталу, ліквідності та ризиків.

5. Показники ефективності: оцінки та аналіз ключових показників ефективності, таких як рентабельність активів, обсяги приваблення депозитів та інші.

6. Звіти про ризики: інформація про ідентифікацію та управління ризиками в банку, включаючи кредитний, ринковий та операційний ризики.

Спеціальний реєстр є інструментом, що дозволяє регуляторам, інвесторам та іншим зацікавленим сторонам відстежувати та оцінювати діяльність банку з точки зору фінансової стійкості, дотримання законодавства та рівня ризиків.

2.3 Основи управління інформаційною безпекою

Управління інформаційною безпекою в банку відповідає стандартам ISO/IEC 27000, які є серією міжнародних стандартів з інформаційної безпеки. Ці стандарти визначають вимоги та рекомендації для створення, впровадження, удосконалення та оцінки ефективності систем управління інформаційною безпекою. Нижче розглянуті ключові аспекти управління інформаційною безпекою в банку в контексті стандартів ISO 27000:

1. Установлення політики інформаційної безпеки: Банк повинен визначити свою політику інформаційної безпеки, враховуючи вимоги стандарту ISO 27001. Ця політика повинна визначати зобов'язання банку щодо захисту інформації та забезпечення відповідності до регуляторних вимог та нормативів.

2. Ризик-орієнтований підхід: Відповідно до стандартів ISO 27005, банк повинен провести оцінку ризиків для ідентифікації та управління потенційними загрозами інформаційній безпеці. Це допомагає визначити необхідні заходи безпеки та пріоритети управління ризиками.

3. Створення системи управління інформаційною безпекою: банк повинен впровадити систему управління інформаційною безпекою відповідно до вимог ISO 27001. Це включає в себе визначення областей застосування, внутрішніх процедур, контрольних точок та планів управління інцидентами.

4. Фізична та технічна безпека: відповідно до стандартів ISO 27002, банк повинен визначити та впровадити необхідні технічні та фізичні заходи безпеки для захисту інформації. Це може включати в себе контроль доступу, шифрування, ведення аудиту безпеки та інші заходи.

5. Система моніторингу та вдосконалення: стандарт ISO 27001 вимагає від банку встановлення системи моніторингу та постійного вдосконалення управління інформаційною безпекою. Це включає в себе проведення аудитів, оцінок та регулярне оновлення політик та процедур.

Здійснення управління інформаційною безпекою відповідно до стандартів ISO 27000 допомагає банку забезпечити ефективний захист інформації та відповідати сучасним вимогам до інформаційної безпеки

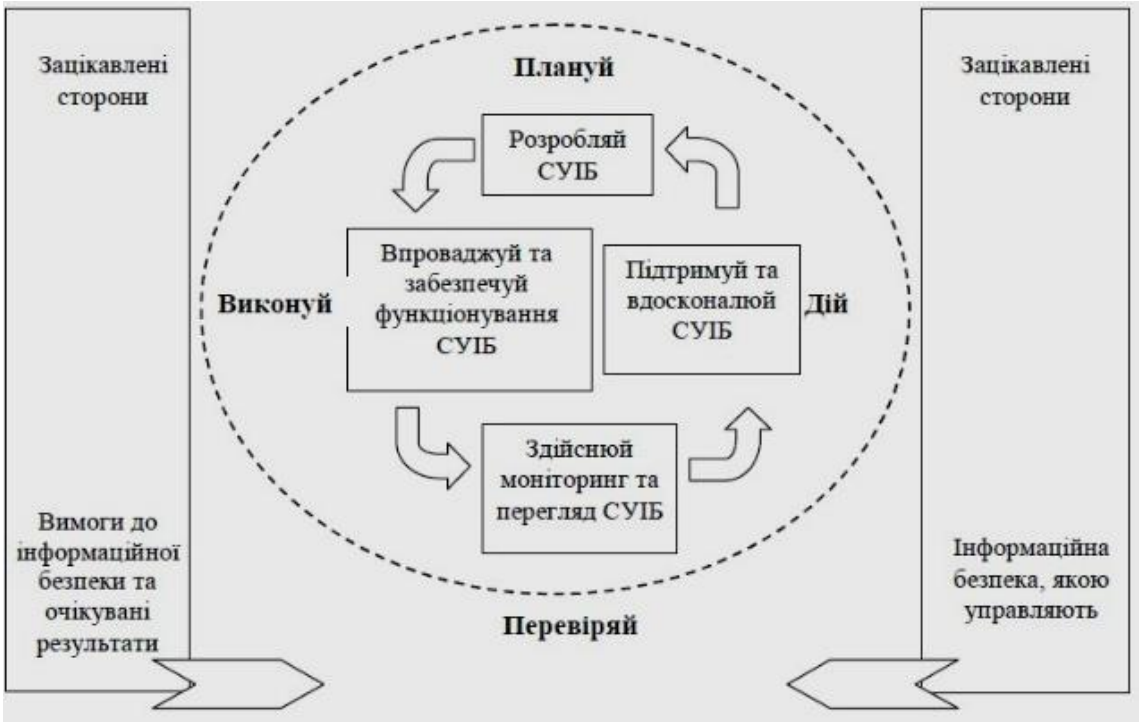


Рис 2.1 Вимоги до інформаційної безпеки

2.4 Моделі загроз, порушників та аналіз ризиків для об'єкту інформаційної діяльності

Моделі загроз — це концептуальні моделі, які допомагають нам зрозуміти, класифікувати й проаналізувати потенційні загрози системам інформаційної безпеки. Ці моделі можна використовувати для ідентифікації, оцінки та управління ризиками. Нижче наведено кілька типових шаблонів загроз:

1. Модель зовнішніх і внутрішніх загроз:

- зовнішні загрози: це також включає атаки зловмисників, не пов'язаних з організацією (наприклад, хакерів, кіберзлочинців).

- внутрішні загрози: виникають в результаті дій або недбалості власних співробітників або осіб, які мають доступ до системи.

2. модель загроз за джерелом:

- активні загрози: включає всі атаки, під час яких зловмисник активно взаємодіє з системою (наприклад, віруси, хакерські атаки).

- пасивні загрози: виникають у результаті стеження або перехоплення інформації без безпосереднього заподіяння шкоди (наприклад, шпигунство, перехоплення даних).

3. моделюйте загрози за цілями:

- фінансові загрози: спрямовані на фінансову вигоду (наприклад, шахрайство, крадіжка даних платіжної картки).

- політичні загрози: обмежуються впливом на політичну чи соціальну ситуацію (наприклад, комп'ютерне шпигунство, політичні кібератаки).

4. модель загрози за технічними методами:

- мережеві загрози: спрямовані на використання слабких місць мережевого з'єднання (наприклад, атаки перехоплення даних).

- програмні загрози: вони виникають через вразливість або помилки програмного забезпечення (наприклад, віруси, хробаки).

5. модель загрози за масштабом:

- локальні загрози: спрямовані на певний об'єкт або систему.

- глобальні загрози: потенційно можуть мати ширший вплив (наприклад, глобальні кібератаки).

розуміння цих закономірностей допомагає банкам та іншим організаціям розробляти ефективні стратегії захисту інформації та реагувати на різні загрози залежно від їх природи та джерела.

Моделі порушників в інформаційній безпеці розглядають різні типи осіб або груп, які можуть спробувати порушити безпеку системи чи отримати несанкціонований доступ до інформації. Нижче подано деякі загальні моделі порушників:

1. Хакери:

- Білі хакери: експерти з інформаційної безпеки, які використовують свої навички для тестування та вдосконалення систем безпеки.

- Сірі хакери: індивіди, які можуть вчиняти несанкціоновані дії, але можуть використовувати свої навички іноді з метою допомоги в усуненні вразливостей.

- Чорні хакери: зловмисники, які вчиняють несанкціоновані дії для особистої вигоди або шкоди.

2. Інсайдери:

- Ненавмисні інсайдери: співробітники, які ненавмисно порушують політики безпеки або допускають необережне використання інформації.

- Навмисні інсайдери: особи, які свідомо діють з шкідливими намірами, викрадаючи, руйнуючи або розголошуючи конфіденційну інформацію.

3. Державні актори:

- Офіційні чи неофіційні представники держав або інших державних організацій, які можуть здійснювати кібершпигунство, кібератаки або інші форми кіберагресії.

4. Кіберзлочинці:

- Особи чи групи, які вчиняють злочинні дії в інтернеті, такі як крадіжка особистої інформації, фінансові шахрайства, атаки на системи тощо.

5. Конкуренти:

- Особи чи організації, які можуть намагатися отримати конкурентну перевагу, викрадаючи або порушуючи інформацію конкурентів.

6. Ідеологічні або активістські групи:

- Групи, які діють з метою пропаганди своїх ідеологій або спроби вплинути на суспільство.

Ці моделі допомагають ідентифікувати потенційних загроз і розробляти стратегії захисту, враховуючи різноманітність порушників та їхні мотивації.

Аналіз ризиків в інформаційній безпеці включає визначення потенційних загроз та оцінку ймовірності та впливу подій, які можуть стати загрозами для безпеки інформації банку. Основні етапи аналізу ризиків включають:

1. Ідентифікація загроз:

- Визначення потенційних загроз для інформаційних активів банку. Це може бути кібератаки, втрата даних, несанкціонований доступ, природні катастрофи, людські помилки тощо.

2. Оцінка ймовірності:

- Визначення ймовірності того, що загроза станеться. Наприклад, ймовірність успішної кібератаки або випадкового втрати даних.

3. Оцінка впливу:

- Визначення потенційного впливу загрози на банк. Це може включати фінансові втрати, втрату репутації, порушення законодавства, перерви в роботі бізнес-процесів тощо.

4. Визначення рівня ризику:

- Об'єднання оцінок ймовірності та впливу для визначення рівня ризику. Це може бути високий, середній або низький рівень ризику.

5. Планування заходів захисту:

- Розробка стратегій та заходів для зменшення ризиків. Це може включати впровадження технічних заходів безпеки, політик безпеки, тренінги для персоналу, резервне копіювання даних, інцидент-менеджмент і т.д.

6. Моніторинг та оновлення:

- Постійне відстеження загроз, оцінка їхньої актуальності та оновлення стратегій та заходів захисту відповідно до нових викликів та технологічних тенденцій.

Аналіз ризиків допомагає банку визначити, які аспекти його інформаційної безпеки є найбільш уразливими та встановити пріоритети для ефективного використання ресурсів забезпечення безпеки.

Оцінка ризиків системи безпеки

Оцінка ризиків системи безпеки є важливим етапом для забезпечення ефективного функціонування інформаційної безпеки. Для цього застосовуються різноманітні методики та інструменти, а результати представляються у вигляді таблиці оцінки ризиків. Нижче наведено загальний підхід та можливий формат таблиці:

Методологія оцінки ризиків:

1. Ідентифікація загроз:

- Визначення загроз: перелік потенційних загроз для інформаційної системи (наприклад, злом системи, втрата даних, зловживання привілеїв).

- Класифікація загроз: визначення їхнього впливу та ймовірності.

2. Оцінка вразливостей:

- Визначення вразливостей: ідентифікація можливих слабкостей в системі безпеки.

- Оцінка вразливостей: визначення рівня вразливостей та їхнього впливу.

3. Оцінка ризиків:

- Розрахунок ризиків: врахування впливу загроз та вразливостей, призведення до визначення рівня ризиків.

Система ризиків банку

Ризики в сфері захисту інформації в банку можуть бути різноманітні та виникати з різних джерел. Основні види ризиків включають:

1. Технічні ризики:

- Кібератаки: можливість злому або атак на банківські інформаційні системи шляхом використання вірусів, хакерських атак, фішингу тощо.

- Технічні збої: проблеми в роботі обладнання, програмного забезпечення чи комунікацій, що можуть призвести до втрати даних або доступу до них.

2. Організаційні ризики:

- Внутрішні загрози: ризик, пов'язаний з діями або бездіяльністю співробітників, які можуть навмисно чи ненавмисно стати джерелом витоку інформації.

- Неадекватна політика безпеки: відсутність чи недостатність правил та стандартів для захисту інформації в банку.

3. Людські ризики:

- Соціальний інжиніринг: обман співробітників банку для отримання доступу до конфіденційної інформації шляхом маніпулювання їхнім відчуттям довіри.

- Недостатня освіта персоналу: відсутність розуміння правил безпеки серед персоналу, що може стати причиною помилок чи недбалості.

4. Зовнішні ризики:

- Зміни у законодавстві: можливість змін у правовому середовищі, які можуть вплинути на вимоги до захисту інформації та відповідність їм.

- Економічні чинники: вплив економічних факторів, таких як фінансова нестабільність, на здатність банку вдосконалювати системи безпеки.

5. Природні ризики:

- Пожежа, повінь, землетруси: природні катастрофи можуть призвести до фізичного пошкодження обладнання та інфраструктури, а також втрати даних.

6. Ризики у сфері обробки даних:

- Втрата даних: можливість втрати або пошкодження інформації внаслідок технічних або людських помилок.

Ефективний управлінський підхід до ризиків полягає у визначенні, оцінці та управлінні цими ризиками, розробці стратегій мінімізації можливих втрат та забезпеченні сталої безпеки інформації в банку.[29,32]

Загрози та вразливість	ймовірність	Вплив	Ризик	Рекомендації
Злом системи	Висока	Великий	Високий	Поссилити заходи аутентифікації та моніторингу
Втрата даних	Середня	Великий	Середній	Регулярні резервні копії та шифрування даних
Зловживання привілеїв	низька	Середній	Низький	Суворе обмеження доступу та моніторинг привілеїв

Таб 2.1 оцінца та управління ризиками

Ключовою метою оцінки ризиків є розробка стратегій управління ризиками та визначення пріоритетних заходів для забезпечення ефективної системи безпеки.

Система Реєстра та обліку банку

Підсистема реєстра та обліку в інформаційній системі банку відіграє важливу роль у забезпеченні ефективного управління та контролю за різними аспектами банківської діяльності. Основні функції та компоненти цієї підсистеми включають Реєстрація та Облік Клієнтів: Ведення бази даних, що містить інформацію про клієнтів банку, їхні рахунки, операції та інші важливі дані. Це включає відомості про фізичних та юридичних осіб, які користуються послугами банку.Фінансовий Облік Збір, обробка та збереження фінансових даних банку, включаючи інформацію про операції, стан рахунків, кредити та

інші фінансові аспекти. Реєстрація Транзакцій Фіксація та облік фінансових транзакцій, здійснюваних клієнтами або банком самостійно. Управління Платіжними Документами: Облік та контроль за платіжними документами, що включає в себе чеки, векселі, платіжні вимоги та інші фінансові інструменти.

Реєстрація та моніторинг кредитів Систематичний облік кредитів, їхніх умов та погашення. Моніторинг платоспроможності клієнтів та визначення ризиків.

Облік цінних паперів Ведення обліку цінних паперів, які можуть бути власністю банку чи його клієнтів.Управління Резервами Реєстрація та облік резервів, які банк зберігає для забезпечення фінансової стійкості та виконання регуляторних вимог.Електронний Документообіг Впровадження електронного документообігу для ефективного обміну та зберігання документів.

Реєстрація та Облік Активів та Зобов'язань Облік та контроль за активами та зобов'язаннями банку, що дозволяє здійснювати аналіз фінансового стану

Ця підсистема є ключовою частиною інформаційної системи банку, забезпечуючи точний облік та контроль за різними аспектами його діяльності.

2.5. Файли HTTP cookies

HTTP cookies (або просто "cookies") - це невеликі текові файли, які веб-сайти зберігають на комп'ютері користувача через його веб-браузер з метою збереження певної інформації. Cookies використовуються для взаємодії з користувачами, зберігання інформації про їхні вибори та надання персоналізованого досвіду використання в Інтернеті. Ось деякі ключові аспекти cookies Зберігання Інформації Cookies дозволяють веб-сайтам зберігати інформацію на пристрої користувача. Це може бути ідентифікатор сесії, мовні налаштування, обрані товари в корзині тощо.

Аутентифікація та Збереження Стану Сесії Cookies використовуються для збереження інформації про авторизацію користувача та збереження стану сесії між запитами до веб-сайту. Персоналізація Користувальницького Досвіду: Вони можуть використовуватися для запам'ятовування користувальницьких налаштувань, таких як мова, розмір шрифту та інші параметри. Відстеження та Аналітика: Cookies дозволяють веб-сайтам відстежувати поведінку користувачів, збирати аналітичні дані та надавати інформацію веб-власникам для аналізу використання сайту

Рекламна Сегментація Cookies використовуються рекламними платформами для створення профілів користувачів та відображення цільованої реклами на веб-сайтах. Заборона Відстеження. Деякі браузери підтримують функцію "Do Not Track", яка дозволяє користувачам вказувати, що вони не бажають бути відстежуваними за допомогою cookies. Термін Дії

Cookies можуть бути тимчасовими (вони зникають після закриття браузера) або постійними (зберігаються на пристрої користувача після закриття браузера). Безпека Використання cookies також пов'язане із забезпеченням безпеки, так як вони можуть допомагати у виявленні шахраїв та наданні захисту від певних видів атак.

Cookies може стосуватися заходів конфіденційності, і користувачі мають право контролювати, яку інформацію вони бажають ділитися через cookies у налаштуваннях свого браузера.[25]

2.6 API- функціональність правила та використання як інтсрументу кібербезпеки

API (інтерфейс програмування застосунків) - це набір правил та інструментів, які дозволяють одному програмному засобу взаємодіяти з іншим. Це надає можливість різним програмам чи сервісам обмінюватися даними і функціональністю.

API визначає, які запитання можуть бути розміщені та отримані, які дії можна виконати, іншими словами, як одному програмному компоненту взаємодіяти з іншим. API може бути представлений у вигляді набору бібліотек, опублікованих в Інтернеті, або у вигляді визначень протоколів, які визначають взаємодію між компонентами.

API може використовуватися для доступу до функцій апаратного забезпечення, взаємодії з веб-сервісами, обміну даними між програмами та багатьма іншими завданнями. Основна ідея полягає в тому, щоб робити різні програми і сервіси сумісними та взаємозамінними через стандартизований спосіб взаємодії.

Функціональність API (інтерфейсу програмування застосунків) залежить від конкретного API та його призначення. Проте загальною метою API є надання можливостей взаємодії між різними програмами, сервісами чи компонентами програмного забезпечення. Ось деякі основні аспекти функціональності API:

Взаємодія API дозволяє програмам обмінюватися даними та взаємодіяти одна з одною. Це може включати передачу даних, виклик функцій, обмін подіями тощо. Доступ до функцій API надає доступ до функціональності певного програмного компонента чи сервісу. Наприклад, у випадку веб-сервісу API може визначати, які операції можна виконувати над ресурсами (наприклад, отримати, оновити, видалити).

Стандартизація комунікації: API визначає стандарти та протоколи для обміну даними. Це робить взаємодію між програмами більш передбачуваною та стандартизованою.

Робота з веб-сервісами Багато API використовуються для роботи з веб-сервісами. Вони можуть бути використані для отримання даних з веб-сервера, відправки запитів, роботи з REST або SOAP протоколами тощо. Розширення функціональності Деякі програми надають API для розширення їх функціональності. Розробники можуть використовувати API для створення додаткових плагінів чи розширень.

Автоматизація завдань API може дозволяти автоматизувати певні завдання, використовуючи функції, які надаються API. Забезпечення безпекиДеякі API мають функції забезпечення, такі як аутентифікація та авторизація, щоб забезпечити безпеку взаємодії між програмами.

Взагалі, API відкриває можливості для інтеграції різних програм і дозволяє їм працювати разом, сприяючи взаємодії та розвитку різноманітних додатків та сервісів.[20-22]

2.7 Застосування API в кібербезпеці

API (інтерфейси програмування застосунків) використовуються в кібербезпеці на різних рівнях та для різноманітних завдань. Ось деякі приклади використання API в кібербезпеці:

1. Системи виявлення та запобігання інцидентам (IDPS): API використовуються для взаємодії між різними компонентами системи IDPS. Наприклад, отримання даних від сенсорів, передача сигналів аларму, блокування мережевого трафіку тощо.

2. Антивірусні програми: Антивірусні рішення використовують API для аналізу файлів, виявлення шкідливого коду, визначення підозрілих дій.

3. Менеджмент ідентифікації та доступу: API використовуються для забезпечення інтеграції між системами управління ідентифікацією та контролем доступу. Це може включати автоматичне надання або відкликання прав доступу.

4. Аналіз загроз та вразливостей: API дозволяють взаємодіяти з іншими системами для отримання інформації про поточні загрози та вразливості. Це може бути важливим для прийняття рішень щодо заходів забезпечення.

5. Системи журналювання та моніторингу безпеки: API використовуються для отримання даних журналування та іншої інформації з систем моніторингу безпеки.

6. Інтеграція з розвідувальними та аналітичними платформами: API дозволяють обмінюватися даними між кібербезпечними платформами та інструментами, що використовуються для аналізу загроз та реагування на інциденти.

7. Системи керування подіями та відновлення: API використовуються для автоматизації відновлення та реагування на кіберінциденти, а також для передачі даних про інциденти у системи управління подіями.

8. Захист веб-додатків: Веб-фаерволи та інші інструменти захисту веб-додатків використовують API для моніторингу та фільтрації HTTP-трафіку.

Взаємодія між різними системами через API допомагає підвищити ефективність та спрощує процеси кібербезпеки, забезпечуючи автоматизацію та вчасну реакцію на потенційні загрози.[30]

2.8. Висновок до розділу

Висновок до другого розділу, реєстру обліку, моделей порушників, моделей загроз та аналізу ризиків є наступним:

Оцінка ризиків є невід'ємною частиною стратегії забезпечення інформаційної безпеки банку. Вона дозволяє ідентифікувати та квантувати потенційні загрози та визначити оптимальні заходи для зменшення ризиків та забезпечення стабільності системи.

Реєстр обліку виступає важливою складовою системи безпеки, надаючи можливість відстежування доступу та маніпулювання інформацією, що допомагає у попередженні неправомірного доступу та виявленні можливих порушень.

Моделі порушників та загроз дозволяють усвідомлено аналізувати потенційні сценарії атак та вживати відповідних превентивних заходів. Ці моделі слугують основою для розробки ефективної стратегії захисту, визначаючи слабкі місця та виявляючи осіб, які можуть стати порушниками.

Аналіз ризиків дозволяє управлінцям банку зосередитися на найбільш критичних аспектах інформаційної безпеки та призначити ресурси для мінімізації потенційних загроз.

Всі ці елементи разом формують комплексний підхід до інформаційної безпеки, що дозволяє банку працювати в умовах високої захищеності та ефективно управляти ризиками. Заходи безпеки охоплюють усі аспекти діяльності банку, включаючи технічні, організаційні та правові підходи. Це включає встановлення систем контролю доступу, впровадження політики конфіденційності, перевірки безпеки, нормативний захист інформації та реагування на потенційні загрози.

При побудові системи інформаційної безпеки вирішальними є такі принципи, як законність, повнота інформації, обґрунтованість заходів та превентивні заходи. Ці принципи спрямовані на дотримання закону, захист усіх типів інформації, розумне використання ресурсів та передбачення потенційних загроз.

Також важливо враховувати людський фактор у системі захисту інформації. Заходи щодо звільнення, обов’язкове навчання персоналу та

дотримання принципів особистої відповідальності допомагають захистити дані від загроз, що постійно змінюються.

Технологічний аспект включає використання технічних і програмних засобів, таких як брандмауери, антивіруси, шифрування, які відіграють ключову роль у забезпеченні цілісності, конфіденційності та доступності інформації.

Усі ці аспекти разом створюють надійну основу інформаційної безпеки банківського сектору, сприяючи виконанню головної мети – достовірності

РОЗДІЛ 3. МЕТОДИКА УДОСКОНАЛЕННЯ ЗАСОБІВ ЗАХИСТУ ІНФОРМАЦІЇ

3.1 Ідентифікація загроз. Створення системи виявлення та аналізу

Першим кроком проведемо оцінку ризиків та загроз. Оцінка єважливим єтапом у розробці стратегії захисту інформації банку. І дозволяє індетифікувати небезпеку та засзделегіть бути готовим до потенційних небезпек.

Ідентифікація поділяється на

- зовнішні
- внутрішні

Зовнішні загрози включають віруси, кіберзагрози, різні типи атак

Внутрішні потенційні загрози серед персоналу , зловживання привілеїв і можливість отримання доступу до конфіденційної інформації

Загальна оцінка ризиків дозволяє вжити необхідних заходів на рівні департаменту, проекту, для конкретних ризиків або на рівні організації загалом. Як тільки загальна оцінка ризиків завершена, на ризик реагують шляхом вжиття одного або декількох відповідних заходів для зменшення ймовірності виникнення ризиків або їхнього впливу на систему.

Другий етап включає в себе впровадження нових технологій та вчасно обновляти ПО.

Нові технології розвиваються дуже швидки і разом з ними розвиваються і нові загрози

Третій етап включає в себе введення процесів аутентиіфкації та авторизації

Двух-факторнааутентифікація запровадить додатковий захист інформації та захистить дані

Четвертий етап – система виявлення порушень

Створення системи виявлення та аналізу аномалій для швидкого реагування на можливі порушення.

3.2 Siem система Qradar

QRadar є однією з популярних систем управління інформаційною та подійною безпекою (SIEM). Нижче наведено основні аспекти і можливості системи QRadar:

1. Збір і аналіз подій: QRadar збирає та аналізує величезний обсяг подій з різних джерел у реальному часі. Це може включати дані з лог-файлів, мережевих пристроїв, застосунків та інших джерел.

2. Кореляція подій: система використовує технологію кореляції для виявлення складних зв'язків та загроз на основі різних подій. Це дозволяє виявляти інциденти, які можуть залишитися непоміченими при аналізі окремих подій.

3. Виявлення загроз: QRadar використовує низку методів, таких як виявлення аномалій та підписів, для виявлення потенційно небезпечної діяльності в мережі. Важливе значення має вчений аналіз для ідентифікації нових та невідомих загроз.

4. Подробний аналіз інцидентів: QRadar надає можливість детально аналізувати інциденти, включаючи події, які їм передували, та їх контекст. Це сприяє ефективній реакції на інциденти та їх подальшому вивченню.

5. Візуалізація даних: система використовує графічні засоби для візуалізації даних та створення зручних для розуміння звітів та графіків. Це допомагає аналітикам та адміністраторам краще розуміти стан безпеки мережі.

6. Інтеграція з іншими системами: QRadar може інтегруватися з іншими продуктами та інфраструктурою безпеки, такими як файерволи, антивіруси, системи управління ідентифікацією, щоб забезпечити комплексний захист.

7.Автоматизована реакція: QRadar дозволяє встановлювати автоматизовані правила та сценарії реакції на певні види подій або загроз. Це спрощує процес відповіді на інциденти.

8. Управління конформністю: QRadar надає інструменти для відстеження та виконання вимог з охорони інформації, а також стандартів та нормативів.

QRadar використовується компаніями та організаціями для удосконалення безпеки їхньої інформаційної інфраструктури та ефективної реакції на кібер загрози[6]

3.3 Порівняння Siem системи qradar з іншою siem системою

Wazuh - це інтегрована платформа для безпеки інформації, яка надає засоби моніторингу безпеки, виявлення загроз і реагування на інциденти в реальному часі. Вона базується на відкритому коді і розроблена для забезпечення безпеки інформаційних систем та мереж.

Основні характеристики Wazuh включають:

1. Система детектора загроз (HIDS/NIDS): Wazuh включає агентів для моніторингу подій та детекторів аномалій на хостах та в мережі. Це дозволяє виявляти можливі загрози та неправомірні дії.

2. Корпоративна спільнота та відкритий код: Wazuh побудована на засадах відкритого коду, що дозволяє користувачам змінювати і вдосконалювати систему за власними потребами. Вона також має активну спільноту, яка допомагає вирішувати питання та надає підтримку.

3. Система управління інцидентами: Wazuh надає можливості реагування на інциденти, включаючи сповіщення, автоматизовані реакції та інтеграцію з іншими системами безпеки.

4. Масштабованість: Платформа легко масштабується від невеликих до великих інфраструктур, що дозволяє використовувати її для захисту різних типів організацій.

Wazuh дозволяє підприємствам виявляти, аналізувати та реагувати на загрози в режимі реального часу**,** роблячи її потужним інструментом для забезпечення кібербезпеки.

Особливості	qradar	wazuh
вартість	2	5
Архітектура розгортання	5	4.1
масштабність	5	4.5
Хмари	4.5	4.0
Інтеграція API	4.5	4.0
інтрефейс	4.3	3.8
Пошук загроз	4	4.5
Сторонні ресурси	4.5	4.2
Якість підтримки	4.1	4.0

Табл 3.1 Порівняння siem систем qradar та wazuh

3.4 X-Force exchange як інформаційна платформа для обміну даних

X-Force Exchange — інформаційна платформа, розроблена IBM, яка забезпечує обмін даними та інтелектуальними ресурсами, пов’язаними з кібербезпекою. Ключовими аспектами X-Force Exchange є:

1. Обмін загрозами: Платформа дозволяє користувачам обмінюватися інформацією про комп’ютерні загрози та вразливості. Це допомагає спільноті кібербезпеки бути більш обізнаними про потенційні загрози.

2. Дані про вразливості: X-Force Exchange містить дані про вразливості, виявлені в програмних продуктах і системах. Це дозволяє організаціям швидше реагувати на потенційні загрози безпеці.

3. Тактична розвідка: Платформа надає тактичну розвідку щодо нових загроз, атак і методів, що дозволяє аналітикам і кіберзахисникам бути в курсі останніх подій у світі кібербезпеки.

4. Велика база знань: X-Force Exchange має обширну базу даних багатьох загроз, включаючи дані про зловмисне програмне забезпечення, індикатори компрометації, звіти про атаки тощо.

5. API та інтеграція: Платформа підтримує API для інтеграції з іншими інструментами та системами безпеки. Це дозволяє інтегрувати дані та розвідку X-Force Exchange у різноманітні рішення кіберзахисту.

6. Інструменти аналізу та візуалізації: Платформа надає інструменти для аналізу та візуалізації даних про загрози. Це допоможе вам зрозуміти контекст і природу кіберзагроз.

X-Force Exchange розширює можливості спільноти кіберзахисту, дозволяючи їм об’єднати зусилля та ефективно боротися із загрозами в онлайн-середовищі.

3.5 Взаємодія X-Force exchange Та API

Для удосконалення засобів захситу інформацію проведемо експеримент

Ми інтегруємо до нашої SIEM системи через APIзагальнодоступний сервіс X-Force exchangedля визначення репутації, рівнів ризиків ip-адрес, хешів , доменів тощо.

X-Force exchange- платформа для обміну інформації про кіберзагрози та безпеку інформаційних технологій

API- набір правил та інструкцій і функцій, які можуть викликати інше програмне забезпечення. І дозволяє програмам взаємодіяти між різними програмами обмінюючись даними та функціоналом. [22]

Ми будемо Використовувати SIEM систему– QRADAR

Для удосконалення засобів захисту інформації проведемо експеримент

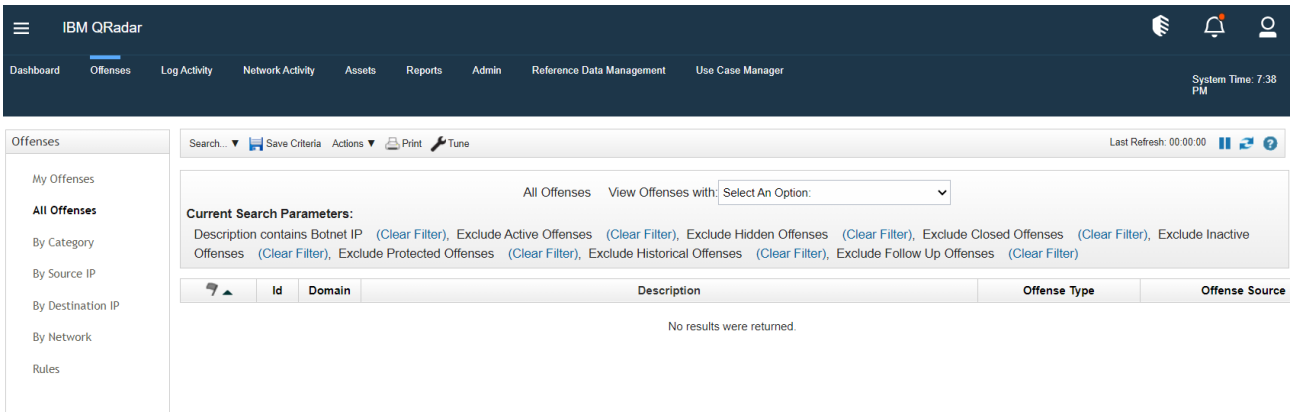


Рис 3.1 у нас відсутня інтеграція сервісу X-Force exchange

В цьому випадку у нає два варіанти розвитку подій :

1. SIEM система генерує нам алерт на основі зазделлегіть створеної нам таблиці в яку ми попредньо власноруч завантажуємо ті IP- адреси в яких ми впевнені, що вони мають високий рівень визику погану репутацію . Цей варіант не зручний

2. SIEM система не генерує нам алерти бо вона немає жодної бд репутації ip-адрес.

Обидва варіанти не вдосконалені в захисті системи і зводять SIEM систему на нівець

На даному рис 3.1 як наслідок ми бачимо що наша SIEM система ніяк не реагує на конекти до адреси – 101.226.26[.]217 яка з недавнього часу була помічена за шкідливою активністю.

Тобто потенційно у нас є заражена машинау нашій мережі за адресою 10.10.10.10 яку ми не бачимо через недостаток актуальних даних в нашій SIEM системі.

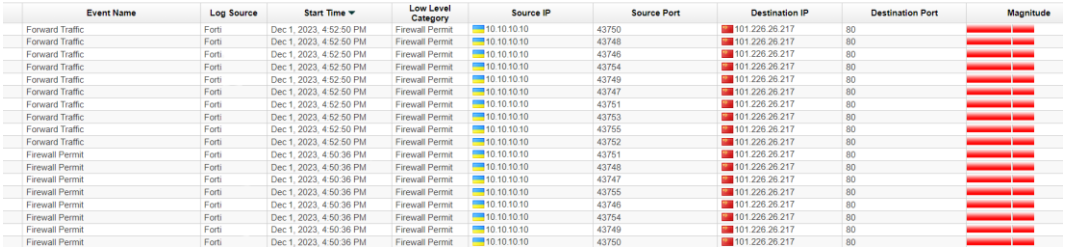


Рис 3.2 активність

Тут для усунення цього недоліку ми зробимо інтеграцію сервісуX-Force exchangedo нашої SIEM системи через API. Так як Апі дає нам змогу взаємодіяти з різними системами на автоматичному рівні

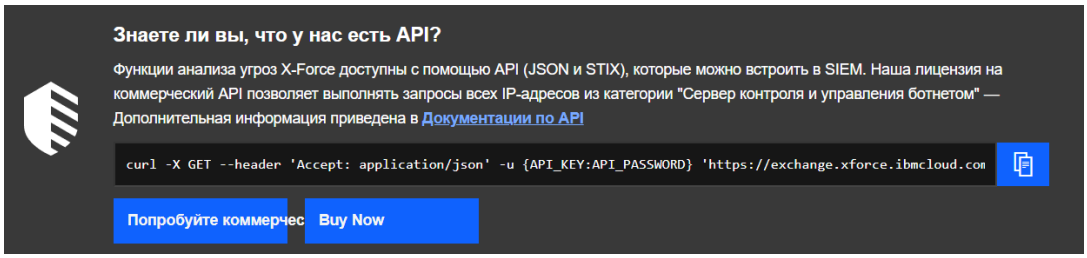


Рис 3.3 прописуєм команду на підключення АПІ

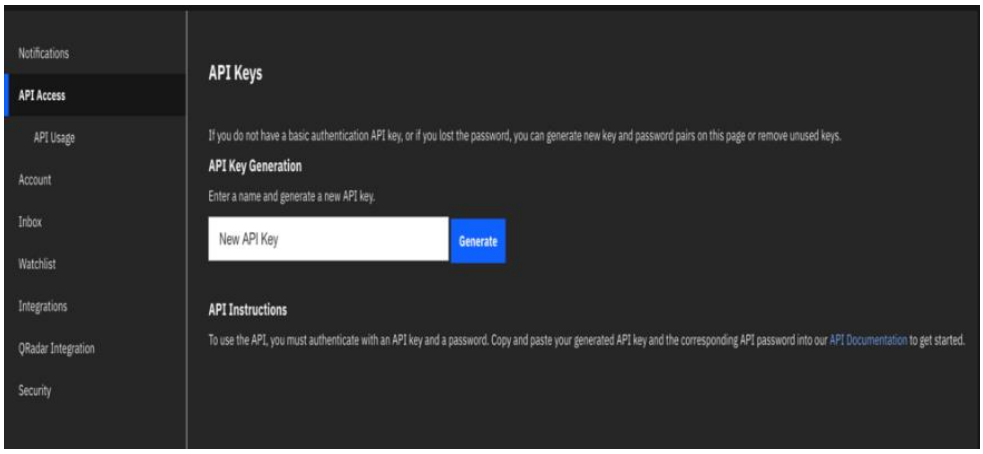


Рис 3.4 Створюємо ключ

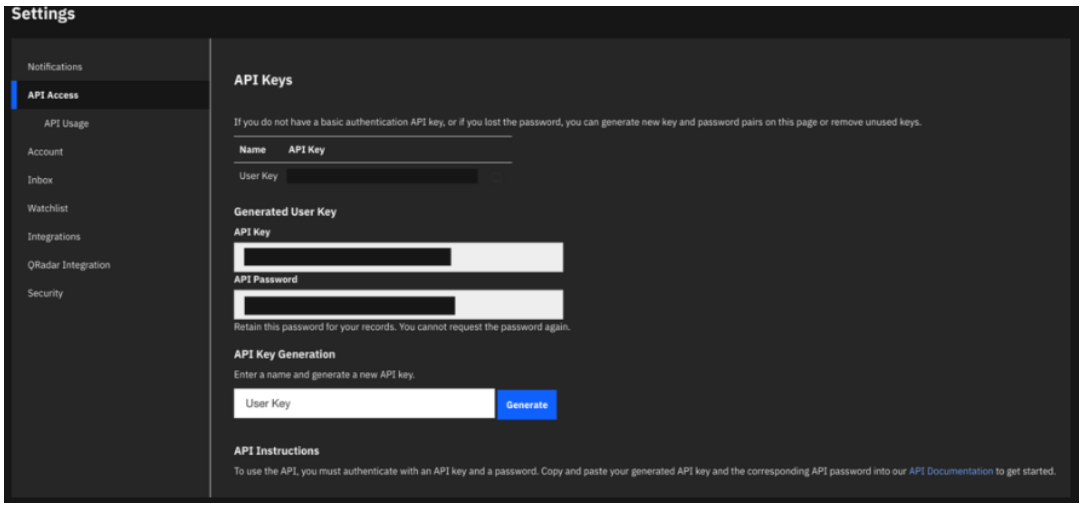


Рис 3.5 генерація ключа

Генеруємо АПІ ключ і пароль і потім на сервері ми вставлємо curl -X GET --header 'Accept: application/json' -u {API_KEY: API_PASSWORD} наші ключі в API-key Та api- password .

В Qradar ми налаштовуємо так щоб по АПІ у нашої SIEM системи були актуальні шкідливі адресиякі виявив сам IBM використовуючимережеві пастки напрклад які виявляють ботнети.

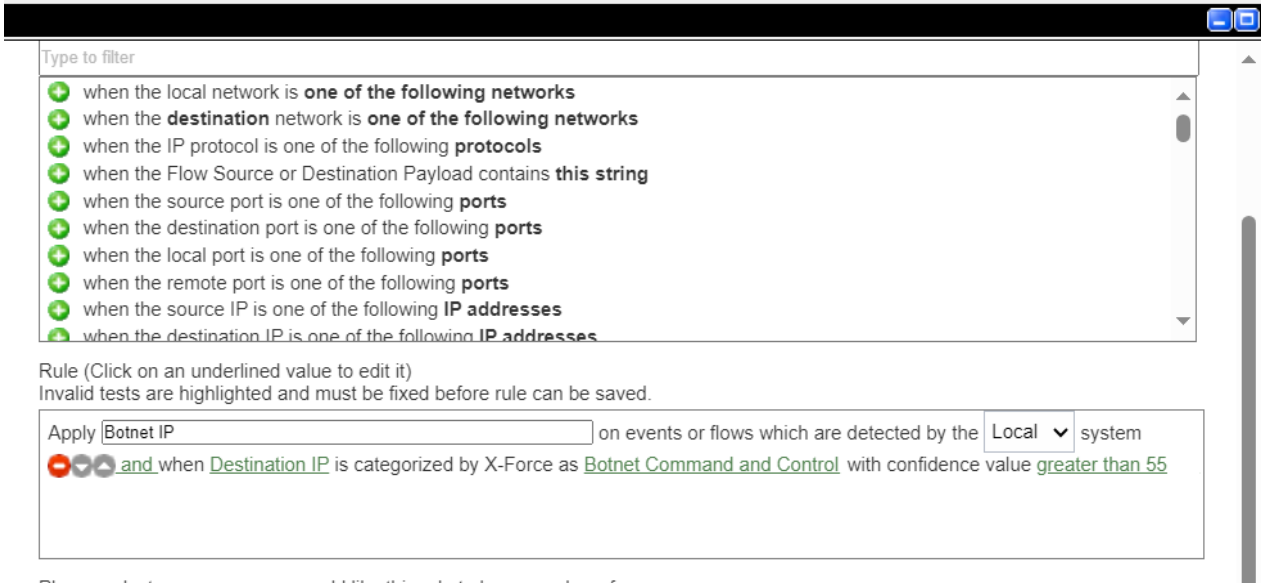


Рис 3.6 створення правила

На рис3.6 ми створюємо правило для SIEM системи для виявлення інцеденту безпеки на основі актуальної бази шкідливих IP- адрес які ми отримали в результаті попередньої дії

Тепер буде генеруватися алерт в тому випадку якщо адреса призначення (адреса до якої звертається наша машина з локальної мережі) буде помічена у шкідливійактивності.

Тут ми можемо побачити що від тепер QRADAR відмічає ті підключення«Botnet IP» . Тепер ми бачимо алерт який система згенерувала автоматично відмітивши події зєднань до адреси 101.226.26[.]217 як потенціні коннект до ботнет мережі.

В результаті чого ми можемо оперативно виявити потенційно заражену машину[26,27]

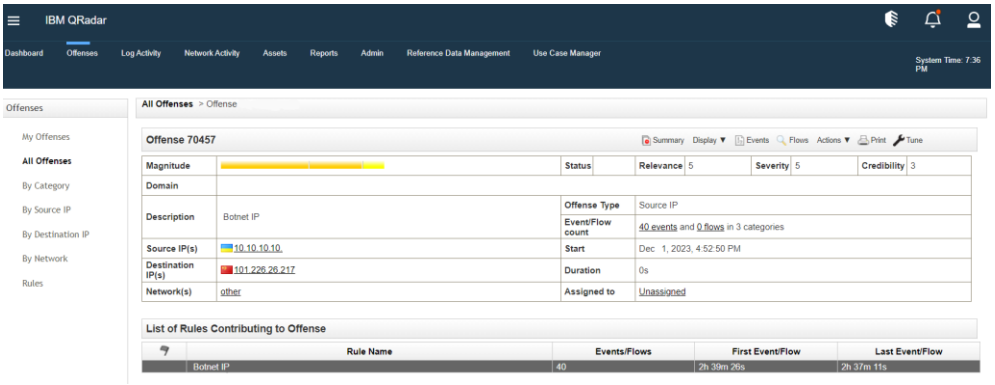
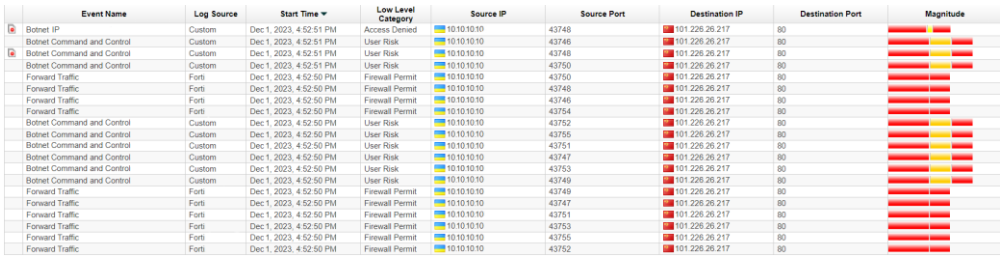


Рис 3.7 виявлення загрози



Event Name	Log Source	Start Time	Low Level Category	Source IP	Source Port	Destination IP	Destination Port	Magnitude
Botnet IP	Custom	Dec 1, 2023, 4:52:51 PM	Access Denied	10.10.10.10	43748	101.226.26.217	80	
Botnet Command and Control	Custom	Dec 1, 2023, 4:52:51 PM	User Risk	10.10.10.10	43746	101.226.26.217	80	
Botnet Command and Control	Custom	Dec 1, 2023, 4:52:51 PM	User Risk	10.10.10.10	43746	101.226.26.217	80	
Botnet Command and Control	Custom	Dec 1, 2023, 4:52:51 PM	User Risk	10.10.10.10	43750	101.226.26.217	80	
Forward Traffic	Forti	Dec 1, 2023, 4:52:50 PM	Firewall Permit	10.10.10.10	43750	101.226.26.217	80	
Forward Traffic	Forti	Dec 1, 2023, 4:52:50 PM	Firewall Permit	10.10.10.10	43748	101.226.26.217	80	
Forward Traffic	Forti	Dec 1, 2023, 4:52:50 PM	Firewall Permit	10.10.10.10	43746	101.226.26.217	80	
Forward Traffic	Forti	Dec 1, 2023, 4:52:50 PM	Firewall Permit	10.10.10.10	43754	101.226.26.217	80	
Botnet Command and Control	Custom	Dec 1, 2023, 4:52:50 PM	User Risk	10.10.10.10	43752	101.226.26.217	80	
Botnet Command and Control	Custom	Dec 1, 2023, 4:52:50 PM	User Risk	10.10.10.10	43755	101.226.26.217	80	
Botnet Command and Control	Custom	Dec 1, 2023, 4:52:50 PM	User Risk	10.10.10.10	43751	101.226.26.217	80	
Botnet Command and Control	Custom	Dec 1, 2023, 4:52:50 PM	User Risk	10.10.10.10	43747	101.226.26.217	80	
Botnet Command and Control	Custom	Dec 1, 2023, 4:52:50 PM	User Risk	10.10.10.10	43753	101.226.26.217	80	
Botnet Command and Control	Custom	Dec 1, 2023, 4:52:50 PM	User Risk	10.10.10.10	43749	101.226.26.217	80	
Forward Traffic	Forti	Dec 1, 2023, 4:52:50 PM	Firewall Permit	10.10.10.10	43749	101.226.26.217	80	
Forward Traffic	Forti	Dec 1, 2023, 4:52:50 PM	Firewall Permit	10.10.10.10	43747	101.226.26.217	80	
Forward Traffic	Forti	Dec 1, 2023, 4:52:50 PM	Firewall Permit	10.10.10.10	43751	101.226.26.217	80	
Forward Traffic	Forti	Dec 1, 2023, 4:52:50 PM	Firewall Permit	10.10.10.10	43753	101.226.26.217	80	
Forward Traffic	Forti	Dec 1, 2023, 4:52:50 PM	Firewall Permit	10.10.10.10	43755	101.226.26.217	80	
Forward Traffic	Forti	Dec 1, 2023, 4:52:50 PM	Firewall Permit	10.10.10.10	43752	101.226.26.217	80	

Ну рисунку 3.8 ми можемо побачити что наша SIEM система виявила BOTNET ip

Давайте розберемося що таке Botnet IP – IP-адреса компютера або іншого пристрою який став частиною ботнету. Іншими словами ботнет – мережа компютерів які були заражені шкідливим програмним забезпеченням і можуть використовуватися зловмисником в його цілях без відома власників компютерів.

- Боти можуть використан для спроб вторгнення
- Ботнет може використовуватися для збору інформації
- Для розсилання спаму або небажаних листів
- Для спрямування великої кількості запитів на сервер (DDOS-атака)

Ми можемо побачитищо правило працює за рахунок API

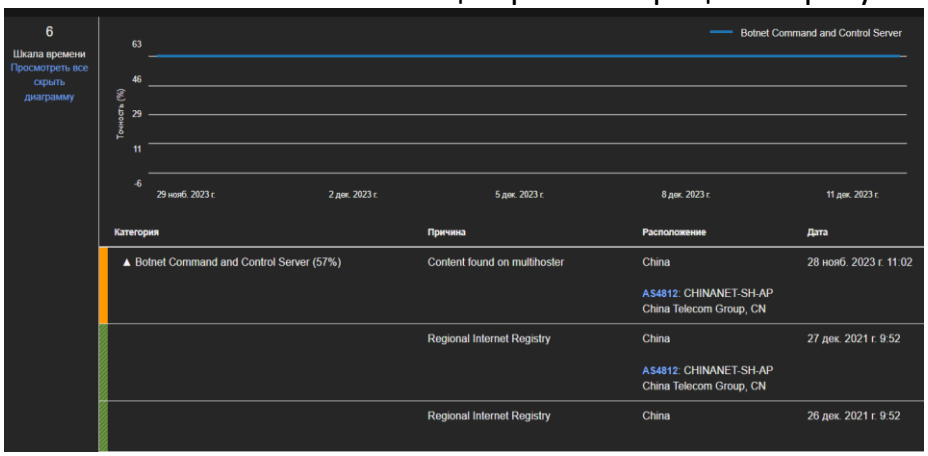


Рис 3.9 Ми можемо побачитищо правило працює за рахунок API

Після проведення тесту на удосконалення засобів захисту можна точно сказати що система реагує на інциденти та забезпечить надійний захист інформацію і безпеку

3.6 Висновок до розділу

Інтеграція подібних сервісів через АПІ дозволяє нам грамотно настроїти роботу нашої SIEM системи. Результатом чого є можливість опертично

реагувати на можливе зараження машин в мережінашого підприємства. Як внаслідок своєчасне усунення проблем систем захисту інформаційної безпеки

Або попередження можливих компрометації даних та мережі підприємства.

Описавши правльно правила та підключення API до нашої системи ми можемо підвести підсумки того що інтеграція API до різних бібліотек там систем потрібна в наш час адже різні атакі віруси появляються кожний день і захист системи моніторитись і вдосконалюватися кожного дня для більш захищеності системи. Провівши атаку ми побачили як API дозволяє швидко реагувати на різні інциденти та своєчасно захистити інформацію в банку.

РОЗДІЛ 4 ОХОРОНА НАВКОЛИШНЬОГО СЕРЕДОВИЩА

Джерела екологічної інформації.

Інформація про стан навколишнього природного середовища (екологічна інформація) – це будь-яка інформація в письмовій, аудіовізуальній, електронній чи іншій матеріальній формі про:

- стан навколишнього природного середовища чи його об’єктів – землі, вод, надр, атмосферного повітря, рослинного і тваринного світу та рівні їх забруднення;
- біологічне різноманіття і його компоненти, включаючи генетично видозмінені організми та їх взаємодію із об’єктами навколишнього природного середовища;
- джерела, фактори, матеріали, речовини, продукцію, енергію, фізичні фактори (шум, вібрацію, електромагнітне випромінювання, радіацію), які впливають або можуть вплинути на стан навколишнього природного середовища та здоров’я людей;
- загрозу виникнення і причини надзвичайних екологічних ситуацій, результати ліквідації цих явищ, рекомендації щодо заходів, спрямованих на зменшення їх негативного впливу на природні об’єкти та здоров’я людей;
- екологічні прогнози, плани і програми, заходи, в тому числі адміністративні, державну екологічну політику, законодавство про охорону навколишнього природного середовища;
- витрати, пов’язані із здійсненням природоохоронних заходів за рахунок фондів охорони навколишнього природного середовища, інших

джерел фінансування, економічний аналіз, проведений у процесі прийняття рішень з питань, що стосуються довкілля.

Основними джерелами такої інформації є дані моніторингу довкілля, кадастрів природних ресурсів, реєстри, автоматизовані бази даних, архіви, а також довідки, що видаються уповноваженими на те органами державної влади, органами місцевого самоврядування, окремими посадовими особами. Корисним інструментом для отримання екологічної інформації та здійснення громадськістю контролю у сфері охорони довкілля є Інспекційний портал (inspections.gov.ua), який є пілотним модулем системи заходів державного нагляду (контролю). Зазначений ресурс містить багато важливої інформації, зокрема відомості про заходи державного нагляду (контролю), їх результати, плани комплексних заходів державного контролю на майбутній період, документи інспекційного характеру.

Існує багато джерел екологічної інформації, які можна використовувати для отримання оновленої та достовірної інформації про стан навколишнього середовища. Ось декілька основних джерел:

Greenpeace:

Основна мета: Greenpeace є міжнародною неприбутковою організацією, яка працює для захисту природи та екології. Вони активно займаються питаннями ядерної енергії, збереженням лісів, кліматом, забрудненням води та багатьма іншими екологічними проблемами.

Environmental Protection Agency (EPA) (США)

Основна мета: EPA в Сполучених Штатах відповідає за регулювання та захист навколишнього середовища. Вони ведуть наукові дослідження, розробляють стандарти та здійснюють моніторинг стану навколишнього середовища.

United Nations Environment Programme (UNEP):

Основна мета: Програма ООН з питань навколишнього середовища координує глобальні зусилля у сфері охорони природи та екології. Вони також проводять дослідження, розробляють стратегії та сприяють міжнародній співпраці для розв'язання екологічних проблем.

Nature та Science (наукові журнали): Основна мета: Nature та Science є одними з найавторитетніших наукових журналів у світі. Вони публікують оригінальні дослідження та огляди з різних наукових галузей, включаючи екологію.

National Geographic - Environment: Основна мета: National Geographic вивчає та висвітлює різноманіття природи, культур та наукових відкриттів. Розділ "Environment" фокусується на екологічних проблемах та зусиллях з їх вирішення.

Ці джерела можуть надати різнобічну та глибоку інформацію про стан навколишнього середовища, актуальні екологічні питання та наукові

досягнення в цій галузі. Завжди слід перевіряти актуальність та достовірність інформації, особливо при вивченні екологічних питань.

Екологічна інформація є важливою складовою діяльності ЕПЛ, оскільки вона є водночас і необхідним джерелом знань, і важливим надбанням, і передумовою та запорукою ефективності еколого-правового руху. Цей напрямок включає інформування громадян шляхом надання консультацій, пошук, аналіз і розповсюдження еколого-правових новин, публікацію журналу "Екологія-Право-Людина", функціонування бібліотеки, видання інформаційно-аналітичних публікацій, функціонування веб-сторінки та співпрацю із ЗМІ.

Розповсюдження щоденних новин відбувається через електронні списки розсилки, на які підписані члени і партнери організації. Списки розсилки дозволяють отримувати найновішу і актуальнішу інформацію, включаючи важливі статистичні дані, результати наукових екологічно-правових досліджень, новини законодавства.

Журнал "Екологія-Право-Людина" є важливим засобом розповсюдження еколого-правової інформації серед екологів, юристів, студентів та зацікавленої громадськості. Маючи широку тематичну гаму, яка включає проблеми природно-заповідного фонду, доступу до екологічної інформації, права людини та ін., журнал є потужним джерелом інформації, а також форумом для обговорення цих проблем.

Бібліотека ЕПЛ здійснює збір матеріалів на екологічну та еколого-правову тематику, систематизацію літератури, слідкує та забезпечує постійне оновлення фонду бібліотеки, інформує про нові надходження до бібліотеки, займається розповсюдженням літератури, веде листування з користувачами бібліотеки, формує галузевий поділ матеріалів, формує бази даних з матеріалів бібліотеки, розробляє та постійно підтримує каталог бібліотеки; веде реєстр відвідувачів, видає та приймає літературу.

Бібліотека ЕПЛ містить екологічні публікації (книги, монографії, журнали, систематизовані газетні статті на тему екології та охорони довкілля),

національні еколого-правові публікації (законодавство, коментарі законодавства, статті, журнали), міжнародні публікації (про міжнародні аспекти охорони довкілля, про національне екологічне законодавство і практику охорони довкілля за кордоном, про міжнародні організації в сфері охорони довкілля, а також відеотеку, до якої входять найвідоміші фільми на екологічну тематику.

ЕПЛ активно працює в напрямку інформування про національне та міжнародне законодавство у сфері екології і видає публікації, які містять аналіз та коментування міжнародних угод, а також аналітичні публікації на різні теми, як наприклад, доступ до інформації чи доступ до правосуддя.

Важливим засобом інформування також є веб-сторінка ЕПЛ, яка містить новини еколого-правового руху та новини екологічного законодавства.

Для оптимізації інформування громадян ЕПЛ співпрацює із ЗМІ, завдяки яким екологічна інформація набуває широкого розповсюдження. Щороку ЕПЛ дає десятки радіо і телеінтерв'ю, пише репортажі для регіональних та національних газет, журналів та вісників, бере участь у прес-конференціях.

ВИСНОВКИ

У ході обговорення було розглянуто різні аспекти інформаційної безпеки в банківському секторі. Важливість заходів забезпечення інформаційної безпеки в банку визначається необхідністю захисту конфіденційної інформації, що стосується клієнтів, фінансових операцій та багатьох інших аспектів діяльності.

Системність заходів інформаційної безпеки передбачає високий ступінь захищеності інформації, охоплення всіх інформаційних ресурсів, планову та безперервну діяльність забезпечення безпеки. Важливо дотримуватися принципів законності, повноти і розумності захисту інформації.

Політика банку відіграє ключову роль у забезпеченні інформаційної безпеки, будуючи систему захисту на основі прийнятих правил, стандартів та організаційних заходів. Принципи повної участі та особистої відповідальності, а також превентивних заходів важливі для ефективного функціонування системи захисту інформації.

Нормативно-правова база банку щодо захисту інформації включає зобов'язання співробітників, договори про конфіденційність та внутрішні робочі процеси. Створення нормативно-правового фонду є основою для правової охорони інформації та діяльності банку.

У сучасних умовах, де інформаційні технології відіграють важливу роль, забезпечення безпеки інформації банку визначається необхідністю застосування технологічних та логічних заходів, системності та комплексності заходів безпеки.

Важливою частиною системи безпеки є також нормативні акти, які визначають режими конфіденційності та відповідальність за порушення заходів захисту. Крім того, розглянуті підсистеми захисту інформації в локальних мережах, загальний підхід до забезпечення безпеки при звільненні працівників та важливість проведення оцінки ризиків системи безпеки.

У порівняльному аналізі SIEM систем, таких як QRadar та Wazuh, було розглянуто їхні характеристики та функціональність. Ці системи відіграють важливу роль у виявленні, моніторингу та реагуванні на інциденти в області кібербезпеки.

Підведемо підсумок ми можемо зрозуміти що кібербезпекав наш час дуже важлива івказує на важливість комплексного підходу до захисту інформації в банку, враховуючи її чутливість, широкий спектр загроз і постійні технологічні зміни. Реалізація ефективної системи безпеки вимагає відповідальності, системності та використання передових технологій та методик.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. МОНІТОРИНГ ТА УПРАВЛІННЯ ІНЦИДЕНТАМИ КІБЕРБЕЗПЕКИ. Довбак В.Й. https: //phys.donnu.edu.ua/wp-content/uploads/sites/10/2020/02/125_kiberbezpeka_vk-9-dv-4_monitoryng-ta-upravlinnya-inczydentamy-kiberbezpeky.pdf

2. Методичні рекомендації щодо управління операційним ризиком в банку https: //bank.gov.ua/admin_uploads/article/%D0%9C%D0%B5%D1%82%D0%BE%D0%B4%D0%B8%D1%87%D0%BD%D1%96_%D1%80%D0%B5%D0%BA%D0%BE%D0%BC%D0%B5%D0%BD%D0%B4%D0%B0%D1%86%D1%96%D1%97_%D1%89%D0%BE%D0%B4%D0%BE_%D1%83%D0%BF%D1%80%D0%B0%D0%B2%D0%BB%D1%96%D0%BD%D0%BD%D1%8F_%D0%BE%D0%BF%D0%B5%D1%80%D0%B0%D1%86%D1%96%D0%B9%D0%BD%D0%B8%D0%BC_%D1%80%D0%B8%D0%B7%D0%B8%D0%BA%D0%BE%D0%BC_%D0%BE%D0%BF%D1%96.pdf?v=4

3. Державна служба спеціального звязку та захисту інформації https: //cip.gov.ua/ua/news/uryad-zatverdiv-poryadok-reaguvannya-na-kiberincidenti-ta-kiberataki

4. С. Толюпа, Є. Толюпа, Є. Агапова / Вплив кібернетичних атак на інформаційну систему // Педагогічні інновації: ідеї, реалії, перспективи. - 2017. - Вип. 2. - С. 83-87

5. Система моніторингу https: //techexpert.ua/it-monitoring/

6. Налаштування SIEM системи Qradar - https: //www.ibm.com/qradar

7. Security Development Lifecycle Threat Modeling Adam Shostack; 2014 год - https: //www.amazon.com/Threat-Modeling-Designing-Adam-Shostack/dp/1118809998

8. The art of computer virus research and defence Peter Szoh 2005 - https: //www.amazon.com/The-Computer-Virus-Research-Defense/dp/0321304543/

9. Security information menegment - https: //www.techtarget.com/searchsecurity/definition/security-information-management-SIM

10. Богуш В.М моніторинг та аудит КБ 1-2 розділ

11. Руководство ISO/IEC 73: 2002,Менеджмент рисков - Словарь-Рекомендации для использования встандартах

12. NIST Special Publication 800-12, An Introduction to Computer Security: The NISTHandbook

13. «Cybersecurity for Indusrty». URL - https: //new.siemens.com/global/en/products/automation/topic-areas/industrial-security.html?gclid=CjwKCAjwzNOaBhAcEiwAD7Tb6LDdxy_jWlkQ9jSg_iLiRYZFGJ8vQDt93gMfVueCnH1fYGwvp hQPXRoC6c4QAvD_BwE&acz=3

14. Security information about siem https: //uk.wikipedia.org/wiki/Security_information_and_event_management_(SIEM)

15. Computer security https: //en.wikipedia.org/wiki/Computer_security

16. Virus - https: //www.eset.com/ua/support/information/entsiklopediya-ugroz/kompyuternyy-virus/

17. Dos and DDos attack - https: //uk.wikipedia.org/wiki/DoS-%D0%B0%D1%82%D0%B0%D0%BA%D0%B0

18. Cookie - https: //en.wikipedia.org/wiki/HTTP_cookie

19. Фішинг та види атак - https: //ru.wikipedia.org/wiki/%D0%A4%D0%B8%D1%88%D0%B8%D0%BD%D0%B3

20. Api (інтерфейс програмування застосунків, інтерфейс прикладного програмування) - https: //uk.wikipedia.org/wiki/%D0%9F%D1%80%D0%B8%D0%BA%D0%BB%D0%B0%D0%B4%D0%BD%D0%B8%D0%B9_%D0%BF%D1%80%D0%BE%D0%B3%D1%80%D0%B0%D0%BC%D0%BD%D0%B8%D0%B9_%D1%96%D0%BD%D1%82%D0%B5%D1%80%D1%84%D0%B5%D0%B9%D1%81

21. APi в банках настройка та підключення - https://habr.com/ru/articles/702106/

22. APi в qradar ta defender xdr - https: //learn.microsoft.com/ru-ru/microsoft-365/security/defender-endpoint/configure-siem?view=o365-worldwide

23. Прикладни́й програ́мний інтерфе́йс у web - https://uk.wikipedia.org/wiki/%D0%9F%D1%80%D0%B8%D0%BA%D0%BB%D0%B0%D0%B4%D0%BD%D0%B8%D0%B9_%D0%BF%D1%80%D0%BE%D0%B3%D1%80%D0%B0%D0%BC%D0%BD%D0%B8%D0%B9_%D1%96%D0%BD%D1%82%D0%B5%D1%80%D1%84%D0%B5%D0%B9%D1%81#%D0%9F%D1%80%D0%B8%D0%BA%D0%BB%D0%B0%D0%B4%D0%BD%D0%B8%D0%B9_%D0%BF%D1%80%D0%BE%D0%B3%D1%80%D0%B0%D0%BC%D0%BD%D0%B8%D0%B9_%D1%96%D0%BD%D1%82%D0%B5%D1%80%D1%84%D0%B5%D0%B9%D1%81_%D1%83_WEB

24. Методи боротьби - https://uk.wikipedia.org/wiki/DoS-%D0%B0%D1%82%D0%B0%D0%BA%D0%B0#%D0%9C%D0%B5%D1%82%D0%BE%D0%B4%D0%B8_%D0%B1%D0%BE%D1%80%D0%BE%D1%82%D1%8C%D0%B1%D0%B8

25. HTTP - https://uk.wikipedia.org/wiki/DoS-%D0%B0%D1%82%D0%B0%D0%BA%D0%B0#HTTP-%D1%84%D0%BB%D1%83%D0%B4

26. Ботнет - https://uk.wikipedia.org/wiki/%D0%91%D0%BE%D1%82%D0%BD%D0%B5%D1%82

27. Механізм маскування ботнету - https://uk.wikipedia.org/wiki/%D0%91%D0%BE%D1%82%D0%BD%D0%B5%D1%82#%D0%9C%D0%B5%D1%85%D0%B0%D0%BD%D1%96%D0%B7%D0%BC_%D0%BC%D0%B0%D1%81%D1%83%D0%B2%D0%B0%D0%BD%D0%BD%D1%8F

28. Siem системи - https://uk.wikipedia.org/wiki/Security_information_and_event_management_(SIEM)

29. Security information and event management - https://ru.wikipedia.org/wiki/SIEM

30. API - https://uk.wikipedia.org/wiki/IPA_(%D0%B7%D0%BD%D0%B0%D1%87%D0%B5%D0%BD%D0%BD%D1%8F)

31. Інформаційна безпека банку - http://obt.inf.ua/page10.html

32. Політика інформаційної безпеки банку - https://www.oschadbank.ua/uploads/0/385-politika_ib.pdf

33. Кібератаки - https://uk.wikipedia.org/wiki/%D0%A5%D0%B0%D0%BA%D0%B5%D1%80%D1%81%D1%8C%D0%BA%D0%B0_%D0%B0%D1%82%D0%B0%D0%BA%D0%B0

34. Кібератаки - https://uk.wikipedia.org/wiki/%D0%9F%D0%B5%D1%80%D0%B5%D0%BB%D1%96%D0%BA_%D0%BA%D1%96%D0%B1%D0%B5%D1%80%D0%B0%D1%82%D0%B0%D0%BA

35. Інформаційна безпека банку Агріколь - https://credit-agricole.ua/o-banke/security