ДЕРЖАВНИЙ УНІВЕРСИТЕТ ІНФОРМАЦІЙНО-ТЕЛЕКОМУНІКАЦІЙНИХ ТЕХНОЛОГІЙ
НАВЧАЛЬНО-НАУКОВИЙ ІНСТИТУТ ЗАХИСТУ ІНОРМАЦІЇ

КАФЕДРА ІНФОРМАЦІЙНОЇ ТА КІБЕРНЕТИЧНОЇ БЕЗПЕКИ

КВАЛІФІКАЦІЙНА РОБОТА

на тему:

«Технологія виявлення загрозливої діяльності і поведінки в ІТ середовищі»

на здобуття освітнього ступеня магістра
зі спеціальності ____125 Кібербезпека_____
(код, найменування спеціальності)
освітньо-професійної програми _Інформаційна та кібернетична безпека_
(назва)

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

Виконав: здобувач вищої освіти групи БСДМ-61
Бугаєнко Нікіта Костянтинович
(ПРИЗВІЩЕ ім'я)
Керівник: _____
(ПРИЗВІЩЕ ім'я)
Рецензент _____
(ПРИЗВІЩЕ ім'я)

КИЇВ – 2024

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

Інформаційної та кібернетичної безпеки

Ступінь вищої освіти Магістр

Спеціальність 125 Кібербезпека

Освітньо-професійна програма Інформаційна та кібернетична безпека

ЗАТВЕРДЖУЮ
Завідувач кафедри ІКБ
_____ Галина ГАЙДУР
“___”_____ 2023 року

З А В Д А Н Н Я
НА КВАЛІФІКАЦІЙНУ РОБОТУ

Бугаєнку Нікіті Костянтиновичу
(прізвище, ім’я, по батькові)

1. Тема кваліфікаційної роботи:
«Технологія виявлення загрозливої діяльності і поведінки в ІТ середовищі»
керівник кваліфікаційної роботи: ГАЙДУР Галина, д.т.н., професор,
(ПРІЗВИЩЕ, Ім’я, науковий ступінь, вчене звання)
затверджені наказом Державного університету інформаційно-комунікаційних технологій від «19» жовтня 2023р. №145.

2. Строк подання студентом кваліфікаційної роботи: 15.12.2023 р.

3. Вихідні дані до кваліфікаційної роботи_____

4. Зміст розрахунково-пояснювальної записки (перелік питань, які потрібно розробити)_____

5. Перелік графічного матеріалу_____

6. Дата видачі завдання__.__.20__р

КАЛЕНДАРНИЙ ПЛАН

№ з/п	Назва етапів магістерської роботи	Строк виконання етапів магістерської роботи	Примітка
1.			
2.			
3.			
4.			
5.			
6.			

Студент _____ _____
(підпис) (прізвище та ініціали)

Керівник магістерської роботи
(підпис) (прізвище та ініціали)

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

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

Направляється здобувач Бугаєнко Н.К. до захисту кваліфікаційної роботи
(прізвище та ініціали)

За спеціальністю 125 Кібербезпека
освітньо-професійної програми Інформаційна та кібернетична безпека
(шифр і назва спеціальності)

на тему: «Технологія виявлення загрозливої діяльності і поведінки в ІТ середовищі».

Кваліфікаційна робота і рецензія додаються.

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

Висновок керівника кваліфікаційної роботи

Керівник кваліфікаційної роботи _____ Галина ГАЙДУР
(підпис) *(Ім'я, ПРІЗВИЩЕ)*
"____" _____ 2023 року

Висновок кафедри про кваліфікаційну роботу

ВІДГУК РЕЦЕНЗЕНТА
на кваліфікаційну роботу

РЕФЕРАТ

Текстова частина магістерської роботи:

Об'єктом магістерської роботи є ІТ-системи та організації, які є потенційними цілями кібератак. *Предметом* роботи є технологія виявлення загрозливої діяльності і поведінки в ІТ середовищі. *Метою* магістерської роботи є дослідження технології виявлення загрозливої діяльності і поведінки в ІТ середовищі.

У роботі будуть використані такі *методи* дослідження, як:

- Аналіз та синтез наукової літератури з даної проблематики.
- Порівняльно-історичний аналіз.
- Описовий аналіз.

У роботі розглянуто теоретичні основи виявлення загрозливої діяльності і поведінки в ІТ середовищі. Визначені основні тенденції розвитку загрозливої діяльності і поведінки в ІТ середовищі. Проаналізовані принципи роботи APT-атак та технології їх виявлення. Визначені фактори, що впливають на загрозливу діяльність і поведінку. Розроблені рекомендації щодо виявлення та запобігання сучасним стійким загрозам. Результати дослідження можуть бути використані в практичній діяльності для підвищення ефективності захисту ІТ-систем і організацій від загрозливої діяльності і поведінки.

Галузь використання – безпека ІТ-систем.

ТЕХНОЛОГІЇ ВИЯВЛЕННЯ, ЗАГРОЗЛИВА ДІЯЛЬНІСТЬ, ПОВЕДІНКА, ІТ СЕРЕДОВИЩЕ, APT-АТАКА, ВРАЗЛИВІСТЬ, ШКІДЛИВЕ ПРОГРАМНЕ ЗАБЕЗПЕЧЕННЯ.

ЗМІСТ

ПЕРЕЛІК УМОВНИХ ПОЗНАЧЕНЬ

ІТ - скорочення від "інформаційні технології". Це галузь, що займається розробкою, створенням, використанням та обслуговуванням інформаційних систем.

DoS-атака - це тип атаки, яка спрямована на блокування доступу до ресурсу або сервісу.

ШІ - скорочення від "штучний інтелект". Це галузь інформатики, яка займається розробкою інтелектуальних агентів - систем, які можуть мислити та діяти самостійно.

МН - скорочення від "машинне навчання". Це галузь штучного інтелекту, яка займається розробкою алгоритмів, які можуть навчатися на даних без попереднього програмування.

IoT - скорочення від "інтернет речей". Це мережа фізичних об'єктів, які оснащені датчиками та можуть взаємодіяти один з одним та з зовнішнім світом за допомогою Інтернету.

APT - скорочення від "advanced persistent threat". Це тип атаки, яка проводиться кваліфікованими хакерами з тривалим терміном проведення.

СПЗ - скорочення від "сучасні постійні загрози". Це синонім терміну "APT".

VA/PT - скорочення від "vulnerability assessment and penetration testing". Це процес оцінки вразливостей систем та мереж та тестування їх на проникнення з метою виявлення та усунення можливих загроз.

SOC - скорочення від "security operations center". Це центр обробки даних, який займається моніторингом безпеки та реагуванням на інциденти.

ВСТУП

Актуальність дослідження. У сучасному світі, який характеризується цифровізацією та глобалізацією, IT-системи та мережі стали життєво важливими для діяльності підприємств, організацій та державних установ. Однак, разом із цим, IT-системи стали більш вразливими до загроз, таких як кібератаки, шпигунство та ін. Одним із найсерйозніших видів загроз є стійкі загрози (APTs), які являють собою комплексні атаки, спрямовані на конкретну ціль і організовані та фінансуються професійними групами хакерів. APT-атаки часто спрямовані на заволодіння конфіденційною інформацією, крадіжку інтелектуальної власності або порушення роботи критичної інфраструктури.

Виявлення APT-атак є складним завданням, оскільки вони часто маскуються під звичайну діяльність користувачів або систем. Для успішного виявлення APT-атак необхідно використовувати комплекс технологій, які дозволяють аналізувати широкий спектр даних, включаючи трафік мережі, поведінку користувачів та системні події.

Ступінь наукової розробки. Питання виявлення загрозливої діяльності і поведінки в IT середовищі є предметом дослідження багатьох науковців і фахівців у сфері IT-безпеки. У науковій літературі представлено широкий спектр підходів до виявлення загроз, а також різні технології, які можуть бути використані для цього. Однак, незважаючи на значний прогрес у цій галузі, проблема виявлення загрозливої діяльності і поведінки в IT середовищі залишається актуальною. Це пов'язано з тим, що загрози постійно розвиваються, а також з тим, що складно виявити загрози, які є добре замасковані.

Практичне значення одержаних результатів. Отримані результати магістерської роботи мають значне практичне значення і можуть бути використані для підвищення ефективності захисту ІТ-систем і організацій від загрозливої діяльності і поведінки.

1 ТЕОРЕТИЧНІ ОСНОВИ ВИЯВЛЕННЯ ЗАГРОЗЛИВОЇ ДІЯЛЬНОСТІ І ПОВЕДІНКИ В ІТ СЕРЕДОВИЩІ

1.1. Аналіз поняття ІТ середовища

Поняття ІТ середовища охоплює широкий спектр аспектів, пов'язаних з використанням інформаційних технологій. Воно включає технічні, програмні, організаційні та людські ресурси, що використовуються для обробки, створення, зберігання та передачі інформації. ІТ середовище може бути статичним, з незмінними компонентами, або динамічним, що постійно змінюється під впливом внутрішніх та зовнішніх факторів.

Внутрішні фактори, які впливають на ІТ середовище, включають стратегічні цілі організації, організаційні структури, людські та фінансові ресурси. Зовнішні фактори охоплюють законодавство, технологічні зміни, конкурентне середовище, а також соціальні та культурні аспекти. Аналіз ІТ середовища дозволяє оцінити його поточний стан, виявити можливості та ризики, а також розробити стратегію розвитку. Для цього можуть використовуватися методи аналізу документів, інтерв'ю з експертами, опитування користувачів та соціологічні дослідження.

На сьогоднішній день термін "інформаційні технології" переважно асоціюється з комп'ютерними системами та програмним забезпеченням. ІТ включають використання комп'ютерів для збору, обробки, перетворення, зберігання, захисту та передачі інформації, задовольняючи інформаційні потреби користувачів. Основною метою ІТ є створення якісного інформаційного продукту, який відповідає запитам користувача. Глобалізація світової економіки та розвиток інформаційного простору призвели до зростання інтенсивності інформаційних потоків, що пояснює швидкий розвиток ІТ у всьому світі. Управління інформацією

займає значну частину часу в управлінській діяльності, тому інформаційне забезпечення є ключовим.

Зростання обсягів інформації про взаємодії на ринку вимагає поліпшення ІТ. Розвиток ринкових відносин породив маркетинг взаємодії, базований на комунікаційних процесах. Це призвело до появи нового терміну – "інформаційно-комунікаційні технології" (ІКТ), який включає телекомунікації, комп'ютери, програмне забезпечення та аудіовізуальні системи, забезпечуючи користувачів можливістю створення, доступу, зберігання, передачі та модифікації інформації.

ІКТ об'єднують методи, процеси та технічні засоби для роботи з даними, включаючи ІТ та телекомунікації, медіа-трансляції, різні види аудіо- та відеообробки, мережеві функції управління та моніторингу. Інформаційні технології, як процес, базуються на чітко регламентованих правилах і залежать від багатьох факторів, класифікованих за ступенем централізації, предметною областю, обсягом управлінських завдань, класом технологічних операцій, типом користувацького інтерфейсу, способом побудови мережі та реалізації в інформаційній системі. Централізовані, децентралізовані та комбіновані технології в ІТ демонструють різні підходи до оброблення інформації. Централізовані технології фокусуються на центральному сервері, децентралізовані – на локальному застосуванні засобів обчислювальної техніки, а комбіновані інтегрують ці процеси з використанням спільних баз даних.

Інформаційно-комунікаційні технології сьогодні стають все більш інтегрованими, поєднуючи роботу з інформацією та живу комунікацію, і в цьому контексті комп'ютери відіграють ключову роль, забезпечуючи гнучку, індивідуалізовану та інтелектуальну взаємодію. У будь-якому сучасному офісі в Україні неможливо обійтися без комп'ютерної техніки. Навіть компанії, які не спеціалізуються на ІТ, часто мають у своєму складі працівника, компетентного в комп'ютерних системах, що підкреслює важливість ІТ-спеціалістів. Актуальність інформаційних технологій у сфері освіти в Україні зростає, що відображається у збільшенні спеціалізацій університетів, написанні сучасних навчальних матеріалів

і розвитку онлайн-ресурсів. Студенти мають можливість дистанційно знайомитися з університетами, оцінюючи інформацію віддалено.

Україна пишається своїм значним числом програмістів, що перевищує цей показник у більшості європейських країн. Однак існує нерівномірність у популярності ІТ-спеціалістів серед роботодавців, особливо в галузях, які користуються високим попитом, наприклад, розробка веб- та мобільних додатків. Галузь інформаційних технологій в Україні - це динамічно змінюване середовище, наповнене інноваціями та різноманітними проектами. Ринок праці у цій сфері росте, і попит на кваліфікованих фахівців зростає з кожним роком.

Термін "інформаційні технології" (ІТ) охоплює різні аспекти, включаючи обробку інформації, новітні методи та інструменти управління економікою. Це може включати процеси обробки даних, створення та використання інструментів і технологій індустрії [1]. Основні принципи нової інформаційної технології (НІТ) включають інтегрованість, гнучкість та інформативність, а її особливості - робота в режимі маніпулювання даними, цілковита інформаційна підтримка та без паперовий обіг документів. У сфері економіки використовуються різні типи ІТ, такі як обробка даних, управління та підтримка прийняття рішень. Ці технології спрямовані на автоматизацію рутинних операцій управлінської праці та задоволення інформаційних потреб різних суб’єктів економіки. Розширення можливостей використання інформаційних технологій в різних сферах суспільства та управління, вирішення економічних завдань і посилення процесів економічної інтеграції, а також трансформація економічних відносин стають можливими завдяки їх класифікації [1]. Класифікація використовує показники, такі як спосіб реалізації в автоматизованих системах, ступінь охоплення завдань управління, клас технологічних операцій, тип користувацького інтерфейсу, спосіб побудови мережі ЕОМ та предметна область обслуговування. Крім того, враховуються ознаки взаємодії між інформаційними технологіями, такі як дискретна і мережева взаємодія, різні варіанти обробки й зберігання даних, розподілена інформаційна база та обробка даних.

Загрозливі дії та поведінка в IT-середовищі - це будь-які дії або наміри, які потенційно можуть завдати шкоди або порушити роботу комп'ютерних систем, мереж або даних. Ці загрози можуть надходити з різних джерел, включаючи як внутрішніх, так і зовнішніх суб'єктів. Внутрішні загрози надходять від осіб, які мають санкціонований доступ до IT-систем організації. Це можуть бути незадоволені працівники, колишні працівники або навіть підрядники [15]. Вони можуть діяти зі злого умислу, недбалості або просто через нерозуміння політики безпеки. Зовнішні загрози походять від осіб або груп, які не мають санкціонованого доступу до IT-систем організації. Це можуть бути хакери, кіберзлочинці або навіть національні держави. Вони можуть бути мотивовані фінансовою вигодою, шпигунством або просто бажанням спричинити збій в роботі. Загрозливі дії та поведінку в IT-середовищі можна класифікувати за кількома різними категоріями, зокрема:

1. Несанкціонований доступ: Це стосується будь-якої спроби отримати доступ до IT-системи без дозволу. Це може включати використання викрадених облікових даних, використання вразливостей або фізичний обхід засобів контролю безпеки.

2. Порушення даних: Це стосується несанкціонованого доступу, розкриття, отримання або знищення конфіденційних даних. Це може включати особисту інформацію, фінансову документацію або інтелектуальну власність.

3. Атаки на відмову в обслуговуванні (DoS): Ці атаки спрямовані на те, щоб перевантажити систему трафіком або запитами, роблячи її недоступною для законних користувачів.

4. Атаки шкідливих програм: Шкідливе програмне забезпечення - це програмне забезпечення, призначене для завдання шкоди комп'ютерній системі. Це можуть бути віруси, хробаки, троянські програми, програми-вимагачі та шпигунські програми.

5. Атаки соціальної інженерії: Ці атаки покладаються на те, щоб обманом змусити людей розкрити конфіденційну інформацію або вжити заходів, які можуть поставити під загрозу безпеку.

IT-середовище постійно розвивається, як і загрози, з якими стикаються організації. Хакери та кіберзлочинці стають все більш витонченими і постійно розробляють нові способи атак на IT-системи. Кібербезпека - це практика захисту IT-систем, мереж і даних від несанкціонованого доступу, використання, розкриття, порушення, модифікації або знищення [8]. Кібербезпека має важливе значення для організацій будь-якого розміру, і вона повинна бути головним пріоритетом для всіх керівників і менеджерів. Крім того, зростаюче використання хмарних обчислень і мобільних пристроїв створило нові вектори атак, про які організаціям необхідно знати. Загрозливі дії та поведінка в IT-середовищі можуть мати значний вплив на організації. Витоки даних можуть призвести до втрати конфіденційної інформації про клієнтів, що може зашкодити репутації організації та призвести до фінансових втрат. DoS-атаки можуть порушити роботу організації та призвести до значних фінансових втрат. Атаки шкідливих програм можуть пошкодити IT-системи та дані організації, а також призвести до фінансових втрат [5]. Мотиви загрозливої діяльності та поведінки в IT-середовищі можуть відрізнятися залежно від суб'єкта. Однак, деякі з найпоширеніших мотивів включають:

- Фінансова вигода: Хакери та кіберзлочинці часто націлені на організації з метою викрадення грошей або фінансової інформації.
- Шпигунство: Національні держави та інші організації можуть займатися кібершпигунством, щоб викрасти конфіденційну інформацію у своїх конкурентів.
- Порушення роботи: Деякі особи або групи можуть здійснювати кібератаки просто для того, щоб викликати дезорганізацію або хаос.
- Зловмисність: окремі особи можуть здійснювати кібератаки на організації зі злого умислу або з метою помсти.

Характер загрозливої діяльності та поведінки в IT-середовищі постійно змінюється, оскільки з'являються нові технології, а зловмисники розробляють нові методи [8]. Деякі з останніх тенденцій включають:

- Використання штучного інтелекту (ШІ) і машинного навчання (МН): Зловмисники все частіше використовують ШІ та МН для автоматизації атак і ускладнення їх виявлення та захисту від них.
- Поширення програм-вимагачів: Програми-вимагачі - це тип шкідливого програмного забезпечення, яке шифрує дані організації і вимагає викуп в обмін на ключ до розшифровки.
- Націленість на ланцюги поставок: Зловмисники все частіше націлюються на ланцюги поставок, щоб отримати доступ до організацій, що знаходяться нижче за течією. Організаціям необхідно застосовувати проактивний підхід до безпеки, впроваджуючи надійні засоби контролю безпеки, навчаючи співробітників і маючи план реагування на інциденти безпеки. Загрозлива діяльність і поведінка в ІТ-середовищі охоплює широкий спектр дій, які можуть завдати шкоди інформаційним системам, даним або користувачам. Серед таких дій виділяються кібератаки, шахрайство, шпигунство, розповсюдження шкідливого програмного забезпечення, фішинг, атаки на кінцеві точки, незаконний доступ до даних та інші види зловмисної діяльності. Однією з найскладніших форм кіберзагроз є APT-атаки (Advanced Persistent Threats), які представляють собою тривалі та цілеспрямовані атаки, що виконуються досвідченими зловмисниками, часто з підтримкою держав. Ці атаки характеризуються високою ступенем скритності та витонченості. Зазвичай вони мають на меті крадіжку даних або шпигунство та можуть тривати місяцями або навіть роками, перш ніж будуть виявлені.

Для вирішення проблеми загрозливої діяльності в ІТ-середовищі, організації застосовують різноманітні методи та засоби. Одним з ключових елементів є реалізація комплексної стратегії кібербезпеки, яка включає захист інфраструктури, виявлення та реагування на інциденти, а також відновлення після атак. Це охоплює встановлення захисних систем, таких як брандмауери, антивірусне та антималварне програмне забезпечення, а також системи виявлення та запобігання вторгненням (IDS/IPS).

Важливим аспектом є також постійний моніторинг та аналіз мережевого трафіку та поведінки систем з метою виявлення незвичайної активності, що може свідчити про кібератаки. Організації також впроваджують політики безпеки, проводять регулярні аудити та тренінги для співробітників, щоб підвищити рівень обізнаності та готовності до реагування на кіберзагрози. Використання шифрування для захисту даних та двофакторної аутентифікації для облікових записів є ще одним важливим кроком у захисті від несанкціонованого доступу та витоку інформації. Крім того, організації часто співпрацюють зі спеціалізованими компаніями з кібербезпеки для отримання експертної підтримки та консультацій.

У цілому, ефективний захист від загрозливої діяльності в IT-середовищі вимагає багаторівневого підходу, що включає технологічні, організаційні та освітні аспекти.

1.2. Аналіз поняття загрозливої діяльності і поведінки в IT середовищі

Загрозливі дії та поведінка в IT-середовищі становлять значний і багатогранний виклик для організацій у різних галузях. Наслідки цих загроз можуть бути далекосяжними, спричиняючи фінансові збитки, шкоду репутації, юридичні зобов'язання та операційні перебої. Змінний характер кіберзагроз вимагає від організацій постійної пильності, проактивних заходів безпеки та навчання співробітників для розпізнання та зменшення загроз. Зловмисники, поєднуючи різні методи атак, здатні проникати в системи і завдати значної шкоди, створюючи складний ландшафт кібербезпеки. Методи атак включають соціальну інженерію, шкідливе програмне забезпечення, атаки на ланцюги постачання, програми-вимагачі та використання ШІ для атак на відмову в обслуговуванні. Організації повинні використовувати багаторівневі захисні системи, регулярно навчати співробітників, застосовувати підхід нульової довіри, використовувати

аналітику загроз та мати чіткі плани реагування на інциденти для ефективного протистояння різноманітним і складним кіберзагрозам.

Щоб повністю зрозуміти вплив цих загроз, важливо заглибитися в їхні конкретні наслідки та дослідити заходи, яких організації можуть вжити для зменшення цих ризиків.

- Фінансові наслідки: Багатогранний тягар

Фінансові наслідки загрозливої діяльності та поведінки часто є найбільш безпосереднім і відчутним занепокоєнням для організацій. Витоки даних, DoS-атаки та зараження шкідливим програмним забезпеченням можуть призвести до значних фінансових втрат [26].

1. Витрати на відновлення даних: Після витоку даних організації стикаються зі складним завданням відновлення втрачених або пошкоджених даних. Цей процес часто вимагає спеціальних знань, складних інструментів і значних витрат часу. Витрати, пов'язані з відновленням даних, можуть бути непомірними, особливо для організацій, які обробляють великі обсяги конфіденційних даних.

2. Втрата продуктивності: Інциденти безпеки можуть призвести до зупинки бізнес-операцій, що призводить до втрати продуктивності та доходів. Співробітники можуть бути не в змозі отримати доступ до критично важливих систем або ефективно виконувати свої завдання під час або після атаки. Такий простій може призвести до втрати продажів, недотримання дедлайнів і зниження операційної ефективності.

3. Судові витрати: Організації мають юридичне зобов'язання захищати свої IT-системи та дані, а невиконання цього зобов'язання може призвести до юридичної відповідальності. Регуляторні органи встановлюють суворі закони про захист даних, і організації можуть зіткнутися зі штрафами, санкціями та судовими позовами, якщо вони порушують ці закони або не забезпечують належний захист конфіденційної інформації. Судові витрати, пов'язані з регуляторними розслідуваннями, судовими позовами та вимогами щодо повідомлення даних, можуть збільшити фінансовий тягар інцидентів, пов'язаних з безпекою.

- Репутаційні збитки: Довготривалий ефект

Вплив загрозливих дій і поведінки виходить за рамки фінансових втрат, часто завдаючи значної шкоди репутації організації [12]. Коли розкривається конфіденційна інформація або відбувається компрометація систем, клієнти можуть втратити впевненість у здатності організації захистити їхні дані та конфіденційність.

- Юридичні зобов'язання: Як орієнтуватися в регуляторному середовищі

Організації стикаються з юридичною відповідальністю, коли вони не можуть належним чином захистити свої IT-системи та дані. Регуляторні органи в різних галузях встановили суворі закони про захист даних, які визначають, як організації обробляють і захищають конфіденційну інформацію. Недотримання цих норм може призвести до:

1. Штрафи та покарання: Регуляторні органи можуть накладати значні штрафи та покарання на організації, які порушують закони про захист даних. Ці штрафи можуть бути значними і мати негативний вплив на фінансові показники організації.

2. Судові позови: Клієнти, працівники та інші зацікавлені сторони можуть подавати позови проти організацій, які не захищають їхні дані. Ці позови можуть призвести до відшкодування збитків, врегулювання та додаткових судових витрат.

3. Регулярні перевірки: Організації, які стикаються з порушеннями безпеки або витоком даних, можуть зіткнутися з підвищеною увагою з боку органів. Ця перевірка може включати в себе розслідування, аудит та додаткові вимоги до дотримання законодавства.

- Операційні збої: Перешкода для безперервності бізнесу

Дії та поведінка загроз можуть порушити роботу організації, перешкоджаючи її здатності ефективно надавати продукти або послуги. Атаки на відмову в обслуговуванні можуть зробити недоступними веб-сайти або додатки, а зараження шкідливим програмним забезпеченням може скомпрометувати критичні системи та зупинити роботу. Ці порушення можуть призвести до[8]

1. Втрати доходів: Коли веб-сайти або додатки недоступні, організації не можуть отримувати дохід від онлайн-продажів або транзакцій. Це може призвести

до значних фінансових втрат, особливо для організацій, які значною мірою покладаються на електронну комерцію або онлайн-сервіси.

2. Незадоволеності клієнтів: Операційні збої можуть призвести до незадоволення та розчарування клієнтів. Клієнти можуть зіткнутися із затримками, скасуванням або відсутністю доступу до критично важливих послуг, що може зашкодити відносинам з клієнтами та підірвати лояльність до бренду.

3. Пошкодженню репутації бренду: Операційні збої можуть також заплямувати репутацію бренду організації. Клієнти можуть сприймати організацію як ненадійну або некомпетентну, якщо вона не в змозі підтримувати послідовну та надійну роботу.

Ось кілька конкретних прикладів того, як дії та поведінка загроз можуть впливати на IT-системи та організації:

Витік даних у компанії роздрібної торгівлі розкриває інформацію про кредитні картки клієнтів, що призводить до значних фінансових втрат компанії через шахрайські платежі та відтік клієнтів. Атака на платформу електронної комерції під час пікового сезону святкових покупок порушує роботу веб-сайту компанії, що призводить до втрати продажів і шкоди репутації.

Шкідливе програмне забезпечення проникає в мережу лікарні, порушуючи догляд за пацієнтами та компрометуючи конфіденційні медичні записи. Через витік даних і припинення надання критично важливих послуг з догляду за пацієнтами лікарня опиняється під пильною увагою законодавчих і регуляторних органів. Організації можуть впроваджувати різні стратегії для пом'якшення впливу загрозливих дій і поведінки:

1. Надійний контроль безпеки: Впровадження брандмауерів, систем виявлення вторгнень та заходів контролю доступу може захистити IT-системи від несанкціонованого доступу та зловмисних атак.

2. Навчання співробітників: Інформування працівників про ризики безпеки та найкращі практики може допомогти запобігти людським помилкам та атакам соціальної інженерії.

3. План реагування на інциденти безпеки: Наявність плану швидкого та ефективного реагування на інциденти безпеки може мінімізувати збитки, спричинені порушенням або атакою.

4. Регулярні перевірки безпеки: Регулярний перегляд та оновлення політик і процедур безпеки може допомогти організаціям випереджати нові загрози та вразливості.

Застосовуючи проактивний підхід до кібербезпеки та постійно адаптуючись до мінливого ландшафту загроз, організації можуть мінімізувати вплив загрозливих дій та поведінки на свої IT-системи та операції.

1.3. Технології виявлення загрозливої діяльності і поведінки в IT середовищі

Технології виявлення загрозливої діяльності та поведінки в IT-середовищі представляють собою комплексний підхід до ідентифікації, аналізу та реагування на потенційні кіберзагрози. Серед основних технологій та методів можна виділити системи виявлення вторгнень та системи запобігання вторгненням, які моніторять мережевий трафік або системні дії для виявлення ознак атак. Безпека кінцевих точок забезпечує захист від шкідливих програм на пристроях користувачів.

Управління подіями та інформацією про безпеку об'єднує дані з різних джерел для виявлення підозрілих дій, забезпечуючи комплексний огляд загроз та їх впливу на IT-інфраструктуру. Віртуалізація безпеки використовує віртуалізовані середовища для ізоляції та аналізу підозрілих програм, зменшуючи ризик поширення шкідливого коду. Шифрування даних допомагає захистити конфіденційність інформації, знижуючи ризики, пов'язані з витоком даних.

Аналіз мережевого трафіку включає моніторинг та аналіз мережевих пакетів, дозволяючи виявляти підозрілі взаємодії та потенційні атаки. Інтелектуальний аналіз загроз збирає та аналізує інформацію про загрози з різних джерел,

допомагаючи краще розуміти та прогнозувати потенційні кібератаки. Ці технології і методи в цілому сприяють створенню міцної та ефективної системи кібербезпеки, адаптованої до постійно змінюваних умов кіберпростору.Оскільки IT-ландшафт продовжує зростати і розвиватися, зростають і загрози, з якими стикаються організації. Щоб бути на крок попереду цих загроз, організаціям необхідно використовувати різноманітні технології для виявлення та реагування на загрозливі дії та поведінку в IT-середовищі.

Аналіз мережевого трафіку (NTA)

NTA - це тип технології безпеки, яка відстежує та аналізує мережевий трафік для виявлення підозрілої активності. Рішення NTA можуть збирати та аналізувати широкий спектр даних, включаючи IP-адреси, номери портів, розміри пакетів і протоколи додатків [43]. Ці дані можна використовувати для виявлення аномалій у мережевому трафіку, які можуть свідчити про атаку.

Аналіз поведінки користувачів і організацій (UBA)

UEBA - це тип технології безпеки, яка відстежує поведінку користувачів і організацій для виявлення аномалій, які можуть вказувати на зловмисну активність. Рішення UEBA можуть збирати та аналізувати широкий спектр даних, включаючи логіни користувачів, шаблони доступу та використання пристроїв. Ці дані можуть бути використані для виявлення користувачів, які поводяться незвично, наприклад, отримують доступ до конфіденційних даних у неробочий час або намагаються увійти в систему з несанкціонованого місця.

Виявлення та реагування на кінцеві точки (EDR)

EDR - це тип технології безпеки, яка відстежує і захищає кінцеві точки, такі як ноутбуки, настільні комп'ютери і сервери. Рішення EDR можуть виявляти та реагувати на широкий спектр загроз, включаючи шкідливе програмне забезпечення, програми-вимагачі та фішингові атаки. Рішення EDR також можуть збирати та аналізувати дані з кінцевих точок, щоб отримати уявлення про поведінку користувачів та потенційні загрози.

Запобігання втраті даних (DLP)

DLP - це тип технології безпеки, яка запобігає витоку або неправомірному використанню конфіденційних даних. Рішення DLP можуть відстежувати та контролювати рух даних як всередині, так і за межами організації. Рішення DLP також можна використовувати для шифрування конфіденційних даних, щоб захистити їх від несанкціонованого доступу.

Управління інформацією та подіями безпеки (SIEM)

SIEM - це тип технології безпеки, який збирає та аналізує дані про безпеку з різних джерел, таких як брандмауери, системи виявлення вторгнень та кінцеві точки. Рішення SIEM можуть співвідносити ці дані для виявлення інцидентів безпеки та оповіщення про них. Рішення SIEM також можна використовувати для створення звітів і інформаційних панелей, які дають уявлення про ризики безпеки.

Аналітика загроз - це дані про загрози, вразливості та методи атак. Організації можуть використовувати дані про загрози для виявлення потенційних загроз, визначення пріоритетів у забезпеченні безпеки та розробки ефективних стратегій безпеки. Дані про загрози можна отримати з різних джерел, включаючи комерційних постачальників, державні установи та розвіддані з відкритих джерел.

Машинне навчання (ML) і штучний інтелект (AI) [45]

ML і AI використовуються для розробки нових та інноваційних способів виявлення загроз і реагування на них. Наприклад, ML можна використовувати для виявлення аномалій у мережевому трафіку, поведінці користувачів і моделях доступу до даних. ШІ можна використовувати для автоматизації завдань безпеки, таких як реагування на інциденти та полювання на загрози.

Це лише деякі з багатьох технологій, які можна використовувати для виявлення та реагування на загрозливі дії та поведінку в IT-середовищі. Використовуючи різноманітні технології, організації можуть покращити свій стан безпеки та захистити свої IT-активи від широкого спектру загроз. Постійний моніторинг та відстеження загроз

Виявлення загроз - це не одноразова подія, вона вимагає постійного моніторингу та проактивного полювання на загрози. Команди безпеки повинні постійно відстежувати мережевий трафік, поведінку користувачів і шаблони

доступу до даних, щоб виявити підозрілі дії, які можуть свідчити про атаку. Полювання на загрози передбачає проактивний пошук потенційних загроз, які могли вислизнути від традиційних методів виявлення. Такий проактивний підхід може допомогти виявити та припинити атаки до того, як вони зможуть завдати значної шкоди. Організації повинні визначати пріоритети своїх зусиль у сфері безпеки, виходячи з потенційного впливу кожної загрози. Системи управління ризиками, такі як MITRE ATT&CK, можуть допомогти організаціям оцінити ризики, спричинені різними загрозами, і відповідно розставити пріоритети в інвестиціях у безпеку [13].

Сучасні постійні загрози (APT) - це складні кібератаки, спрямовані на конкретні організації або окремих осіб з метою отримання довгострокової вигоди. APT зазвичай здійснюються висококваліфікованими зловмисниками, які добре фінансуються та мають доступ до сучасних інструментів і ресурсів.

- Принципи APT-атак [41]:

Цілеспрямованість: APT-атаки не схожі на традиційні кібератаки, які поширюються масово і без розбору атакують кожного, хто натискає на посилання або відкриває вкладення. APT-атаки ретельно плануються і виконуються, а зловмисники витрачають час на вивчення своїх цілей і виявлення вразливостей, якими вони можуть скористатися.

Невидимість: APT розроблені таким чином, щоб бути непомітними та уникати виявлення. Зловмисники використовують різноманітні методи, щоб приховати свої сліди, такі як використання кастомного шкідливого програмного забезпечення, експлойтів нульового дня та просунутих методів маскування.

Стійкість: APT-атаки розроблені таким чином, щоб бути постійними, тобто зловмисники зберігають доступ до своїх цілей протягом тривалого часу. Це дозволяє їм збирати конфіденційні дані, красти інтелектуальну власність або порушувати роботу.

- Поширені методи APT-атак:

Списовий фішинг: Списовий фішинг - це тип фішингової атаки, яка спрямована на конкретних осіб або організації. Зловмисники надсилають

електронні листи, які виглядають як повідомлення від законного джерела, наприклад, колеги, клієнта або постачальника. Ці листи зазвичай містять шкідливе посилання або вкладення, після переходу за яким на комп'ютер жертви буде інстальовано шкідливе програмне забезпечення.

Атаки на водопій: Атаки "водопою" - це тип атак, спрямованих на веб-сайти, які часто відвідують жертви зловмисників. Зловмисники компрометують ці веб-сайти і впроваджують на них шкідливий код. Коли жертви відвідують веб-сайти, шкідливий код виконується на їхніх комп'ютерах і встановлює шкідливе програмне забезпечення.

Атаки нульового дня: Атаки нульового дня - це тип атак, які використовують вразливості в програмному забезпеченні, про які невідомо виробнику програмного забезпечення. Зловмисники використовують ці вразливості, щоб отримати доступ до комп'ютерів своїх жертв до того, як виробник встигне випустити виправлення.

- Як захиститися від APT [28]:

Навчання співробітників: Одна з найважливіших речей, яку можуть зробити організації для захисту від APT, - це навчити своїх співробітників усвідомлювати ризики, виявляти та уникати фішингових атак. Співробітники часто є найслабшою ланкою в ланцюгу безпеки. Програми підвищення обізнаності та навчання з питань безпеки можуть допомогти розповісти працівникам про новітні загрози, методи соціальної інженерії та безпечні практики роботи в Інтернеті. Підвищуючи обізнаність працівників, організації можуть зменшити ризик людських помилок та покращити загальний рівень безпеки. Вразливості в програмному забезпеченні та системах можуть надати зловмисникам плацдарм для компрометації IT-систем. Організаціям необхідно мати надійну програму управління вразливостями, щоб своєчасно виявляти, оцінювати та усувати вразливості [8].

Незважаючи на всі зусилля організацій, інциденти безпеки неминуче трапляються. Наявність чітко розробленого плану реагування на інциденти має вирішальне значення для ефективного реагування та пом'якшення наслідків інцидентів безпеки. План повинен визначати ролі та обов'язки, протоколи комунікації та процедури локалізації, ліквідації та відновлення. Кібербезпека - це

спільна відповідальність. Організації повинні співпрацювати з колегами по галузі, державними установами та постачальниками засобів кібербезпеки, щоб обмінюватися інформацією про загрози, вразливості та методи атак. Така співпраця може допомогти покращити загальний стан кібербезпеки всіх залучених організацій [12].

Для захисту від кіберзагроз важливо використовувати комплексний підхід, який включає різноманітні заходи безпеки. По-перше, встановлення та оновлення антивірусного програмного забезпечення допоможе виявляти та блокувати шкідливі програми. Регулярне оновлення операційної системи та всіх програм забезпечує захист від відомих вразливостей. Створення міцних та унікальних паролів для всіх облікових записів, а також використання двофакторної аутентифікації, додатково забезпечує захист від несанкціонованого доступу.

Важливо також бути обережними при отриманні електронних листів, особливо з незнайомих джерел, та уникати відкриття підозрілих вкладень або клікання по посиланням у таких повідомленнях. Резервне копіювання даних є важливою практикою, оскільки це може допомогти відновити важливу інформацію у випадку атаки з використанням шкідливого програмного забезпечення. Використання VPN може забезпечити додатковий рівень захисту, особливо при підключенні до публічних Wi-Fi мереж.

Забезпечення фізичної безпеки пристроїв також важливе, оскільки це допомагає запобігти несанкціонованому доступу до апаратного забезпечення. Освіта та обізнаність в галузі кібербезпеки є ключовими, оскільки багато атак здійснюються через соціальну інженерію та шахрайство. Проведення регулярних тренінгів з безпеки для персоналу може допомогти усвідомити ризики та вчасно реагувати на загрози. Нарешті, співпраця з фахівцями з кібербезпеки та консультування з ними може забезпечити додатковий рівень захисту та допомогти адаптувати стратегію безпеки до специфіки конкретної організації або індивідуальних потреб.

Виявлення та реагування на загрозливі дії та поведінку в IT-середовищі є складним і постійним викликом. Використовуючи різноманітні технології,

ефективно інтегруючи та організовуючи їх, застосовуючи проактивний підхід до виявлення загроз та реагування на них, а також розвиваючи культуру обізнаності з питань кібербезпеки, організації можуть значно покращити свою здатність захищати свої ІТ-активи та мінімізувати наслідки кібератак.

2 ТЕХНОЛОГІЯ ВИЯВЛЕННЯ ЗАГРОЗЛИВОЇ ДІЯЛЬНОСТІ І ПОВЕДІНКИ В ІТ СЕРЕДОВИЩІ

2.1. Багаторівневий підхід до виявлення загрозливої діяльності і поведінки в ІТ середовищі

Багаторівневий підхід до виявлення загрозливої діяльності та поведінки в ІТ середовищі включає застосування різних методів та інструментів на кожному рівні ІТ інфраструктури, що забезпечує більш повне та ефективне виявлення потенційних загроз.

Фізичний рівень: Тут використовуються методи та інструменти для захисту фізичних ІТ-активів. Це включає відеоспостереження, контроль доступу, захист периметра, а також моніторинг фізичних параметрів середовища, таких як температура та вологість.

Мережевий рівень: На цьому рівні акцент робиться на безпеці мережі. Використовуються системи виявлення вторгнень (IDS), системи виявлення аномалій, системи фільтрації трафіку та системи управління доступом до мережі (NAC), які допомагають виявити та запобігти атакам на мережеву інфраструктуру та несанкціонованому доступу.

Системний рівень: Тут застосовуються антивірусні та антишпигунські програми, програми для виявлення та усунення вразливостей, а також системи управління інформаційною безпекою (SIEM). Ці інструменти фокусуються на захисті операційних систем, застосунків та інших програмних компонентів.

Поведінковий рівень: Методи на цьому рівні включають аналіз журналів подій, аналіз поведінки користувачів та систем. Це дозволяє виявляти загрози, пов'язані з аномальною поведінкою користувачів або систем.

Оптимальне використання цих методів та інструментів залежить від конкретних потреб організації, але важливо застосовувати комплексний підхід, що охоплює всі чотири рівні.

Конкретні приклади застосування включають використання системи виявлення вторгнень для моніторингу мережевої інфраструктури, програм для виявлення вразливостей у програмному забезпеченні, а також систем управління доступом до мережі для контролю доступу та виявлення аномалій у поведінці користувачів. Важливо, щоб організація регулярно переглядала та оновлювала свій підхід до виявлення загроз, щоб він відповідав поточним загрозам та потребам організації. ThreatMark Anti-Fraud Suite є передовим рішенням нового покоління для виявлення шахрайства, розробленим компанією ThreatMark [14]. Воно базується на поведінковому профілюванні та машинному навчанні, надаючи банкам можливість ефективно захищати свої онлайн та мобільні канали.

В умовах постійної еволюції кіберзагроз, традиційні системи, зосереджені на виявленні шкідливого коду або аналізі транзакцій, часто виявляються недостатньо ефективними. У відповідь на це, ThreatMark Anti-Fraud Suite впроваджує багаторівневий захист, що включає комплексний підхід та аналіз поведінки та біометрії користувачів, дозволяючи виявляти навіть атаки нульового дня.

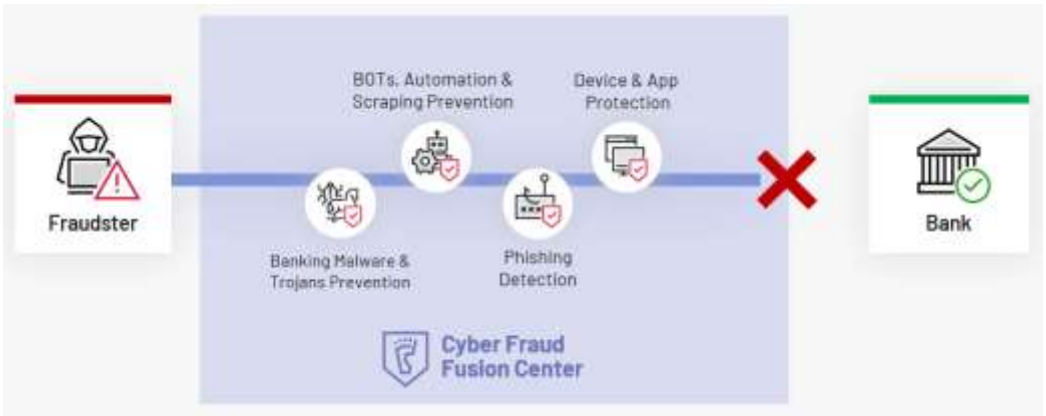

Рис. 2.1. Схема роботи ThreatMark [14]

Ключові елементи системи включають:

- **Поведінкове профілювання:** Моніторинг дій клієнтів в системі з оцінкою сотень параметрів, включаючи поведінкові паттерни, параметри сесії, деталі транзакцій, біометрію та взаємодію з веб-формою і мобільним додатком.

- **Машинне навчання:** Аналіз поведінки клієнтів та сотень технічних та фінансових параметрів за допомогою сучасних досягнень у сфері машинного навчання та штучного інтелекту, що дозволяє виявляти підозрілу активність на ранніх етапах.
- **Багаторівневий підхід:** Збалансоване поєднання різних рівнів захисту, від поведінкового аналізу до аналізу транзакцій, для підвищення швидкості виявлення загроз та зниження помилкових спрацьовувань.

ThreatMark застосовує передові технології для виявлення загроз в цифровому просторі. Їхня система, ThreatMark Anti-Fraud Suite (AFS), ретельно моніторить та аналізує дані, які відображаються у браузері користувача, а також ті, що знаходяться у прихованому коді програми. Вона автоматично перевіряє виявлені відмінності, щоб встановити відповідність з відомими ознаками шкідливого ПЗ. У разі співпадіння, система повідомляє про виявлення загрози [14].

Якщо виявляються невідомі аномалії, вони надсилаються до Центру боротьби з кібершахрайством ThreatMark (CFFC) для детального аналізу. ThreatMark також виявляє потенційно небезпечні налаштування та нестандартні дії, які можуть бути ознакою фінансового шкідливого ПЗ, що намагається виконати автоматизовану транзакцію. Система ThreatMark здатна розпізнавати різноманітні види шахрайства на всіх типах пристроїв - від зловживання обліковими записами і новими шахрайськими обліковими записами до фішингу, SIM-swapping, вішингу, бот-атак, шкідливого ПЗ, RAT-атак та інших.

Крім самого виявлення, ThreatMark розвиває інтелектуальні можливості розвідки загроз, що допомагає навчитися на минулих атаках та запобігти їх повторенню в майбутньому. Відповідаючи на постійно ускладнюючіся методи шахраїв, система надає банкам необхідні інструменти для захисту своїх активів та репутації.

Сучасні постійні загрози (СПЗ) становлять значний виклик для організацій через їхні витончені технології та здатність залишатися невиявленими протягом тривалого часу. Для ефективного виявлення та запобігання цим загрозам необхідний багаторівневий підхід до безпеки. Основою багаторівневого підходу є

багаторівнева архітектура безпеки. Ця архітектура визначає різні рівні захисту, кожен з яких має власний набір засобів контролю та технологій безпеки. Ці рівні працюють разом, щоб забезпечити комплексний захист, створюючи численні перешкоди для зловмисників [11].

До загальних рівнів багаторівневої архітектури безпеки відносяться::

1. Мережева безпека: Цей рівень спрямований на захист периметра мережі від несанкціонованого доступу. Він включає брандмауери, системи виявлення/запобігання вторгнень (IDS/IPS) та системи виявлення та запобігання DDoS-атакам.

2. Безпека додатків: Цей рівень спрямований на захист додатків від вразливостей та атак. Він включає брандмауери веб-додатків (WAF), інструменти тестування безпеки та інструменти управління вразливостями додатків.

3. Безпека пристроїв: Цей рівень спрямований на захист окремих пристроїв, таких як ноутбуки та сервери, від шкідливого програмного забезпечення та інших загроз. Він включає антивірусне/антивірусне програмне забезпечення, рішення для виявлення та реагування на загрози на кінцевих точках (EDR) та білі списки додатків.

4. Безпека даних: Цей рівень спрямований на захист конфіденційних даних у стані спокою, під час передачі та використання. Він включає шифрування даних, рішення для запобігання втраті даних (DLP) та рішення для резервного копіювання/відновлення даних.

5. Управління ідентифікацією та доступом (IAM): Цей рівень зосереджений на контролі доступу до ресурсів на основі ідентифікаційних даних та дозволів користувачів. Він включає багатофакторну автентифікацію (MFA), управління привілейованим доступом (PAM) та управління ідентифікацією та доступом (IAG).

Побудова системи корпоративної інформаційної безпеки розпочинається з гарантування комплексного захисту кінцевих точок від шкідливих програм, мережевих атак, несанкціонованого доступу та крадіжки даних. Сучасний ландшафт загроз вимагає багаторівневого підходу до забезпечення безпеки.

Значущість і складність захисту кінцевих точок підсилюються тим, що саме ці точки стають частішим об'єктом атак зловмисників. Ланцюжок атак може розпочинатися з різних методів доставки, таких як електронна пошта, Інтернет або шкідливі додатки через USB-пристрої.

Для охоплення всього ланцюжка атак необхідно використовувати різні технології та методи виявлення і захисту. На етапі доставки відповідальність лежить на системах, таких як аналіз репутації файлу, захист браузера і фільтрація URL, локальний брандмауер, контроль пристроїв і додатків. Модуль Host IPS або "віртуальний патчінг" захищає від заражень і поширення по мережі. Технології машинного навчання аналізують шкідливе програмне забезпечення перед і після запуску файлу. На завершальному етапі проводиться аналіз репутації командних центрів і моніторинг мережевої активності [19].

При впровадженні сучасних рішень для ефективного захисту робочих станцій і серверів, особлива увага повинна бути приділена їхній здатності запобігати зараженню на кожному етапі. Крім високоточного виявлення сучасних загроз, комплекс захисту кінцевих точок повинен відповідати вимогам щодо низького навантаження на кінцеві точки і легкого управління.

Symantec Endpoint Protection та Trend Micro OfficeScan XG є рішеннями, що володіють усіма цими характеристиками. Обидва продукти визнані лідерами відповідно до останнього тестування AV-TEST, забезпечуючи максимальну ефективність як на світовому ринку, так і в Україні.

Symantec Endpoint Protection – це комплексна антивірусна система, розроблена для боротьби з сучасними складними загрозами безпеки. Trend Micro OfficeScan використовує високоточне машинне навчання разом з різними методами захисту від загроз з використанням технологій XGen. Обидва рішення мають багаторівневий підхід до захисту від сучасних атак, мають низький рівень споживання ресурсів і легкі в управлінні. Однак перед остаточним впровадженням експерти рекомендують провести попереднє тестування ефективності обох рішень у зв'язку з складною структурою сучасних корпоративних мереж.

Розуміння ландшафту загроз і постійний моніторинг нових загроз мають вирішальне значення для ефективного виявлення та попередження ПНП. Впровадження засобів розвідки та аналізу загроз дозволяє організаціям:

- Ідентифікувати та визначити пріоритетність загроз: Збираючи та аналізуючи інформацію про загрози з різних джерел, організації можуть отримати уявлення про новітні тактики, методи та процедури (ТТП) боротьби з НМУ. Ця інформація може бути використана для визначення пріоритетності загроз і зосередження зусиль з безпеки на сферах з найбільшим ризиком.
- Виявляти та реагувати на атаки: Відстеження загроз і процеси реагування на інциденти мають важливе значення для швидкого і ефективного виявлення та реагування на атаки з використанням технологій, спрямованих на викрадення людей (МРТ). Розвідка загроз може бути використана для інформування цих процесів, гарантуючи, що організації будуть готові реагувати на конкретні загрози, з якими вони стикаються.

Керування засобами та процесами безпеки вручну може забирати багато часу та бути схильним до помилок. Інструменти автоматизації та оркестрування безпеки (SAO) можуть допомогти організаціям покращити стан безпеки шляхом автоматизації рутинних завдань, таких як:

- Встановлення виправлень безпеки та управління вразливостями: Інструменти SAO можуть автоматизувати процес виявлення, визначення пріоритетів і застосування виправлень безпеки до вразливих систем.
- Реагування на інциденти: Інструменти SAO можуть автоматизувати завдання реагування на інциденти, такі як ізоляція заражених систем, збір судових доказів і сповіщення відповідного персоналу.
- Інтеграція розвідданих про загрози: Інструменти SAO можуть інтегрувати канали розвідки загроз у системи безпеки, що дає змогу виявляти загрози в режимі реального часу та реагувати на них.

Багаторівневий підхід до безпеки — це організована стратегія, що використовує кілька рівнів захисту для ефективного захисту хмарних додатків.

Кожен рівень спрямований на різні аспекти безпеки, що дозволяє компаніям забезпечити більший контроль та гнучкість у захисті своїх хмарних програм [34].

- Перший рівень — це контроль доступу, що допомагає регулювати, хто має доступ до хмарних програм та даних. Використання методів автентифікації та авторизації дозволяє гарантувати, що тільки авторизовані користувачі можуть отримати доступ до програм.
- Другий рівень — шифрування даних. Цей рівень допомагає захистити конфіденційну інформацію, зробивши її незрозумілою для читання без належного ключа шифрування. Використання шифрування даних гарантує безпеку інформації та перешкоджає її неправомірному доступу.
- Третій рівень — управління вразливістю. Він дозволяє виявляти та усувати потенційні вразливості в хмарних програмах, забезпечуючи безпеку відмовозахисних механізмів.
- Четвертий рівень — це безпека мережі. Застосування брандмауерів, систем виявлення вторгнень та інших методів захисту дозволяє ефективно захищати хмарні програми від мережевих загроз.
- Останній рівень — безпека програм. Використання заходів безпеки допомагає захистити хмарні додатки від різноманітних загроз, таких як шкідливий код чи атаки міжсайтових сценаріїв.

Багаторівневий підхід дозволяє компаніям ефективно захищати свої хмарні програми, забезпечуючи безпеку на різних рівнях. З урахуванням росту використання хмарових технологій важливо розглядати та впроваджувати цей підхід для забезпечення надійного захисту хмарних додатків.

Зараз хмарні обчислення набувають популярності в бізнес-середовищі завдяки своїй економічній ефективності та зручності. Проте, пов'язані з ними ризики безпеки можуть викликати обурення в багатьох компаніях. Для забезпечення безпеки даних і систем важливо впровадити безпечні хмарні обчислення.

- Одним з перших кроків є налагодження безпечних методів автентифікації. Це включає в себе встановлення надійних протоколів, таких як

двофакторна та багатофакторна автентифікація. Такі протоколи гарантують, що доступ до систем і даних мають лише авторизовані користувачі. Крім того, важливо переконатися, що всі дані шифруються під час їх зберігання в хмарі.

- По-друге, слід переконатися, що постачальник хмарних послуг відповідає необхідним стандартам безпеки, таким як ISO 27001, що охоплює управління інформаційною безпекою. Також важливо, щоб постачальник мав бездоганну історію безпеки та використовував оновлені технології безпеки.
- По-третє, потрібно регулярно переглядати політику хмарних обчислень, налаштовувати політики контролю доступу та правила безпеки. Це також включає налаштування систем моніторингу та журналу для відстеження всіх дій і сповіщення про будь-які підозрілі активності.

Використовуючи ці підходи, можна забезпечити безпеку використання хмарних обчислень, захищаючи дані та системи від можливих загроз. Зниження ризиків безпеки хмарних додатків може бути досягнуте за допомогою автоматизації, що забезпечить захист конфіденційних даних. Автоматизація сприяє виявленню та усуненню проблем безпеки ще до того, як вони стануть серйозними. Цей процес допомагає економити час та ресурси організації. Також автоматизація дозволяє ефективно реагувати на потенційні загрози. Організації можуть також використовувати автоматизацію для забезпечення безпеки своїх даних, включаючи шифрування, моніторинг активності користувачів та виявлення підозрілих дій. Завдяки автоматизації, ризики безпеки можуть бути зменшені, а ймовірність порушення безпеки великої системи значно знижується [12].

Важливо також розглянути можливість використання автоматизованих інструментів для забезпечення дотримання вимог щодо безпеки. Ці інструменти допомагають перевірити відповідність стандартам та галузевим вимогам. Використовуючи автоматизацію, організації можуть бути впевнені, що їхні системи відповідають найвищим стандартам безпеки. Загалом, автоматизація є потужним інструментом для зниження ризиків безпеки хмарних програм. Вона допомагає організаціям ефективно заощаджувати час, гроші та ресурси, забезпечуючи при цьому безпеку їхніх систем. Використовуючи автоматизовані

рішення, організації можуть забезпечити, що їхні дані залишаються в безпеці, а їхні системи залишаються надійними.

2.2. Технології виявлення та останні інциденти APT-атак

Термін APT використовується для опису атак, під час яких зловмисники чи їх група докладають зусиль для нелегітимного та тривалого втручання в мережу жертви, з метою отримання конфіденційної інформації чи виконання інших цілей. APT атака об'єднує три ключові складові: "Advanced" - використання різноманітних методів та інструментів, "Persistent" - підтримка постійної присутності у внутрішньому середовищі для вилучення цінної інформації, і "Threat" - спрямованість на досягнення конкретних цілей, часто пов'язаних з отриманням фінансової, технологічної та іншої інформації. За визначенням NIST, APT описується як комплексний противник з високим рівнем знань та ресурсами, який стрімко адаптується та веде атаки з метою вилучення інформації або підриву цільових організацій протягом тривалого періоду [24].

Таблиця 2.1.

Порівняння APT атак із традиційними атаками

Характеристика	**APT атака**	**Традиційна атака**
Порушник	Визначена високоорганізована група людей	Одна або декілька людей
Ціль	Конкретні організації, урядові установи, комерційні підприємства	Невизначена, переважно індивідуальна система
Мета	Фінансові вигоди, конкурентні та стратегічні переваги	Фінансові вигоди, демонстрація здібностей

Підхід	Неодноразові спроби, пристосовуються до опору захисним засобам, тривалий термін	Короткострокова, одноразова

Продовження таблиці.2.1.

Порівняння APT атак із традиційними атаками

Під час аналізу методів виявлення загроз APT були виявлені моделі Kill Chain та Diamond, що є основними для виявлення та аналізу вторгнень. Модель Kill Chain включає 7 фаз, які допомагають виявити вторгнення, розкривають тактику противника та його процедури. Ця модель визначає етапи, які противники повинні пройти для досягнення своєї мети в мережі. Зупинка на будь-якому етапі може призвести до припинення атаки, і фахівці інформаційної безпеки мають завдання блокувати дії зловмисників на різних стадіях, зокрема на ранніх, для ефективного запобігання. Оскільки сучасні постійні загрози (APT) стають все більш витонченими і поширеними, організаціям необхідно використовувати надійні технології виявлення для захисту своїх мереж і даних. Ці технології відіграють вирішальну роль у виявленні потенційних загроз і своєчасному впровадженні стратегій їх усунення. Ось огляд деяких ключових технологій виявлення, що використовуються для боротьби з APT [14]:

Захист кінцевих точок: Рішення для захисту кінцевих точок забезпечують комплексний захист кінцевих точок, таких як настільні комп'ютери, ноутбуки та мобільні пристрої. Вони відстежують і виявляють зловмисні дії, включаючи зараження шкідливим програмним забезпеченням, виконання підозрілих файлів і спроби несанкціонованого доступу. Передові рішення для захисту кінцевих точок включають алгоритми машинного навчання та штучного інтелекту для аналізу поведінки кінцевих точок і виявлення аномалій, які можуть свідчити про атаку APT.

Мережева безпека: Інструменти мережевої безпеки відстежують і контролюють мережевий трафік для виявлення і блокування шкідливих дій. Вони

використовують такі технології, як системи виявлення вторгнень (IDS), системи запобігання вторгненням (IPS) і брандмауери для фільтрації вхідного і вихідного трафіку, запобігаючи несанкціонованому доступу, поширенню шкідливого програмного забезпечення і витоку даних. Інструменти мережевої безпеки також забезпечують видимість шаблонів мережевого трафіку, що дозволяє захисникам виявляти аномалії та потенційні загрози.

Аналіз поведінки користувачів та організацій (UEBA): Рішення UEBA аналізують моделі поведінки користувачів і організацій, щоб виявити відхилення від нормальної діяльності, які можуть свідчити про APT-атаку. Вони відстежують логіни користувачів, шаблони доступу, використання даних і активність пристроїв, створюючи базову лінію для нормальної поведінки і відзначаючи аномалії, які можуть свідчити про несанкціонований доступ або зловмисну діяльність.

Запобігання втраті даних (DLP): Рішення DLP відстежують і контролюють рух даних в організації, щоб запобігти несанкціонованому витоку даних. Вони використовують такі методи, як фільтрація контенту, шифрування даних і моніторинг кінцевих точок, щоб гарантувати, що конфіденційні дані не передаються поза дозволеними каналами. Рішення DLP можуть допомогти організаціям дотримуватися правил конфіденційності даних і захистити конфіденційну інформацію від несанкціонованого доступу.

Розвідка загроз: Канали розвідки загроз надають організаціям інформацію в режимі реального часу про найновіші APT-загрози, вразливості та методи атак. Ця інформація може бути використана для проактивного оновлення систем безпеки, впровадження стратегій пом'якшення наслідків та навчання персоналу служби безпеки. Джерелами розвідданих про загрози є урядові установи, постачальники систем безпеки та організації, що займаються дослідженням загроз.

Для аналізу атак на розподілені обчислювальні системи використовуються різноманітні методи, включаючи аналіз сигнатур, статистичний аналіз, аналіз систем станів, графи сценаріїв атак, експертні системи, методи засновані на специфікації, нейронні та імунні мережі, груповий аналіз та поведінкову біометрію.

Аналіз сигнатур базується на порівнянні даних системи з відомими сигнатурами атак, збереженими у базі даних. Цей метод швидкий і точний для виявлення відомих атак, але не може виявити нові типи атак. Статистичний аналіз використовує створені статистичні профілі нормальної поведінки системи і виявляє атаки через відхилення від цих профілів. Цей метод адаптивний і може виявляти невідомі атаки, але схильний до помилкових спрацьовувань.

Аналіз систем станів розглядає роботу системи як послідовність станів і переходів, ідентифікуючи неприйнятні шляхи зміни станів як потенційні атаки. Цей метод може пропустити атаки зі складними сценаріями. Графи сценаріїв атак створюються для ідентифікації всіх можливих неправильних поведінок системи, але через свою складність цей метод рідко використовується для виявлення вторгнень.

Інші методи, як нейронні мережі та імунні мережі, використовують більш складні алгоритми для аналізу поведінки системи, але також можуть бути складні у впровадженні та налаштуванні. Вибір конкретного методу аналізу залежить від специфіки системи та характеру потенційних загроз.

Експертні системи працюють на основі набору фактів та правил висновку для ідентифікації атак, але вимагають значних обчислювальних зусиль. Методи засновані на специфікаціях визначають атаки, порушуючи встановлені обмеження поведінки, але обмежені можливістю еволюції специфікацій.

Нейронні та імунні мережі використовуються для класифікації поведінки системи, проте можуть бути складними у впровадженні. Груповий аналіз розділяє поведінку системи на кластери, визначаючи аномалії, але може мати схожі недоліки, що і статистичний аналіз, такі як висока ймовірність помилкових спрацьовувань. Деякі методи, як графи сценаріїв атак та експертні системи, майже не використовуються у сучасних системах через їхню велику обчислювальну складність. Нейронні мережі, хоча і адаптивні, вимагають точного тестового набору для ефективного навчання. Статистичний аналіз та груповий аналіз мають певну ефективність, але також схильні до помилкових позитивних результатів.

- Нещодавні інциденти APT

Ландшафт кібербезпеки постійно змінюється, а учасники APT-атак розробляють все більш витончені методи для компрометації організацій. Нещодавні гучні інциденти APT підкреслюють потребу в надійних стратегіях виявлення та пом'якшення наслідків:

Атака на ланцюжок постачання SolarWinds: У 2020 році від атаки на ланцюжок поставок SolarWinds постраждали тисячі організацій, в тому числі державні установи та компанії зі списку Fortune 500. Зловмисники скомпрометували вихідний код SolarWinds і вбудували шкідливе програмне забезпечення в програмне забезпечення Orion, яке потім використовувалося для шпигунства за клієнтами SolarWinds [14]. Цей інцидент продемонстрував потенційний вплив атак на ланцюги поставок і необхідність впровадження надійних практик безпеки постачальників.

Атака вірусу-здирника Colonial Pipeline: У 2021 році атака вірусу-здирника Colonial Pipeline порушила ланцюжок постачання палива в США, завдавши значних економічних збитків. Атака підкреслила потенційний вплив програм-вимагачів на критичну інфраструктуру та необхідність для організацій мати надійні стратегії кіберстійкості [26].

Вразливості Microsoft Exchange ProxyLogon: У 2021 році вразливості в Microsoft Exchange ProxyLogon дозволили зловмисникам захопити сервери Microsoft Exchange, що вплинуло на мільйони користувачів. Цей інцидент продемонстрував важливість своєчасного виправлення вразливостей і необхідність для організацій підтримувати сучасні системи безпеки.

Для аналізу конкретного рішення щодо захисту від APT-атак та загрозливої діяльності, розглянемо як приклад систему виявлення та запобігання вторгненням (IDS/IPS). Ця технологія використовується для моніторингу мережевого трафіку та системної активності з метою виявлення шкідливих дій або порушень безпеки.

Функції та архітектура IDS/IPS:

- IDS (Intrusion Detection System) використовує підписи атак, аналіз поведінки або комбінацію обох для виявлення небезпечної активності.

- IPS (Intrusion Prevention System) виконує ті ж функції, що й IDS, але також активно блокує або запобігає виявленим атакам.

- Системи можуть бути розгорнуті як мережеві (NIDS/NIPS) або хост-базовані (HIDS/HIPS) залежно від потреби в захисті мережевого трафіку або конкретних пристроїв.

- Розширені функції включають інтеграцію з іншими системами безпеки, такими як файрволи, антивірусне програмне забезпечення та системи управління подіями безпеки (SIEM).

Можливості:

- Ефективне виявлення різних видів кібератак, включаючи APT, фішинг, DDoS та інші.

- Здатність адаптуватися до нових загроз завдяки оновленням підписів атак та алгоритмів поведінкового аналізу.

- Моніторинг в реальному часі та швидке реагування на інциденти.

Порівняння з іншими рішеннями:

- У порівнянні з традиційними антивірусами, IDS/IPS орієнтовані більше на мережевий трафік та поведінку систем, ніж на шкідливі файли.

- Відмінність від файрволів полягає в більш глибокому аналізі трафіку та можливості виявлення витончених атак.

- SIEM системи збирають та аналізують дані з багатьох джерел, включаючи IDS/IPS, але фокусуються на кореляції подій та довгостроковому аналізі для виявлення складних загроз.

Останні інциденти APT-атак підкреслюють необхідність розширеного моніторингу та аналізу. Сучасні APT кампанії часто використовують поліморфний код, соціальну інженерію та живуть довго в системі до виявлення, що вимагає більш складних засобів захисту, таких як IDS/IPS з розширеними аналітичними функціями та інтеграцією з іншими системами безпеки.

- Додаткові кроки для захисту від APT

На додаток до впровадження технологій виявлення, організації можуть вжити кілька проактивних заходів для захисту від APT:

1. Навчати співробітників: Навчання з питань безпеки має вирішальне значення для того, щоб працівники могли виявляти та уникати потенційних атак APT. Сюди входить навчання щодо фішингових електронних листів, тактик соціальної інженерії та гігієни паролів.

2. Впроваджуйте надійні політики паролів: Впроваджуйте надійні політики паролів, які вимагають складних паролів, регулярної зміни паролів та багатофакторної автентифікації (MFA) для посилення безпеки облікових записів.

3. Створіть плани реагування на інциденти: Наявність комплексного плану реагування на інциденти забезпечує скоординоване та ефективне реагування на APT-атаки. Компанії повинні регулярно переглядати та оновлювати свою систему безпеки, враховуючи нові загрози та технології, що розвиваються.

Використовуючи комбінацію технологій виявлення, проактивних заходів безпеки та постійного моніторингу, організації можуть підвищити свою кіберстійкість і ефективно захистити свої мережі та дані від зростаючої загрози APT-атак.

2.3. Функціональність IPS та її порівняння з альтернативами

Системи виявлення вторгнень (IDS) та системи запобігання вторгнень (IPS) є ключовими інструментами для оборони мереж від різноманітних атак, хоча між ними існують значні відмінності. IDS зосереджені на пасивному зборі даних про мережевий трафік та аналізі цих даних для виявлення підозрілої активності. Якщо така активність виявляється, система IDS видає попередження для подальшого аналізу. З іншого боку, IPS активно втручається, збираючи дані та блокуючи підозрілу активність у разі її виявлення. Функціональні можливості IPS охоплюють виявлення вторгнень за допомогою різних методів, таких як підбір паролів, атаки

на відкриті порти, експлуатація вразливостей та поширення шкідливого програмного забезпечення. Крім того, IPS можуть блокувати атаки через фільтрацію трафіку, перенаправлення або ізоляцію пристроїв, а також відстежувати вторгнення для допомоги в розслідуванні інцидентів.

У порівнянні з альтернативними методами захисту мереж, такими як фільтрація трафіку чи антивірусні програми, IPS мають переваги в виявленні різних типів загроз, блокуванні атак та відстеженні вторгнень. Однак, вони можуть бути складними в налаштуванні, а також іноді створюють помилкові тривоги, що веде до блокування законного трафіку [19].

При виборі IPS, організаціям потрібно враховувати свої конкретні потреби. Організації, які шукають захист від широкого спектру загроз, можуть розглядати використання IPS, тоді як ті, хто має обмежені ресурси або шукає простіше рішення, можуть віддавати перевагу іншим методам захисту мереж. Система SIEM централізує інформацію про діяльність зловмисного програмного забезпечення та порушення стандартної роботи, обробляючи дані з багатьох джерел і застосовуючи методи фільтрації загроз для розрізнення справжньої активності від хибних спрацьовувань. Деякі IDS можуть виявити мережеві атаки на ранніх стадіях, інші ж можуть розпізнавати раніше невідомі атаки, що є характеристикою систем IPS. Часто програмно-апаратні рішення комбінують функціональність обох типів систем, що відомо як IDPS.

IDS можна класифікувати за різними ознаками, зокрема за розмірами від окремих комп'ютерів до великих мереж, а також за методами виявлення загроз, як-от виявлення на основі сигнатур або виявлення аномалій. Серед різновидів IDS виділяються NIDS (системи виявлення вторгнень у мережу) та HIDS (системи виявлення вторгнень на основі хоста). Розглядаючи класичну класифікацію СВВ, можна виділити системи рівня мережі, системи рівня хоста та системи оцінки вразливостей системи. Кожна з цих систем має свої унікальні характеристики та сфери застосування.

Несистемні характеристики реакції на результати аналізу можна розділити на інформативні та активні. У випадку інформативної реакції, зацікавлені сторони

отримують сповіщення про виявлені проблеми. Активні дії, як-от блокування IP-адрес зловмисників, є більш безпосередніми втручаннями. На практиці, ці характеристики часто розмежовують системи виявлення вторгнень (IDS) та системи запобігання вторгненням (IPS), хоча багато IDS можуть бути інтегровані в IPS для забезпечення більш комплексного захисту.

У процесі моніторингу мережі використовуються різні типи даних, зокрема дані на мережевому вузлі та дані на рівні мережі. Дані вузла мережі стосуються окремого вузла і його взаємодії з іншими вузлами, що дозволяє виявити атаки на конкретний хост. Такі дані можуть включати інформацію про мережеву активність вузла, його налаштування, файли та процеси. Ці дані можуть бути зібрані як безпосередньо на вузлі, так і ззовні за допомогою інструментів, таких як мережеві сканери. З іншого боку, дані про мережу надають загальне уявлення про взаємодію всієї мережі. Зазвичай повні дані мережі не збираються через великі вимоги до ресурсів, а IDS аналізують трафік, що протікає через маршрутизатор. Також існує можливість збору даних безпосередньо з вузла, де запущена IDS, що може забезпечити додатковий контроль.

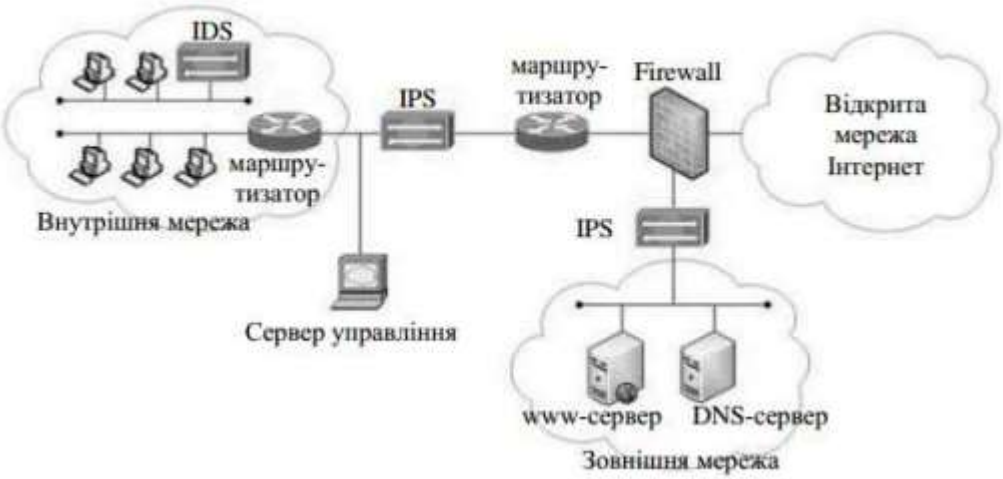

Рис. 2.2. Схема розміщення IDPS у мережі [26]

Методи отримання даних у СВВ варіюються від активних до пасивних, а також змішаних методів. Пасивні системи просто відстежують ситуацію без безпосереднього втручання, що є типовим для більшості IDS та систем рівня хоста.

Наприклад, вони можуть оцінювати відповідність прав на системний файл до шаблону в базі даних та видають попередження, якщо відповідності не досягнуто.

Сучасні системи виявлення атак та запобігання вторгненням, такі як IDPS, використовують поєднання підходів IDS та IPS для виявлення та блокування спроб злому. IDPS поєднує сніфер, аналізатор та систему сповіщення (блокування), і може контролювати роботу мережевих пристроїв та операційних систем, виявляти несанкціоновані дії та автоматично виконувати функції, визначені адміністратором, такі як повідомлення адміністратора, зміна налаштування брандмауера, переривання зв'язку TCP або запуск програми. За методами виявлення вторгнень існують системи на основі аналізу сигнатур та пошуку аномалій. Системи на основі сигнатур порівнюють трафік з базою сигнатур атак, а системи на пошуку аномалій виявляють статистичні аномалії або незвичайну частоту подій [26]. Класифікація IDPS також включає мережні IDPS (NIDPS), які аналізують мережевий трафік, і системні IDPS, які фокусуються на виявленні атак на рівні окремих хостів або систем.

Альтернативою IPS є система фільтрації трафіку (firewall). Firewalls можуть блокувати загрози, використовуючи правила для фільтрації трафіку на основі його джерела, призначення, протоколу або контенту. Однак, firewalls не можуть виявляти аномалії або відомі загрози, як це може робити IPS. Іншою альтернативою IPS є система виявлення та запобігання вторгненням (IDS/IPS) [34]. IDS/IPS поєднує в собі функції IDS та IPS в одному пристрої або програмному забезпеченні. IDS/IPS може бути хорошим вибором для організацій, які хочуть отримати переваги як IDS, так і IPS. Вибір між IPS, firewall або IDS/IPS залежить від конкретних потреб організації. Організації, які потребують високоефективного виявлення та блокування загроз, повинні розглянути можливість використання IPS. Організації, які потребують менш складного та менш дорогого рішення, можуть розглянути можливість використання firewall або IDS/IPS.

2.4. Визначення шляхів подальшого розвитку та вирішення проблеми

Сучасні постійні загрози (APT) становлять значну загрозу, що постійно розвивається, для організацій будь-якого розміру. Їхні витончені методи, прихований підхід і цілеспрямовані атаки роблять їх грізним супротивником у ландшафті кібербезпеки. Щоб протистояти цій еволюціонуючій загрозі, організаціям необхідно прийняти комплексний підхід, який охоплює не лише виявлення та запобігання, але й постійний моніторинг та вдосконалення [19].

- Розширюйте можливості виявлення та запобігання

Використовуйте штучний інтелект (ШІ) та машинне навчання (МН): ШІ та ML можуть відігравати вирішальну роль в аналізі величезних обсягів даних для виявлення аномалій і потенційних загроз, які можуть свідчити про APT-атаки. Ці технології можна інтегрувати в системи безпеки, щоб підвищити точність виявлення загроз і зменшити кількість хибних спрацьовувань.

Навчання (ML) в кібербезпеці:

1. Посилення сегментації мережі: Сегментація мережі може обмежити поширення APT-атаки, ізолюючи критичні системи та дані від менш чутливих мереж. Це допомагає стримати атаку і запобігти масштабним пошкодженням. Організаціям слід впроваджувати методи мікросегментації для подальшої ізоляції критично важливих активів і створення менших, більш керованих сегментів мережі.

2. Підвищення обізнаності та навчання користувачів: Інформування співробітників про APT-атаки та їхню тактику має вирішальне значення для запобігання атакам соціальної інженерії та спробам фішингу. Регулярні тренінги з підвищення обізнаності про безпеку можуть допомогти працівникам виявляти підозрілі електронні листи, веб-сайти та дії, зменшуючи ризик людської помилки, яка часто слугує відправною точкою для APT-атак.

3. Спеціалісти з пошуку загрози: Спеціальні команди полювання на загрози можуть проактивно шукати і виявляти потенційні APT-атаки в мережі

організації. Ці команди повинні мати доступ до передових інструментів і методів для аналізу даних про загрози та виявлення прихованої шкідливої активності.

4. Використовуйте канали розвідки загроз: Канали розвідки загроз надають організаціям інформацію в режимі реального часу про найновіші APT-загрози, вразливості та методи атак. Цю інформацію можна використовувати для проактивного оновлення систем безпеки, впровадження стратегій пом'якшення наслідків і навчання персоналу служби безпеки.

5. Безперервне управління вразливостями: Організації повинні надавати пріоритет своєчасному управлінню вразливостями, оперативно виправляючи відомі вразливості, щоб запобігти їх використанню групами APT. Інструменти сканування вразливостей та процеси управління виправленнями повинні бути інтегровані в робочий процес безпеки організації.

6. Регулярні аудити та оцінки безпеки: Регулярне проведення аудитів та оцінок безпеки допомагає організаціям виявити слабкі місця в системі безпеки та усунути їх до того, як ними зможуть скористатися групи APT. Ці оцінки повинні охоплювати мережеву безпеку, безпеку кінцевих точок, контроль доступу та можливості реагування на інциденти.

7. Впроваджуйте культуру кібербезпеки: Впровадження культури кібербезпеки в організації має важливе значення для довгострокового захисту від APT-атак. Це передбачає підкреслення важливості кібербезпеки для всіх співробітників, заохочення відкритого спілкування про проблеми безпеки та винагороду за безпечну поведінку.

Прийнявши ці стратегії та сприяючи безперервному циклу вдосконалення, організації можуть значно підвищити свою кіберстійкість та ефективно захиститися від загрози APT-атак. Визначення можливих шляхів подальшого розвитку та вирішення проблеми кібербезпеки вимагає комплексного підходу, який би включав розвиток технологій, поліпшення процесів управління, освітні ініціативи та законодавчі зміни.

Одним із ключових аспектів є вдосконалення технологічних інструментів безпеки. Це включає розвиток систем штучного інтелекту та машинного навчання

для виявлення та реагування на кібератаки в реальному часі. Використання передових технологій, таких як поведінковий аналіз, аномалійне виявлення та автоматизоване реагування, може значно покращити здатність організацій ідентифікувати та нейтралізувати загрози. Підвищення рівня освіти та обізнаності користувачів є ще одним важливим напрямком. Регулярні тренінги з кібербезпеки, семінари та кампанії з підвищення обізнаності можуть зменшити ризики, пов'язані з людським фактором, такі як фішинг або випадкове розголошення інформації.

Поліпшення управлінських процесів і політик безпеки також відіграє ключову роль. Це означає впровадження строгих політик безпеки, регулярні аудити та оцінки вразливостей, а також розробку та дотримання планів реагування на інциденти.

Законодавчі зміни та співпраця на міжнародному рівні також можуть сприяти покращенню кібербезпеки. Це включає розробку та імплементацію законів, які регулюють кіберпростір, сприяють обміну інформацією про загрози та встановлюють стандарти безпеки для організацій і технологій. Інтеграція і співпраця між різними інструментами та рішеннями безпеки, що охоплюють мережеву безпеку, захист кінцевих точок, управління ідентифікацією та доступом, також є ключовими для створення єдиної та ефективної системи захисту.

На закінчення, неперервний моніторинг, аналіз та адаптація до змінюваного ландшафту кіберзагроз є необхідними для підтримки високого рівня безпеки. Це включає в себе відстеження нових технік атак, розвиток загроз та впровадження необхідних змін у стратегію та інструменти кібербезпеки.

3 РОЗРОБКА РЕКОМЕНДАЦІЙ ВИКОРИСТАННЯ ТЕХНОЛОГІЇ ВИЯВЛЕННЯ ЗАГРОЗЛИВОЇ ДІЯЛЬНОСТІ І ПОВЕДІНКИ В ІТ СЕРЕДОВИЩІ

3.1. Розробка рекомендацій щодо застосування технологій виявлення загрозливої діяльності на основі IPS/IDS

При застосуванні технологій виявлення загрозливої діяльності, заснованих на IPS/IDS, першочергово необхідно чітко визначити цілі і завдання, такі як виявлення, блокування, відстеження та повідомлення про загрози. Це допоможе обрати найбільш відповідні технології. Крім того, глибокий аналіз ІТ-інфраструктури допоможе зрозуміти її тип, масштаб, важливість активів та вразливі місця.

Під час вибору технологій слід враховувати встановлені цілі, характеристики ІТ-інфраструктури, важливість активів, вразливості, а також фінансові можливості. Після цього слідують етапи налаштування технологій, включаючи налаштування правил для виявлення загроз, блокування та відстеження, що є ключовим для ефективності їх роботи. Оперативний моніторинг технологій включає аналіз звітів, блокування та відстеження загроз, дозволяючи своєчасно виявити та реагувати на загрози. У разі виявлення загрози, потрібно мати готові плани реакції, які можуть включати блокування, видалення або повідомлення про загрозу.

Підтримка та оновлення технологій також є важливими, оскільки вони забезпечують усунення помилок, вдосконалення функціональності та оновлення баз даних загроз і правил виявлення.

Крім специфічних рекомендацій, важливо пам'ятати, що технології виявлення загроз є лише частиною комплексної системи захисту ІТ-інфраструктури. Необхідне навчання персоналу та регулярне тестування технологій для забезпечення їх ефективності.

Сучасні системи виявлення та запобігання вторгнень на системному рівні (IDPS) активно використовують журнали подій для автоматичного виявлення атак, використовуючи при цьому складні математичні методи. Ці системи постійно моніторять системні журнали та файл безпеки, порівнюючи нові записи з відомими сигнатурами атак. У випадку виявлення збігу, IDPS сповіщає адміністратора або активує визначені механізми реагування [19]. Такі системи постійно вдосконалюються, інтегруючи нові методи виявлення, включаючи перевірку контрольних сум системних ключів та виконуваних файлів на наявність несанкціонованих змін.

З іншого боку, системи виявлення вторгнень мережевого рівня відрізняються своєю відносною економічністю, оскільки їм потрібно встановлювати датчики лише у ключових точках мережі. Вони також здатні виявляти атаки, ігноровані системами системного рівня, аналізуючи заголовки мережевих пакетів і вміст тіла даних. Ці системи можуть оперативно реагувати на атаки в реальному часі, важко для зловмисників видалити сліди їхньої присутності. Крім того, вони незалежні від операційної системи. IDPS системного рівня, з іншого боку, може точно визначати успішність атаки, моніторити конкретні хости та виявляти атаки, недоступні для мережевих систем. Вони також здатні працювати у мережах з шифруванням та комутацією без потреби в додатковому обладнанні.

Враховуючи ці переваги, майбутнє IDPS, ймовірно, буде полягати у поєднанні інтегрованих системних та мережевих компонентів. Такий синтез дозволить підвищити загальну ефективність захисту мережі від атак, забезпечивши при цьому більшу гнучкість та строгі правила безпеки.

На сучасному ринку IT-технологій представлена значна кількість програмних та апаратно-програмних комплексів систем виявлення та запобігання вторгненням (IDPS), серед яких можна виділити такі системи, як Kerio WinRoute Firewall, Snort, McAfee Entercept, ETrust Intrusion Detection, Symantec ManHunt. Однак, важливо зазначити, що розробники цих систем часто не надають об'єктивного опису їх переваг та недоліків, що ускладнює вибір для користувачів. З метою уніфікації тестування IDPS, розробляється єдиний стандарт.

Для об'єктивного порівняння IDPS використовуються такі показники [26]:

- **Клас виявлених атак:** Визначає, які типи атак здатний виявити IDPS, з урахуванням місцезнаходження об'єкта атаки, атакованого ресурсу, специфіки впливу на ресурс та ознаки розподіленого характеру нападу.
- **Рівень моніторингу системи:** Вказує на рівень, на якому система збирає дані для виявлення атаки. Може включати різні рівні спостереження, від хоста до мережевих хостів і додатків.
- **Метод виявлення вторгнень:** Ключовий показник, що включає методи виявлення аномалій та зловживань, та їхні додаткові характеристики, такі як ступінь спостереження, функція перевірки, адаптивність та стабільність.
- **Масштабованість:** Визначає можливості додавання нових мережевих ресурсів і каналів даних до аналізу та управління єдиною розподіленою системою.
- **Відкритість:** Визначає, наскільки відкритою є система для інтеграції інших методів виявлення вторгнень та сторонніх компонентів.
- **Формування адекватної реакції на напад:** Визначає наявність вбудованих механізмів для адекватної реакції на атаку та її реєстрацію.
- **Безпека:** Ступінь захисту IDPS від атак на його компоненти, включаючи захист інформації в обігу, стійкість до виходу з ладу компонентів і наявність слабких місць.

Таким чином, ідеальна система виявлення вторгнень повинна бути здатна розпізнавати всі класи атак, аналізувати поведінку захищеної системи на всіх рівнях, адаптуватися до невідомих атак, бути масштабованою та відкритою для інтеграції, забезпечувати вбудовані механізми реагування на вторгнення, а також бути захищеною від кібератак на компоненти.

3.2. Методики впровадження захисних систем

Впровадження систем безпеки - це складне завдання, яке починається з ретельної оцінки та аналізу ризиків. Цей початковий крок має вирішальне значення для виявлення потенційних загроз, вразливостей і наслідків інцидентів, що, в свою

чергу, допомагає визначити пріоритети у сфері безпеки. Заходи фізичної безпеки є фундаментальним аспектом цього процесу. Вони передбачають встановлення камер спостереження, систем сигналізації, систем контролю доступу, таких як ключові картки або біометричні дані, охоронне освітлення та фізичні бар'єри, такі як паркани, ворота або стовпчики. Основна мета цих заходів - стримувати, виявляти, затримувати та реагувати на фізичні загрози.

У сучасну цифрову епоху не менш важливими є заходи кібербезпеки. Вони включають впровадження брандмауерів, антивірусного програмного забезпечення, систем виявлення вторгнень і забезпечення безпечної мережевої архітектури. Регулярне оновлення програмного забезпечення та системні патчі мають вирішальне значення для підтримання надійної кібербезпеки.

Безпека даних і шифрування мають вирішальне значення для захисту конфіденційної інформації. Впровадження надійних протоколів шифрування даних як під час передачі, так і в стані спокою, а також надійних засобів автентифікації та контролю доступу є життєво важливими. Роль співробітників у підтримці безпеки неможливо переоцінити. Регулярні тренінги та програми підвищення обізнаності необхідні для того, щоб озброїти персонал знаннями для розпізнавання та уникнення потенційних загроз безпеці, таких як фішингові атаки або тактика соціальної інженерії. Розробка чітких політик і процедур безпеки та забезпечення їх дотримання є ключовим аспектом комплексної стратегії безпеки. Це включає визначення ролей, обов'язків, планів реагування на інциденти та проведення регулярних аудитів [32].

Регулярний аудит і тестування заходів безпеки за допомогою таких заходів, як тестування на проникнення і навчання з безпеки, мають вирішальне значення для виявлення вразливостей і забезпечення ефективності наявних заходів безпеки.

Інтеграція різних систем безпеки, таких як фізична та IT-безпека, може забезпечити більш цілісне рішення безпеки. Така інтеграція гарантує, що різні системи ефективно взаємодіють і працюють разом. Планування реагування на надзвичайні ситуації та інциденти є ще одним важливим елементом. Наявність чітко визначених планів реагування на різні типи інцидентів безпеки, такі як витік

даних або фізичне вторгнення, має важливе значення для швидкого та ефективного реагування з метою мінімізації збитків.

Нарешті, критично важливим є дотримання законодавчих і нормативних вимог. Системи та протоколи безпеки повинні відповідати відповідним законам, нормативним актам та галузевим стандартам, щоб уникнути юридичних зобов'язань та штрафів. Таким чином, впровадження систем безпеки - це багатогранний процес, який вимагає ретельного планування, регулярного навчання та оновлення, а також комплексного підходу для ефективного управління як фізичними, так і цифровими загрозами.

Методики впровадження захисних систем варіюються і в основному поділяються на адаптивні та плановані. Адаптивні методики передбачають поступове впровадження захисних систем відповідно до виявлених загроз, що забезпечує організації гнучкість та адаптивність до змін у сфері безпеки. Вони включають оцінку загроз, розробку плану впровадження, впровадження та оцінку ефективності системи захисту.

З іншого боку, плановані методики базуються на заздалегідь розробленому плані впровадження, що дозволяє забезпечити більшу передбачуваність і контроль. Вони включають розробку плану, підготовку, впровадження, тестування та введення системи захисту в експлуатацію.

Вибір між адаптивними та плановаными методиками залежить від складності системи захисту, розуміння загроз, фінансових можливостей та відповідності вимогам регуляторів. Адаптивні методики краще підходять для організацій з обмеженими фінансами, складною системою захисту і нестабільними загрозами. Плановані методики ефективні для організацій із достатніми фінансами, відносно простою системою захисту і стабільними загрозами.

Незалежно від обраної методики, важливо залучати кваліфікованих фахівців, планувати процес впровадження, проводити тестування та регулярно оновлювати систему захисту [32]. Такий підхід допоможе забезпечити ефективне впровадження захисних систем та захистити IT-інфраструктуру від різноманітних загроз, таких як віруси, шпигунське ПЗ, фішинг, атаки на мережеву інфраструктуру та

несанкціонований доступ. Вибір методики також залежить від типу та масштабу IT-інфраструктури, важливості IT-активів, бюджету та відповідності законодавчим вимогам.

3.3. Розробка комплексної стратегії захисту організації

З урахуванням надзвичайного зростання кібератак, організації, які впроваджують IoT, продовжують адаптуватися до проблем безпеки, які становлять загрозу їхньому бізнесу в динамічному конкурентному середовищі. Багато кібератак вдається уникнути технічних заходів забезпечення безпеки, використовуючи вразливості, пов'язані з людським фактором, такими як знання та навички в галузі безпеки, а також маніпуляції людськими чинниками для отримання несанкціонованого доступу до критично важливих промислових активів. Використання кількісного підходу (статистичного аналізу) дозволяє отримати кількісну оцінку потенційних здібностей кібербезпеки промислових суб'єктів, виявлення найменш захищених ланок в операційній сфері з найвищою ймовірністю кібератак та направлення зусиль на підвищення загального рівня безпеки. Участь людського фактору необхідна для доповнення існуючих технічних підходів до забезпечення безпеки в напрямку загальної кібербезпеки. Дослідники, такі як Баді та Лашкар [26], відзначають дві категорії факторів, що впливають на безпеку комп'ютерних систем: людський та організаційний. Зазначено, що з цих двох категорій людський фактор виявляється найбільш вагомим. Зусилля щодо забезпечення безпеки, з урахуванням людського фактора, можуть покращити можливості людських компонентів операційних технологій для розпізнавання кібернетичних загроз та ефективної реакції на них.

У сучасну цифрову епоху загрози кібербезпеці постійно розвиваються, тому для організацій як ніколи важливо інвестувати в навчання користувачів та програми підвищення обізнаності з питань безпеки. Ефективні програми можуть

допомогти працівникам розпізнавати та повідомляти про підозрілу активність, що в кінцевому підсумку захистить організацію від кібератак. Щоб ефективно вирішувати ризики безпеки, важливо розуміти найпоширеніші загрози, з якими стикаються користувачі. Таблиця 3.2. нижче наводить кілька поширених загроз та відповідних методів обізнаності:

Таблиця 3.2.

Поширені загрози безпеки та методи обізнаності

Загроза	Опис	Метод обізнаності
Фішинг	Спроби обманути користувачів, щоб вони розкрили конфіденційну інформацію, представившись легітимним джерелом, наприклад, електронними листами від банків або онлайн-сервісів.	Навчати користувачів розпізнавати фішингові електронні листи, перевіряючи на наявність терміновості, помилок у написанні, несподіваних вкладень та легітимності відправника.
Зловмисне програмне забезпечення	Зловмисне програмне забезпечення, призначене для пошкодження комп'ютерної системи, наприклад, віруси, черви та шпигунське програмне забезпечення.	Навчати користувачів бути обережними при відкритті вкладень та завантаженні файлів з невідомих джерел, а також використовувати антивірусне та анти-зловмисне програмне забезпечення.
Соціальне інжиніринг	Використання обману для manipulation користувачів до виконання дій, які можуть скомпрометувати їхню безпеку, наприклад, надання особистої інформації або натискання на шкідливі посилання.	Навчати користувачів бути обережними щодо технік соціальної інженерії, таких як підгодовування та підстановка, і уникати надання конфіденційної інформації людям, яких вони не знають і не довіряють.
Атаки на паролі	Спроби вгадати або зламати пароль користувача.	Навчати користувачів створювати сильні паролі з великими та малими літерами, цифрами та символами, і уникати використання одного пароля для декількох облікових записів.

Окрім розуміння загроз, дані можуть надати цінні уявлення про ефективність різних методів навчання. Таблиця 3.3. надає порівняння:

Таблиця 3.3.

Ефективність різних методів навчання користувачів

Метод навчання	**Ефективність**
Модулі електронного навчання	Помірна
Інтерактивні симуляції	Висока
Ігри	Висока
Вміст на основі відео	Висока
Реальні приклади та кейс-стадії	Висока

Як вказує таблиця, інтерактивні методи навчання, такі як симуляції, ігри та відео, зазвичай значно ефективніші, ніж традиційні модулі електронного навчання. Ці методи залучають користувачів і забезпечують більш запам'ятовується навчальний досвід. Для підтримки організації на шляху до підвищення обізнаності користувачів про безпеку є кілька цінних ресурсів. У Таблиці 3 наведено кілька ключових прикладів.

Таблиця 3.4.

Ресурси для підвищення обізнаності про безпеку

Ресурс	**Опис**
Проект безпеки відкритих веб-додатків (OWASP)	Надає ресурси та інформацію про безпеку веб-додатків.
Центр інтернет-безпеки (CIS)	Пропонує тести безпеки та найкращі практики.
Національний інститут стандартів і технологій (NIST)	Розробляє стандарти та рекомендації з кібербезпеки.
PhishMe	Проводить симуляції фішингу та навчання.
KnowBe4	Пропонує тренінги з підвищення обізнаності про безпеку та симуляції фішингу.
Інститут SANS	Проводить навчання та сертифікацію з кібербезпеки.

Використання цих ресурсів допоможе впроваджувати найкращі практики, бути в курсі нових загроз та отримати доступ до навчальних матеріалів для постійного вдосконалення вашої програми [35]. Конкретний приклад того, як дані можуть сприяти покращенню програми, розглянемо наступний скрипт Python для тесту на знання безпеки користувачів:

```
import random

# Define list of questions and answers
questions = [
    "What is the purpose of a firewall?",
    "What are some signs of a phishing email?",
    "How often should you change your password?",
    "What is the strongest type of password?",
    "What should you do if you suspect your computer is infected with malware?",
]

answers = [
    "To protect a computer network from unauthorized access.",
    "Urgent requests, misspelled words, and unexpected attachments.",
    "At least every three months.",
    "A long password with a mix of upper and lowercase letters, numbers, and symbols.",
    "Disconnect from the internet and run a scan with antivirus software.",
]

# Shuffle questions and answers
random.shuffle(questions)
random.shuffle(answers)

# Create a dictionary to store the correct answer for each question
correct_answers = dict(zip(questions, answers))
```

```
# Run the quiz
score = 0
for question in questions:
    user_answer = input(f"{question} ")
    if user_answer.lower() == correct_answers[question].lower():
        print("Correct!")
        score += 1
    else:
        print(f"Incorrect. The correct answer is: {correct_answers[question]}")

# Print the final score
print(f"You answered {score} out of {len(questions)} questions correctly.")
```

Це приклад скрипта на Python, який можна використовувати для створення тесту на обізнаність користувачів щодо безпеки. Скрипт можна легко адаптувати для включення більшої кількості запитань і різних типів запитань.

У Києві, Україна, існує ряд компаній, які пропонують послуги оцінки вразливостей та тестування на проникнення. При виборі компанії важливо враховувати її досвід, репутацію та методологію. Оцінка вразливостей та тестування на проникнення (VA/PT) є критично важливими заходами для організацій будь-якого розміру в сучасному ландшафті загроз. Регулярно проводячи такі оцінки, організації можуть проактивно виявляти, визначати пріоритети та усувати вразливості у своїх системах та мережах до того, як ними скористаються зловмисники [41].

Переваги регулярного проведення VA/PT:

1. Покращення стану безпеки: Регулярна перевірка на вразливості допомагає виявити та усунути вразливості до того, як ними скористаються зловмисники. Це зменшує ризик витоку даних, фінансових втрат та репутаційних збитків.

2. Покращена відповідність вимогам: Багато регуляторних вимог вимагають регулярного проведення VA/PT. Проведення цих оцінок допомагає організаціям продемонструвати дотримання відповідних норм.

3. Пріоритезація зусиль з виправлення ситуації: VA/PT надає чітку картину вразливостей за ступенем серйозності та потенціалом використання, що дозволяє організаціям визначати пріоритети для усунення недоліків і зосереджуватися на найбільш важливих питаннях у першу чергу.

4. Підвищення обізнаності: Регулярне проведення VA/PT допомагає підвищити рівень обізнаності про ризики безпеки серед працівників та керівництва, сприяючи розвитку культури безпеки в організації.

Методологія ОВД/ПТ

ОВД/ПТ включає в себе низку кроків:

1. Планування: Визначення обсягу оцінювання, визначення активів, що підлягають оцінюванню, та встановлення реалістичних цілей і термінів.

2. Оцінка вразливостей: Використовуйте автоматизовані інструменти та ручні методи для виявлення вразливостей у системах та додатках.

3. Тестування на проникнення: Спроба використати виявлені вразливості для імітації реальних атак та оцінки ефективності засобів контролю безпеки.

4. Звітування: Документування результатів VA/PT, включаючи виявлені вразливості, ступінь їх серйозності та рекомендовані кроки з їх усунення.

5. Усунення вразливостей: Своєчасне усунення виявлених вразливостей з урахуванням їхньої критичності та потенційного впливу.

Частота проведення ОВР/ПТ залежить від кількох факторів, таких як розмір організації, галузь, регуляторні вимоги та ландшафт загроз. Однак, як правило, рекомендується проводити ОВ/ФТ:

- Щонайменше щороку: для забезпечення постійного виявлення та усунення вразливостей.
- Після значних змін: для оцінки впливу змін на стан безпеки, наприклад, впровадження нових систем або додатків.

- Після інциденту безпеки: виявлення будь-яких вразливостей, які були використані, та впровадження коригувальних заходів.

Впроваджуючи комплексну та регулярну програму VA/PT, організації можуть значно покращити свій стан безпеки та зменшити ризик кібератак. Постійно оцінюючи та вдосконалюючи свою систему безпеки, ви зможете випереджати нові загрози та захищати цінні активи вашої організації. Оцінки уразливості та тестування на проникнення (VA/PT) є важливими заходами для організацій будь-якого розміру. Активно ідентифікуючи, пріоритизуючи та виправляючи уразливості в своїх системах і мережах, організації можуть значно знизити ризик кібератак. Python, завдяки своїм широким бібліотекам і простоті використання, може бути цінним інструментом у діяльності VA/PT [41].

Переваги використання Python для VA/PT:

- Велика екосистема бібліотек: Python пропонує різні бібліотеки, такі як requests, nmap, scapy, і beautifulsoup4, які можуть полегшити виконання різних завдань VA/PT, таких як сканування уразливості, розробка exploitів і аналіз мережі.
- Легкість автоматизації: Скриптові можливості Python дозволяють автоматизувати повторювані завдання, заощаджуючи час і забезпечуючи послідовність у процесах VA/PT.
- Швидке прототипування: Короткозорість і простий синтаксис Python дозволяють швидко розробляти власні інструменти та скрипти для конкретних потреб.
- Велика і активна спільнота: Python-спільнота надає обширну документацію, навчальні посібники та ресурси підтримки, що полегшує вивчення та використання бібліотек для VA/PT.

Таблиця 3.5.

Бібліотеки Python для VA/PT:

Бібліотека	**Функціональність**
requests	Виконує HTTP-запити та обробляє відповіді. Корисно для отримання даних веб-сторінки та взаємодії з API.
nmap	Виконує мережеве виявлення та сканування відкритих портів і служб.

scapy	Створює та аналізує мережеві пакети для виявлення уразливостей та розробки exploitів.
beautifulsoup4	Розпарсовує HTML- і XML-дані для автоматизованого сканування уразливостей веб-додатків.

Продовження таблиці 3.5.

Бібліотеки Python для VA/PT:

Скрипти Python для VA/PT:

Ось приклад скрипта Python, який демонструє простий сканер уразливості:

```
import requests

# Define the target URL
target_url = "https://example.com"

# Make an HTTP request
response = requests.get(target_url)

# Check for common vulnerabilities in the response
if "X-Powered-By" in response.headers:
    print(f"Warning: X-Powered-By header is present, potentially revealing the server software.")

if response.status_code == 404:
    print(f"Warning: The server doesn't handle 404 errors properly, potentially leading to directory listing vulnerabilities.")

# Further analysis and checks can be added...
```

Це базовий приклад, але він демонструє, як скрипти Python можна використовувати для автоматизації завдань сканування уразливості. З подальшим розвитком такі скрипти можна інтегрувати в більші рамки VA/PT для всебічних оцінок безпеки. Інсайти на основі даних: Бібліотеки Python, такі як pandas, можна

використовувати для аналізу та візуалізації даних, зібраних під час діяльності VA/PT. Це дозволяє краще зрозуміти виявлені вразливості, їхню серйозність і тенденції в часі. Ось приклад використання pandas для оцінки ризиків:

```
import pandas as pd

# Create a DataFrame of vulnerabilities with columns for severity, exploitability, and remediation effort
vulnerability_data = [
    {"severity": "High", "exploitability": "Easy", "remediation_effort": "Medium"},
    {"severity": "Medium", "exploitability": "Medium", "remediation_effort": "Low"},
    ...
]

df = pd.DataFrame(vulnerability_data)

# Calculate risk score based on severity, exploitability, and remediation effort
df["risk_score"] = df["severity"] * df["exploitability"] * df["remediation_effort"]

# Analyze the risk score distribution and prioritize remediation efforts
print(df.describe())
```

Використовуючи Python для аналізу даних, організації можуть приймати обґрунтовані рішення щодо пріоритетності усунення вразливостей на основі факторів ризику. Універсальність і простота використання Python роблять його потужним інструментом для діяльності з антикорупційного аудиту та антикорупційного захисту. Використовуючи бібліотеки та скрипти, організації можуть автоматизувати завдання, підвищити ефективність та отримати цінну інформацію про стан своєї безпеки. Впровадивши Python у процеси VA/PT, можна покращити свою систему безпеки та захистити свої критичні активи від кіберзагроз. "Люди", відомі також як "робоча сила", часто є найвразливішим елементом в ланцюгу операційної безпеки, а потенціал безпеки організації такий

самий слабкий, як його найвразливіший компонент. Розуміння можливостей безпеки працівників, які випливають з їхніх знань і навичок, визначення стану безпеки організації, орієнтованого на персонал, і визначення конкретних найбільш вразливих елементів робочої сили (найвразливішої ланки) в системі, є важливим для оцінки загального рівня безпеки. Найвразливішою ланкою є персонал з найменшими знаннями і практичними навичками в галузі безпеки, необхідними для досягнення цілей безпеки. По суті, найвразливішою ланкою є найменш захищені особи в операційній сфері, які мають найбільшу ймовірність стати жертвами кібератак [8]. Ці людські елементи представляють собою найлегший вектор для атак і становлять найбільш вразливу точку входу в систему, незалежно від будь-яких інших заходів безпеки. Виявлення цих найвразливіших місць через оцінку є важливою складовою стратегії забезпечення безпеки. Виявлення та усунення найвразливіших ланок еквівалентно підняттю планки безпеки працівників організації.

Дослідження показують, що здібності людей взаємозалежні, тому середні значення можна використовувати для узгодженого визначення загального потенціалу безпеки [27]. Є розумно розглядати кожного користувача як незалежного і потенційного вектора для входу в систему, незалежно від інших. Таким чином, підвищення найвразливішої ланки вводиться в процес оцінки можливостей, коли узгоджені рейтинги можливостей безпеки неявно вказують на заходи слабкості або уразливості перед кібератаками. Сукупність різних значень в наборі рейтингів можливостей вказує на різні незалежні вразливості або слабкі місця, які можуть сприяти успішним кібератакам.

Концепція захисту безпеки, у поєднанні з базовими показниками вразливості та кількісним представленням, може сприяти простій і чіткій ідентифікації потенційних слабких ланок. Нова схема оцінки є п'ятиетапним процесом оцінки можливостей кібербезпеки персоналу, який включає в себе визначення, збір даних, формулювання, уявлення та атрибуцію. Оцінка безпеки персоналу повинна ґрунтуватися на конкретних політиках та вимогах безпеки, відповідно до стандартів та передових методів. Існує кілька стандартів безпеки, таких як NIST SP

800-53, ISO/IEC 27001, ISO/IEC 27002, які містять розділи з рекомендаціями відповідно до вимог і керівних принципів [33].

- NIST SP 800-53 - це стандарт Національного інституту стандартів і технологій США (NIST), який містить рекомендації щодо управління інформаційною безпекою. Розділ 8 цього стандарту містить рекомендації щодо оцінки безпеки персоналу.
- ISO/IEC 27001 - це міжнародний стандарт, який визначає вимоги до системи управління інформаційною безпекою (СУІБ). Розділ 8 цього стандарту також містить рекомендації щодо оцінки безпеки персоналу.
- ISO/IEC 27002 - це міжнародний стандарт, який містить керівні принципи з управління інформаційною безпекою. Розділ 8 цього стандарту також містить рекомендації щодо оцінки безпеки персоналу.

Ці стандарти містять рекомендації щодо таких аспектів оцінки безпеки персоналу:

- Цілі оцінки - оцінка безпеки персоналу повинна мати чіткі цілі, які визначатимуть, що саме потрібно оцінити.
- Обсяг оцінки - оцінка повинна охоплювати всіх працівників, які мають доступ до конфіденційної інформації або систем.
- Методи оцінки - оцінка може проводитися за допомогою різних методів, таких як опитування, інтерв'ю, тестування знань та навичок.
- Результати оцінки - результати оцінки повинні бути документовані та використані для розробки заходів щодо покращення безпеки.

Оцінка безпеки персоналу є важливим компонентом загальної програми управління інформаційною безпекою. Вона допомагає організаціям оцінити ризики, пов'язані з персоналом, та розробити заходи щодо їх зменшення. Приклад розгортання захисту організації від кіберзагроз включає ряд ключових кроків і рішень. Спочатку важливо зосередитися на фізичній безпеці, що охоплює контроль доступу до приміщень, де знаходяться сервери та інше важливе обладнання. Потім налаштувати файрволи та антивірусні системи для захисту мережі і пристроїв від шкідливих програм і несанкціонованого доступу.

Важливим елементом є встановлення систем виявлення та запобігання вторгненням (IDS/IPS), які моніторять мережевий трафік на предмет підозрілої активності. Це допомагає швидко ідентифікувати та реагувати на потенційні загрози. Шифрування даних є критично важливим для захисту конфіденційної інформації, особливо при зберіганні та передачі через мережу. Також важливо регулярно робити резервні копії важливих даних для забезпечення їх відновлення у разі втрати або пошкодження.

Управління ідентифікацією та доступом, включаючи використання сильних паролів і двофакторної аутентифікації, є ключовим для запобігання несанкціонованому доступу до систем. Крім того, важливо проводити регулярні навчання з кібербезпеки для співробітників, адже людський фактор часто є найслабшою ланкою в системі безпеки. Це допомагає зменшити ризик від соціальної інженерії та фішингових атак.

Нарешті, рекомендується впровадити політику реагування на інциденти, яка визначає процедури для реагування на безпекові порушення. Це допомагає забезпечити оперативне виявлення, ізоляцію та вирішення інцидентів, мінімізуючи потенційну шкоду. Цей багаторівневий підхід до захисту допомагає створити міцну оборону проти різноманітних кіберзагроз, адаптовану до специфіки конкретної організації.

ВИСНОВКИ

У ході дослідження технології виявлення загрозливої діяльності і поведінки в ІТ середовищі було проведено аналіз теоретичних основ, здійснено аналіз проблеми виявлення загрозливої діяльності і поведінки в ІТ середовищі, розроблено рекомендації щодо виявлення та запобігання сучасним стійким загрозам.

1. Аналіз теоретичних основ

У рамках цього завдання було проведено аналіз поняття та класифікації загрозливої діяльності і поведінки в ІТ середовищі, впливу загрозливої діяльності і поведінки на ІТ-системи і організації, основних тенденцій розвитку загрозливої діяльності і поведінки в ІТ середовищі, а також технологій виявлення загрозливої діяльності і поведінки в ІТ середовищі. До загрозливої діяльності і поведінки відносяться атаки на ІТ-системи, несанкціонований доступ до інформації, поширення шкідливого програмного забезпечення, зловживання ІТ-ресурсами та інші. Загрозлива діяльність і поведінка може мати серйозні наслідки для ІТ-систем і організацій, такі як пошкодження або знищення інформації, відмова в обслуговуванні, фінансові збитки, шкода репутації. Основними тенденціями розвитку загрозливої діяльності і поведінки в ІТ середовищі є зростання складності та спеціалізації атак, зростання використання автоматизованих інструментів для здійснення атак, зростання використання соціальної інженерії для залучення жертв, зростання масштабів атак.

2. Аналіз проблеми виявлення загрозливої діяльності і поведінки в ІТ середовищі

Аналіз проблеми виявлення загрозливої діяльності і поведінки в ІТ середовищі показав, що ця проблема є актуальною та складною. Зростаюча складність ІТ-інфраструктури, а також розвиток нових технологій, які використовуються зловмисниками, ускладнюють виявлення загроз.

На основі проведеного дослідження було розроблено наступні рекомендації щодо виявлення та запобігання сучасним стійким загрозам:

- Впровадження багаторівневого підходу до безпеки

Впровадження багаторівневого підходу до безпеки передбачає використання різних методів і технологій виявлення загроз, які діють на різних рівнях ІТ-системи. Це дозволяє підвищити ефективність виявлення загроз і зменшити ризик їх уникнення.

- Покращення навчання та обізнаності користувачів

Підвищення обізнаності користувачів про загрози інформаційної безпеки та способи їх захисту є важливим фактором підвищення рівня безпеки ІТ-систем. Користувачі повинні бути навчені розпізнавати загрози та знати, як діяти в разі інциденту безпеки.

- Проведення регулярної оцінки вразливостей та тестування на проникнення

Регулярна оцінка вразливостей дозволяє виявити уразливості в ІТ-системах, які можуть бути використані зловмисниками. Тестування на проникнення дозволяє перевірити, чи можуть зловмисники отримати доступ до ІТ-системи і здійснити атаку.

- Обмін даними про загрози та співпраця з іншими організаціями

Обмін даними про загрози та співпраця з іншими організаціями дозволяє отримувати інформацію про останні загрози та розробляти спільні заходи реагування на інциденти безпеки. Запропоновані рекомендації можуть бути використані організаціями для підвищення рівня безпеки своїх ІТ-систем і зменшення ризику інцидентів безпеки.

Висновки та пропозиції. Проведене дослідження дозволяє зробити наступні висновки:

- Технологія виявлення загрозливої діяльності і поведінки в ІТ середовищі є важливим компонентом системи захисту ІТ-активів організації.

- Для ефективного виявлення загроз необхідно використовувати багаторівневий підхід, який включає в себе використання різних методів та інструментів.
- Важливо регулярно оновлювати та налаштовувати захисні системи для забезпечення їх ефективності.

На основі отриманих результатів дослідження було розроблено ряд рекомендацій, які можуть бути використані організаціями для підвищення ефективності виявлення загроз.

ПЕРЕЛІК ПОСИЛАНЬ

1. Ісак Л. Інформаційні технології. *Grail of science*. 2023. № 30. С. 187–191. URL: https://doi.org/10.36074/grail-of-science.04.08.2023.030 (дата звернення: 07.12.2023).

2. Кушнарьов В. В. Інформаційна освіта України та кібербезпека в сучасному інформаційному просторі. *Міжкультурна комунікація в контексті глобалізаційного діалогу: стратегії розвитку. ч 3*. 2022. URL: https://doi.org/10.36059/978-966-397-281-7-67 (дата звернення: 07.12.2023).

3. Мєшкова-Кравченко Н. В., Тарасюк А. В. Оцінка економічної безпеки підприємства. *Вісник Херсонського національного технічного університету*. 2021. Т. 76, № 1. С. 204–212. URL: https://doi.org/10.35546/kntu2078-4481.2021.1.26 (дата звернення: 07.12.2023).

4. Сопілко І. Інформаційна безпека та кібербезпека: порівняльно-правовий аспект. *Scientific works of national aviation university. series: law journal "air and space law"*. 2021. Т. 2, № 59. С. 110–115. URL: https://doi.org/10.18372/2307-9061.59.15603 (дата звернення: 07.12.2023).

5. Нечипоренко І. Д. Кібербезпека: захист від фішингу : thesis. 2018. URL: http://essuir.sumdu.edu.ua/handle/123456789/66886 (дата звернення: 07.12.2023).

6. Плєхова Г., Суханова Н., Левтеров А. Кібербезпека: загрози, рішення. *Theoretical foundations in economics and management*. 2022. P. 681–692. URL: https://doi.org/10.46299/isg.2022.mono.econ.2.9.6 (date of access: 07.12.2023).

7. Татомир І. Кібербезпека університетів як спосіб протидії фішинговому шахрайству. *Економічний дискурс*. 2020. Вип. 1. С. 59–67.

8. Чубаєвський В. Методи управління корпоративною інформаційною безпекою. *Економіка та суспільство*. 2022. № 43. URL: https://doi.org/10.32782/2524-0072/2022-43-49 (дата звернення: 06.12.2023).

9. Ani U. D., He H., Tiwari A. Human factor security: evaluating the cybersecurity capacity of the industrial workforce. *Journal of systems and information*

technology. 2019. Vol. 21, no. 1. P. 2–35. URL: https://doi.org/10.1108/jsit-02-2018-0028 (date of access: 06.12.2023).

10. Bykowski K. Building an IT incident response plan. *AI Enabled Security Automation*. URL: https://swimlane.com/blog/it-incident-response-plan/ (date of access: 06.12.2023).

11. Cis. *CIS*. URL: https://www.cisecurity.org/ (date of access: 06.12.2023).

12. Daniel Ani U. P., He H. M., Tiwari A. Human capability evaluation approach for cyber security in critical industrial infrastructure. *Advances in intelligent systems and computing*. Cham, 2016. P. 169–182. URL: https://doi.org/10.1007/978-3-319-41932-9_14 (date of access: 05.12.2023).

13. Da Veiga A., Eloff J. H. P. A framework and assessment instrument for information security culture. *Computers & security*. 2010. Vol. 29, no. 2. P. 196–207. URL: https://doi.org/10.1016/j.cose.2009.09.002 (date of access: 08.12.2023).

14. Early warning threat detection - threatmark. *ThreatMark*. URL: https://www.threatmark.com/use-cases/early-warning-threat-detection/ (date of access: 20.12.2023).

15. Frąckiewicz M. Хмарні обчислення та безпека хмарних програм: як забезпечити безпеку програм у хмарі. *TS2 SPACE*. URL: https://ts2.space/uk/хмарні-обчислення-та-безпека-хмарних-2/#gsc.tab=0 (дата звернення: 06.12.2023).

16. Geborkoff J. The crucial role of AI in cybersecurity: a necessity for modern defense. *LinkedIn: Log In or Sign Up*. URL: https://www.linkedin.com/pulse/crucial-role-ai-cybersecurity-necessity-modern-jesse-geborkoff-y3zhc#:~:text=These%20threats%20often%20operate%20stealthily,cybersecurity%20approaches%20are%20frequently%20overwhelmed. (date of access: 05.12.2023).

17. Labs P. What is security posture?. *THE COMPLETE SECURITY VALIDATION PLATFORM*. URL: https://www.picussecurity.com/resource/glossary/what-is-security-posture#:~:text=As%20the%20first%20line%20of,latest%20threats%20and%20best%20practices. (date of access: 05.12.2023).

18. Losinskyi K. Overview of the core enterprise security levels. *Infopulse*. URL: https://www.infopulse.com/blog/enterprise-security-levels-overview#:~:text=To%20mitigate%20risks%20and%20reduce,or%20defense-in-depth. (date of access: 06.12.2023).

19. Mwim E. N., Mtsweni J. Systematic review of factors that influence the cybersecurity culture. *Human aspects of information security and assurance*. Cham, 2022. P. 147–172. URL: https://doi.org/10.1007/978-3-031-12172-2_12 (date of access: 06.12.2023).

20. National institute of standards and technology. *NIST*. URL: https://www.nist.gov/ (date of access: 04.12.2023).

21. OWASP foundation, the open source foundation for application security | OWASP foundation. *OWASP Foundation, the Open Source Foundation for Application Security | OWASP Foundation*. URL: https://owasp.org/ (date of access: 06.12.2023).

22. Security threats of Internet-reachable ICS / S. Abe et al. *2016 55th annual conference of the society of instrument and control engineers of japan (SICE)*, Tsukuba, Japan, 20–23 September 2016. 2016. URL: https://doi.org/10.1109/sice.2016.7749239 (date of access: 06.12.2023).

23. Swanagan M. Types of security controls explained. *PurpleSec*. URL: https://purplesec.us/security-controls/#:~:text=Layering%20Security%20Controls&text=Defense-in-depth%20is%20a,a%20breach%20in%20your%20systems. (date of access: 06.12.2023).

24. Varela-Vaca A. J., Gasca R. M. Towards the automatic and optimal selection of risk treatments for business processes using a constraint programming approach. *Information and software technology*. 2013. Vol. 55, no. 11. P. 1948–1973. URL: https://doi.org/10.1016/j.infsof.2013.05.007 (date of access: 04.12.2023).

25. Young C. S. Information technology risk factors. *Information security science*. 2016. P. 251–261. URL: https://doi.org/10.1016/b978-0-12-809643-7.00011-5 (date of access: 08.12.2023).

26. An effective cybersecurity training model to support an organizational awareness program / R. Sabillon et al. *Journal of cases on information technology*. 2019.

Vol. 21, no. 3. P. 26–39. URL: https://doi.org/10.4018/jcit.2019070102 (date of access: 08.12.2023).

27. Buford J. F. K. Cyber security, situation management, and impact assessment II and visual analytics for homeland defense and security II: 5 and 8-9 April 2010, Orlando, Florida, United States. Bellingham, Wash : SPIE, 2010.

28. Chebib T. Digital identity: a human-centered risk awareness study. *Muma business review*. 2021. Vol. 5. P. 031–033. URL: https://doi.org/10.28945/4826 (date of access: 04.12.2023).

29. Darem A. Anti-Phishing awareness delivery methods. *Engineering, technology & applied science research*. 2021. Vol. 11, no. 6. P. 7944–7949. URL: https://doi.org/10.48084/etasr.4600 (date of access: 04.12.2023).

30. Desman M. B. Building an information security awareness program. London : Taylor and Francis, 2001.

31. Geeks of Gurukul. Python VS java. *LinkedIn: Log In or Sign Up*. URL: https://www.linkedin.com/pulse/python-vs-java-geeks-of-gurukul#:~:text=Community%20and%20community%20support,share%20knowledge%20and%20solve%20problems. (date of access: 07.12.2023).

32. Gilliam B. P. Threat intelligence in support of cyber situation awareness. 2017. URL: https://scholarworks.waldenu.edu/dissertations/4493 (date of access: 08.12.2023).

33. Goode J. Comparing training methodologies on employee's cybersecurity countermeasures awareness and skills in traditional vs. socio-technical programs : dissertation. 2018. URL: https://nsuworks.nova.edu/gscis_etd/1045 (date of access: 07.12.2023).

34. Hacker Combat™. Cybersecurity isn't just an "IT problem". *LinkedIn: Log In or Sign Up*. URL: https://www.linkedin.com/pulse/cybersecurity-isnt-just-problem-hacker-combat-cybersecurity-commun#:~:text=In%20this%20collective%20approach,%20cybersecurity,is%20both%20inadequate%20and%20shortsighted. (date of access: 07.12.2023).

35. Haney J. The federal cybersecurity awareness programs:. Gaithersburg, MD : National Institute of Standards and Technology, 2022. URL: https://doi.org/10.6028/nist.ir.8420 (date of access: 06.12.2023).

36. Kim L. Cybersecurity awareness. *Nursing*. 2017. Vol. 47, no. 6. P. 65–67. URL: https://doi.org/10.1097/01.nurse.0000516242.05454.b4 (date of access: 06.12.2023).

37. Lee N. Counterterrorism and cybersecurity: total information awareness. New York, NY : Springer New York, 2013. 234 p.

38. Lima A. J. C. Advanced persistent threats : master's thesis. 2015. URL: http://hdl.handle.net/10451/20168 (date of access: 05.12.2023).

39. Managing information security risk :. Gaithersburg, MD : National Institute of Standards and Technology, 2011. URL: https://doi.org/10.6028/nist.sp.800-39 (date of access: 08.12.2023).

40. Measuring the effectiveness of security awareness programs: what you need to know. *CybSafe*. URL: https://www.cybsafe.com/blog/measuring-the-effectiveness-of-security-awareness-training/ (date of access: 06.12.2023).

41. Pack J. Situational awareness for SCADA systems. *CyberSec '18: fifth cybersecurity symposium*, Coeur d' Alene Idaho. New York, NY, USA, 2018. URL: https://doi.org/10.1145/3212687.3212865 (date of access: 05.12.2023).

42. Poston H. E. Python for cybersecurity. Wiley & Sons, Limited, John, 2022.

43. Price C. Security: an introduction. *Security journal*. 2012. Vol. 25, no. 3. P. 287–289. URL: https://doi.org/10.1057/sj.2012.17 (date of access: 08.12.2023).

44. Python A. Myth no 3: the vulnerability of the west to terrorism. *Debunking seven terrorism myths using statistics*. 2020. P. 35–44. URL: https://doi.org/10.1201/9781003034230-4 (date of access: 08.12.2023).

45. Rainbow Secure. The importance of cybersecurity awareness for businesses. *LinkedIn: Log In or Sign Up*. URL: https://www.linkedin.com/pulse/importance-cybersecurity-awareness-businesses-rainbowsecure#:~:text=There%20are%20several%20reasons%20why,leading%20cause%20of%20data%20breaches. (date of access: 07.12.2023).

46. Sebastian A. What is VAPT and why VAPT important for your business?. *LinkedIn: Log In or Sign Up*. URL: https://www.linkedin.com/pulse/what-vapt-why-important-your-business-alvin-sebastian#:~:text=By%20regularly%20conducting%20VAPT,%20organizations,damage%20to%20the%20company's%20reputation. (date of access: 07.12.2023).

47. Security awareness training: why should your organization invest in it?. *enVista*. URL: https://envistacorp.com/blog/what-is-security-awareness-training-the-importance-and-types/#:~:text=Continuous%20Training&text=It's%20important%20to%20note%20that,changes%20in%20the%20threat%20landscape. (date of access: 07.12.2023).

48. Singgalen Y. A., Purnomo H. D., Sembiring I. Exploring msmes cybersecurity awareness and risk management : information security awareness. *IJCCS (indonesian journal of computing and cybernetics systems)*. 2021. Vol. 15, no. 3. P. 233. URL: https://doi.org/10.22146/ijccs.67010 (date of access: 05.12.2023).

49. Softić J., Vejzović Z. Impact of vulnerability assesment and penetration testing (VAPT) on operating system security. *2023 22nd international symposium INFOTEH-JAHORINA (INFOTEH)*, East Sarajevo, Bosnia and Herzegovina, 15–17 March 2023. 2023. URL: https://doi.org/10.1109/infoteh57020.2023.10094095 (date of access: 05.12.2023).

50. Unic V. Vulnerability testing: methods, tools, and 10 best practices. *Bright Security*. URL: https://brightsec.com/blog/vulnerability-testing-methods-tools-and-10-best-practices/#:~:text=Automated%20tools%20can%20quickly%20identify,impact,%20and%20ease%20of%20exploitation. (date of access: 07.12.2023).

51. van Loenen J. Information security awareness. *Research world*. 2015. Vol. 2015, no. 54. P. 53. URL: https://doi.org/10.1002/rwm3.20288 (date of access: 05.12.2023).

52. Vulnerability assessment and penetration testing - breachlock. *BreachLock*. URL: https://www.breachlock.com/resources/blog/vulnerability-assessment-and-penetration-

testing/#:~:text=In%20today's%20digital%20landscape,%20cybersecurity,of%20a%20comprehensive%20security%20strategy. (date of access: 07.12.2023).

53. Vulnerability assessment and penetration testing (VAPT) - outsourced IT support services company in singapore and malaysia. *Outsourced IT Support Services Company Singapore - Win-Pro*. URL: https://winpro.com.sg/vulnerability-assessment-penetration-testing-vapt/#:~:text=How%20often%20should%20VA%20and,the%20ever-evolving%20threat%20landscape. (date of access: 04.12.2023).

54. Wood C. Information security awareness raising methods. *Computer fraud & security bulletin*. 1995. Vol. 1995, no. 6. P. 13–15. URL: https://doi.org/10.1016/0142-0496(95)80197-9 (date of access: 04.12.2023).

ДОДАТКИ

Додаток А

Рис. 2.1. Схема роботи ThreatMark [14]

Додаток Б

Таблиця 2.1.

Порівняння APT атак із традиційними атаками

Характеристика	**APT атака**	**Традиційна атака**
Порушник	Визначена високоорганізована група людей	Одна або декілька людей
Ціль	Конкретні організації, урядові установи, комерційні підприємства	Невизначена, переважно індивідуальна система
Мета	Фінансові вигоди, конкурентні та стратегічні переваги	Фінансові вигоди, демонстрація здібностей
Підхід	Неодноразові спроби, пристосовуються до опору захисним засобам, тривалий термін	Короткострокова, одноразова

Додаток В

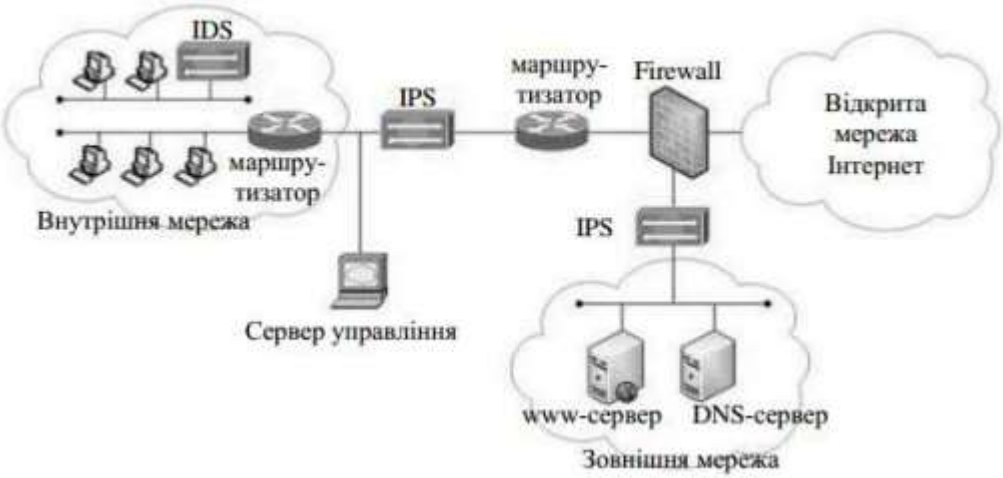

Рис. 2.2. Схема розміщення IDPS у мережі

Додаток Д

Таблиця 3.2.

Поширені загрози безпеки та методи обізнаності

Загроза	Опис	Метод обізнаності
Фішинг	Спроби обманути користувачів, щоб вони розкрили конфіденційну інформацію, представившись легітимним джерелом, наприклад, електронними листами від банків або онлайн-сервісів.	Навчати користувачів розпізнавати фішингові електронні листи, перевіряючи на наявність терміновості, помилок у написанні, несподіваних вкладень та легітимності відправника.
Зловмисне програмне забезпечення	Зловмисне програмне забезпечення, призначене для пошкодження комп'ютерної системи, наприклад, віруси, черви та шпигунське програмне забезпечення.	Навчати користувачів бути обережними при відкритті вкладень та завантаженні файлів з невідомих джерел, а також використовувати антивірусне та анти-зловмисне програмне забезпечення.
Соціальне інжиніринг	Використання обману для manipulation користувачів до виконання дій, які можуть скомпрометувати їхню безпеку, наприклад, надання особистої інформації або натискання на шкідливі посилання.	Навчати користувачів бути обережними щодо технік соціальної інженерії, таких як підгодовування та підстановка, і уникати надання конфіденційної інформації людям, яких вони не знають і не довіряють.
Атаки на паролі	Спроби вгадати або зламати пароль користувача.	Навчати користувачів створювати сильні паролі з великими та малими літерами, цифрами та символами, і уникати використання одного пароля для декількох облікових записів.

Додаток К

Таблиця 3.3.

Ефективність різних методів навчання користувачів

Метод навчання	**Ефективність**
Модулі електронного навчання	Помірна
Інтерактивні симуляції	Висока
Ігри	Висока
Вміст на основі відео	Висока
Реальні приклади та кейс-стадії	Висока

Додаток Л

Таблиця 3.4.

Ресурси для підвищення обізнаності про безпеку

Ресурс	**Опис**
Проект безпеки відкритих веб-додатків (OWASP)	Надає ресурси та інформацію про безпеку веб-додатків.
Центр інтернет-безпеки (CIS)	Пропонує тести безпеки та найкращі практики.
Національний інститут стандартів і технологій (NIST)	Розробляє стандарти та рекомендації з кібербезпеки.
PhishMe	Проводить симуляції фішингу та навчання.
KnowBe4	Пропонує тренінги з підвищення обізнаності про безпеку та симуляції фішингу.
Інститут SANS	Проводить навчання та сертифікацію з кібербезпеки.

Додаток М

Таблиця 3.5.

Бібліотеки Python для VA/PT:

Бібліотека	**Функціональність**
requests	Виконує HTTP-запити та обробляє відповіді. Корисно для отримання даних веб-сторінки та взаємодії з API.
nmap	Виконує мережеве виявлення та сканування відкритих портів і служб.
scapy	Створює та аналізує мережеві пакети для виявлення уразливостей та розробки exploitів.
beautifulsoup4	Розпарсовує HTML- і XML-дані для автоматизованого сканування уразливостей веб-додатків.