МІНІСТЕРСТВО ОСВІТИ ТА НАУКИ УКРАЇНИ

ВИЩИЙ НАВЧАЛЬНИЙ ЗАКЛАД «УНІВЕРСИТЕТ «КРОК»

Фаховий коледж Університету «КРОК»

ДИПЛОМНА РОБОТА

за темою

«Дослідження впливу кібератак у 21 столітті та запровадження мір кібербезпеки»

Студент 4 курсу групи	Керівник дипломної роботи
ІПЗ-20к-1	к.т.н., доцент
	(посада керівника)
Цемах Артур Романович	**Чернозубкін Ігор Олександрович**
(прізвище, ім'я та по-батькові студента)	(прізвище, ім'я та по-батьковікерівника)
	До захисту
	(резолюція «До захисту»)
(підпис студента)	10.06.24 (дата)
	(підпис викладача)

Київ, 2024 рік

СКОРОЧЕННЯ

DDoS (Distributed Denial of Service) - Розподілене відмовлення в обслуговуванні. Атака, яка передбачає перевантаження цільової системи великою кількістю запитів з багатьох джерел, що призводить до її недоступності.

IDS (Intrusion Detection System) - Система виявлення вторгнень. Програмне або апаратне забезпечення, яке моніторить мережу або систему на наявність шкідливої активності або порушень політики безпеки.

ПЗ (Програмне забезпечення) - Програмне забезпечення. Сукупність програмних інструментів, які використовуються для виконання конкретних завдань на комп'ютері.

Ransomware - Програмне забезпечення-вимагач. Тип шкідливого програмного забезпечення, яке блокує доступ до даних користувача або системи і вимагає викуп за відновлення доступу.

Малваре (Malware) - Шкідливе програмне забезпечення. Будь-яке програмне забезпечення, створене для пошкодження або несанкціонованого доступу до комп'ютерних систем.

Фішинг (Phishing) - Викрадення даних через підробні веб-сайти. Метод соціальної інженерії, що використовується для викрадення конфіденційної інформації, такої як паролі та дані кредитних карт, шляхом видачі себе за довірені джерела.

SQL (Structured Query Language) - Структурована мова запитів. Мова програмування, яка використовується для управління та маніпулювання реляційними базами даних.

IoT (Internet of Things) - Інтернет речей. Мережа фізичних пристроїв, транспортних засобів, побутових приладів та інших предметів, вбудованих з електронікою, програмним забезпеченням, сенсорами та мережевим підключенням, що дозволяє цим об'єктам збирати і обмінюватися даними.

VPN (Virtual Private Network) - Віртуальна приватна мережа. Технологія, яка створює безпечне з'єднання через менш безпечну мережу, наприклад, інтернет.

APT (Advanced Persistent Threat) - Персистентна цілеспрямована загроза. Комплекс тривалих і цілеспрямованих атак, зазвичай здійснюваних національними державами або організаціями, для доступу до конфіденційної інформації.

AV (Antivirus) – Антивірус. Програмне забезпечення, яке виявляє, запобігає та видаляє шкідливі програми з комп'ютерних систем.

SIEM (Security Information and Event Management) - Управління інформацією та подіями безпеки. Платформа, яка забезпечує реальний час аналізу подій безпеки, що генеруються мережевим обладнанням та додатками.

CISO (Chief Information Security Officer) - Головний офіцер з інформаційної безпеки. Високопоставлений керівник, відповідальний за розробку та впровадження інформаційної безпеки у компанії.

SCADA (Supervisory Control and Data Acquisition) - Система диспетчерського управління та збору даних.

USB (Universal Serial Bus) - Універсальна послідовна шина.

PLC (Programmable Logic Controller) - Програмований логічний контролер.

IDS (Intrusion Detection System) – система виявлення вторгнень

IPS (Intrusion Prevention System) – система запобігання вторгнень

DDoS (Distributed Denial of Service) – розподілене відмовлення в обслуговуванні

C&C (Command and Control) – командно-контрольний сервер

ЗМІСТ

ВСТУП

У сучасному світі, де інформаційні технології займають ключове місце в житті суспільства, питання кібербезпеки стає все більш актуальним. З розвитком цифрових технологій зростає і кількість кібератак, які спричиняють значні збитки як для окремих користувачів, так і для організацій та держав. Атаки на критичну інфраструктуру, викрадення конфіденційної інформації, поширення шкідливого програмного забезпечення — це лише декілька прикладів загроз, з якими стикається сучасне суспільство. Тому дослідження впливу кібератак у 21 столітті та розробка ефективних заходів кібербезпеки є вкрай необхідними для забезпечення стабільності та безпеки цифрового простору.

Метою даної дипломної роботи є аналіз впливу кібератак у 21 столітті та розробка рекомендацій щодо впровадження ефективних заходів кібербезпеки. Для досягнення поставленої мети були визначені наступні завдання:

- Провести огляд і класифікацію основних видів кібератак та їх наслідків.
- Вивчити економічні, соціальні та політичні аспекти впливу кібератак.
- Проаналізувати сучасні методи захисту від кібератак та оцінити їх ефективність.
- Розробити рекомендації щодо вдосконалення системи кібербезпеки на різних рівнях.

У ході дослідження використовувалися різноманітні методи, що дозволили комплексно підходити до вирішення поставлених завдань. Основні методи дослідження включають:

- Аналіз літературних джерел: Вивчення наукових статей, звітів, нормативних документів та інших публікацій, присвячених питанням кібербезпеки.
- Статистичний аналіз: Збір і аналіз даних про кібератаки, їх частоту, характер і наслідки.
- Моделювання та симуляція: Створення моделей кібератак і систем захисту для оцінки їх ефективності в різних сценаріях.
- Експертні оцінки: Залучення фахівців у галузі кібербезпеки для отримання експертних висновків і рекомендацій.

Дипломна робота складається з чотирьох основних розділів, висновків, переліку використаних джерел та додатків. У першому розділі представлений аналіз існуючої інформації щодо теми дослідження, включаючи порівняльний аналіз існуючих рішень та їх ефективності. Другий розділ присвячений проектним і технічним рішенням у сфері кібербезпеки, розглядаються різні види забезпечення, такі як інформаційне, математичне та програмне. У третьому розділі детально описуються розроблені рекомендації щодо вдосконалення заходів кібербезпеки, а також представлено результати моделювання та симуляцій. Четвертий розділ містить практичні рекомендації щодо впровадження розроблених заходів у реальних умовах.

Завершується робота висновками, в яких підведено підсумки дослідження, сформульовані основні висновки та рекомендації. У додатках наведено додаткові матеріали, які доповнюють основний зміст роботи, зокрема графіки, таблиці, приклади програмного коду та документація. Таким чином, дана дипломна робота має на меті не лише аналіз сучасного стану кібербезпеки, але й розробку конкретних практичних рекомендацій для покращення захисту інформаційних систем від кібератак. Значущість цього дослідження полягає у забезпеченні більш надійного та безпечного цифрового

простору, що є критично важливим для стабільного розвитку суспільства та економіки.

1. АНАЛІЗ ВПЛИВУ ТА ЗАХОДІВ ПРОТИДІЇ КІБЕРАТАКАМ У 21 СТОЛІТТІ

1.1. Сучасний стан та історія кібератак у 21 столітті

Кібератаки є однією з найбільших загроз для сучасного суспільства. У цьому підрозділі ми розглянемо розвиток кібератак з початку 21 століття, їх вплив на різні сфери життя, а також найвідоміші випадки.

1.1.1. Сучасний стан кібератак

Кібератаки стали щоденною реальністю для урядів, бізнесу та індивідуальних користувачів. Основні типи кібератак включають:

- **DDoS-атаки**: Перевантаження серверів великою кількістю запитів, що призводить до їхньої недоступності.
- **Фішинг**: Викрадення особистих даних через підробні веб-сайти.
- **Малваре**: Поширення шкідливого програмного забезпечення.
- **Ransomware**: Шифрування даних з метою вимагання викупу.

Історія кібератак показує, як вони стали більш поширеними та витонченими, що призвело до серйозних наслідків для держав, компаній та окремих користувачів. Наприклад, атака на Естонію у 2007 році паралізувала державні та фінансові установи, тоді як WannaCry у 2017 році завдала збитків на мільярди доларів у понад 150 країнах.

1.1.2. Історія кібератак

З початку 21 століття кібератаки стали більш поширеними і витонченими, що призвело до серйозних наслідків для держав, компаній та окремих

користувачів. Нижче наведені деякі з найбільш відомих та значущих кібератак, які відбулися за цей період (рис 1.1).

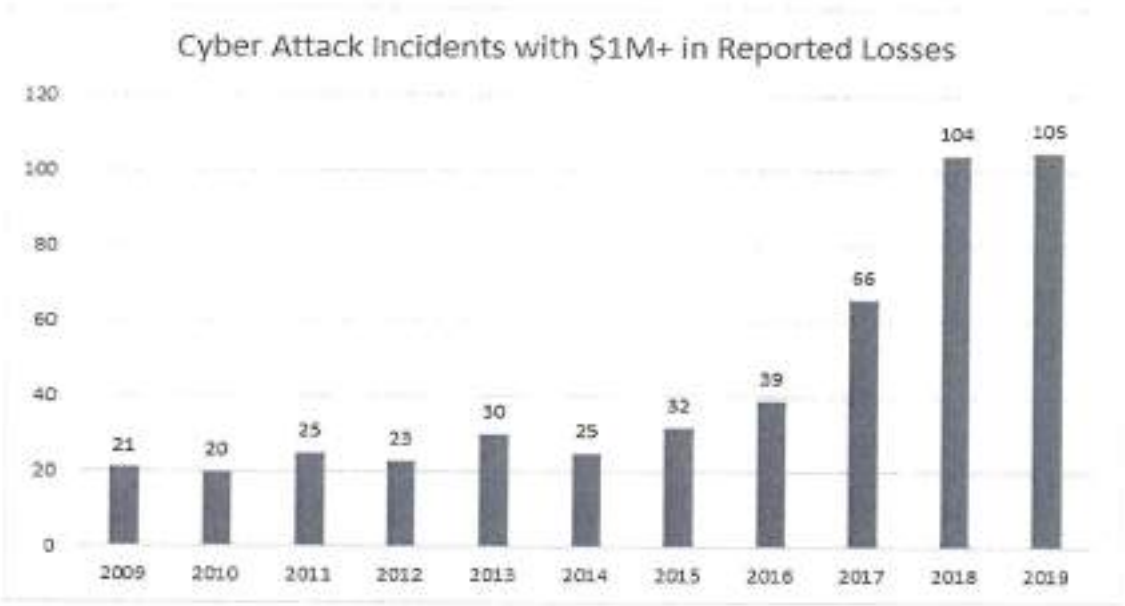

Рисунок 1.1 - Графік кількості кібератак за роками

З початку 21 століття відбулися численні масштабні кібератаки, серед яких:

- **Атака на Естонію (2007)**: Паралізувала державні та фінансові установи.
- **WannaCry (2017)**: Завдала збитків на мільярди доларів у понад 150 країнах.
- **NotPetya (2017)**: Викликала багатомільярдні збитки глобальним корпораціям.

1.1.3. Атака на Естонію (2007)

У 2007 році Естонія стала першою країною, що зазнала широкомасштабної кібератаки, яка паралізувала державні та фінансові установи. Атака розпочалася у квітні і тривала кілька тижнів, завдаючи значних збитків.

- **Причина**: Атака була викликана суперечкою між Естонією та Росією через перенесення радянського воєнного пам'ятника з центру Таллінна.
- **Характер атаки**: Основним видом атак були DDoS (Distributed Denial of Service), які перевантажували веб-сайти урядових установ, банків та медіа.
- **Наслідки**: Урядові веб-сайти, онлайн-банкінг та медіа стали недоступними. Атака змусила уряд переосмислити стратегії кібербезпеки та інвестувати в їх покращення.
- **Висновок**: Атака на Естонію стала важливим сигналом для інших країн щодо необхідності зміцнення кібербезпеки та розробки національних стратегій захисту від кібератак.

1.1.4. WannaCry (2017)

WannaCry, також відомий як WannaCrypt, став одним із найбільших інцидентів з використанням програм-вимагачів (ransomware) у 21 столітті(рис 1.1.2).

- **Причина**: Вірус WannaCry використовував експлойт EternalBlue, розроблений Агентством національної безпеки США (NSA), який було викрадено та опубліковано групою хакерів Shadow Brokers.
- **Характер атаки**: WannaCry поширювався через мережі, шифруючи файли на комп'ютерах і вимагаючи викуп у біткоїнах за їх розшифровку. Вірус вразив понад 200,000 комп'ютерів у більш ніж 150 країнах.
- **Наслідки**: Серед постраждалих були лікарні (National Health Service у Великій Британії), транспортні компанії, банки та інші великі організації. Загальні збитки оцінюються в мільярди доларів, а багато критично важливих сервісів були тимчасово недоступні.

- **Висновок**: WannaCry підкреслив важливість своєчасного оновлення програмного забезпечення та застосування заходів безпеки для захисту від шкідливого ПЗ.

Рисунок 1.2 - Вікно вірусу WannaCry

1.1.5. NotPetya (2017)

Атака NotPetya, яка відбулася у тому ж році, що і WannaCry, стала ще одним значним інцидентом з використанням програм-вимагачів, але з іншими цілями та наслідками(рис.1.1.1).

- **Причина**: NotPetya був створений як шкідливе програмне забезпечення для деструкції даних, маскуючись під програму-вимагач. Він використовував ті ж уразливості, що і WannaCry.
- **Характер атаки**: NotPetya поширювався через оновлення програмного забезпечення бухгалтерського обліку в Україні (M.E.Doc). Вірус

шифрував файли на комп'ютерах, але механізм розшифровки не існував, що робило відновлення даних неможливим.

- **Наслідки**: Атака почалася в Україні, але швидко поширилася на глобальні корпорації, такі як Maersk, Merck та FedEx. Загальні збитки оцінюються у мільярди доларів. Багато компаній зазнали значних перебоїв у роботі через втрату даних.
- **Висновок**: NotPetya показала, що кіберзагрози можуть бути використані як інструмент кібервійни, спрямований на дестабілізацію критичної інфраструктури країн та компаній.

Рисунок 1.3 - Вікно вірусу NotPetya

1.1.6 Інші значущі кібератаки

Окрім зазначених вище атак, варто згадати інші значущі інциденти:

- **Stuxnet (2010)**: Перший відомий комп'ютерний вірус, спрямований на знищення фізичних об'єктів, а саме іранських ядерних центрифуг.
- **Sony Pictures Hack (2014)**: Атака на Sony Pictures Entertainment, яка призвела до витоку конфіденційної інформації та фінансових втрат.
- **SolarWinds (2020)**: Складна атака на мережеве програмне забезпечення, що вплинула на численні урядові агенції та приватні компанії в США.

1.1.7. Stuxnet (2010)

Stuxnet вважається першим відомим комп'ютерним вірусом, створеним для знищення фізичних об'єктів. Цей вірус був спрямований на руйнування іранських ядерних центрифуг і викликав значний резонанс у сфері кібербезпеки(рис.1.1.3).

- **Причина**: Stuxnet був розроблений для того, щоб сповільнити або зупинити розвиток іранської ядерної програми. Вірус був розроблений спільними зусиллями США та Ізраїлю.
- **Характер атаки**: Stuxnet був надзвичайно складним шкідливим програмним забезпеченням, яке інфікувало комп'ютерні системи, що керували промисловим обладнанням (PLC) у ядерних об'єктах. Вірус був розроблений таким чином, щоб непомітно змінювати параметри роботи центрифуг, викликаючи їх пошкодження.
- **Наслідки**: Атака Stuxnet зруйнувала значну кількість центрифуг, що сповільнило іранську ядерну програму на кілька років. Крім того, Stuxnet став прецедентом для створення інших кіберзброї та підкреслив необхідність захисту промислових систем.
- **Висновок**: Stuxnet показав, що кібератаки можуть мати реальні фізичні наслідки і бути використані як інструмент міжнародних конфліктів.

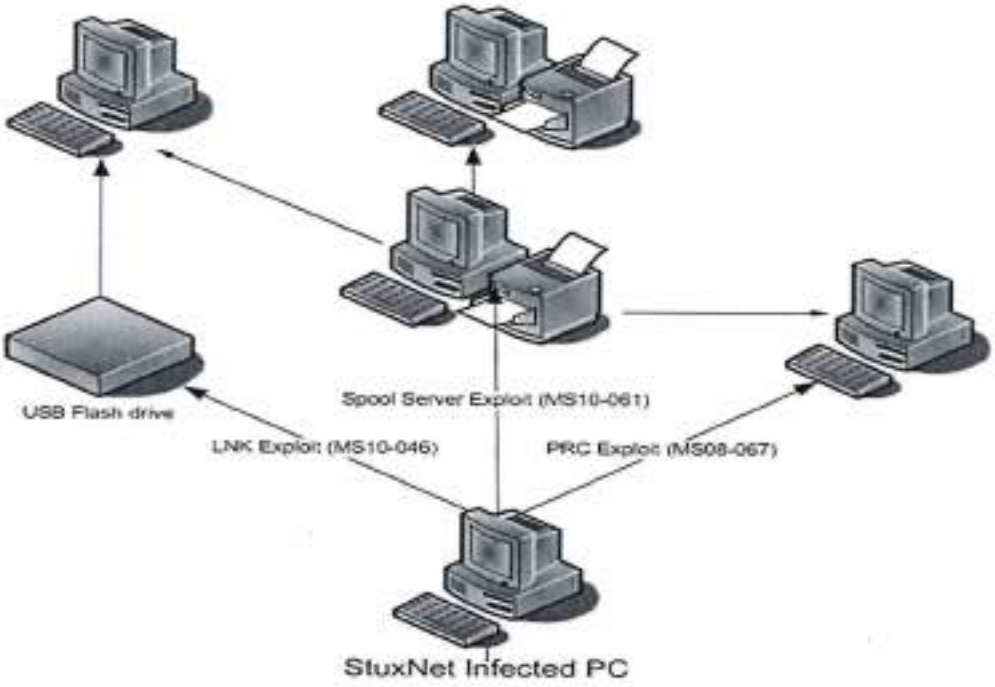

Рисунок 1.4 - Схема роботи вірусу Stuxnet

1.1.8. Sony Pictures Hack (2014)

Атака на Sony Pictures Entertainment у 2014 році стала однією з найбільш резонансних кібератак, що призвела до витоку конфіденційної інформації та значних фінансових втрат для компанії.

- **Причина**: Атака була здійснена групою хакерів, яка назвала себе "Guardians of Peace" (GOF). Вважається, що атака була відповіддю на вихід фільму "Інтерв'ю", який сатирично зображував лідера Північної Кореї Кім Чен Ина.
- **Характер атаки**: Хакери отримали доступ до внутрішніх мереж Sony Pictures, викрали конфіденційні дані, включаючи особисту інформацію співробітників, неопубліковані фільми, сценарії, електронні листи та фінансові документи. Вони також знищили значну кількість даних на серверах компанії.

- **Наслідки**: Витік конфіденційної інформації завдав значного удару по репутації Sony Pictures, викликав фінансові втрати та призвів до судових позовів. Крім того, атака підкреслила важливість кібербезпеки для захисту корпоративних даних.
- **Висновок**: Атака на Sony Pictures показала, що кіберзлочинці можуть використовувати конфіденційні дані для шантажу та завдання шкоди компаніям, а також підкреслила необхідність захисту від внутрішніх та зовнішніх загроз.

1.1.9 SolarWinds (2020)

Атака на SolarWinds у 2020 році стала однією з найскладніших та наймасштабніших кібератак, що вплинула на численні урядові агенції та приватні компанії в США.

- **Причина**: Атака була спрямована на ланцюг поставок програмного забезпечення SolarWinds, яке використовували тисячі організацій по всьому світу. Вважається, що атака була здійснена хакерською групою, яка підтримується російським урядом.
- **Характер атаки**: Хакери змогли проникнути в систему оновлень програмного забезпечення SolarWinds і вставити шкідливий код у легальні оновлення. Коли ці оновлення були встановлені клієнтами SolarWinds, хакери отримали доступ до їхніх систем.
- **Наслідки**: Атака вплинула на численні урядові агенції США, включаючи Міністерство фінансів, Міністерство торгівлі та інші, а також на приватні компанії. Це призвело до витоку конфіденційної інформації та значних фінансових втрат.
- **Висновок**: Атака на SolarWinds підкреслила вразливість ланцюгів поставок програмного забезпечення і необхідність посилення заходів безпеки для запобігання подібним інцидентам у майбутньому.

Таблиця 1.1.

Основні типи кібератак та їх характеристика

Тип атаки	Характеристика	Приклад
DDoS	Перевантаження серверів запитами	Атака на Dyn у 2016 році
Фішинг	Викрадення даних через підроблені сайти	Атака на Gmail у 2017 році
Малваре	Впровадження шкідливого ПЗ	Атака WannaCry у 2017 році
Ransomware	Шифрування даних з вимогою викупу	Атака NotPetya у 2017 році

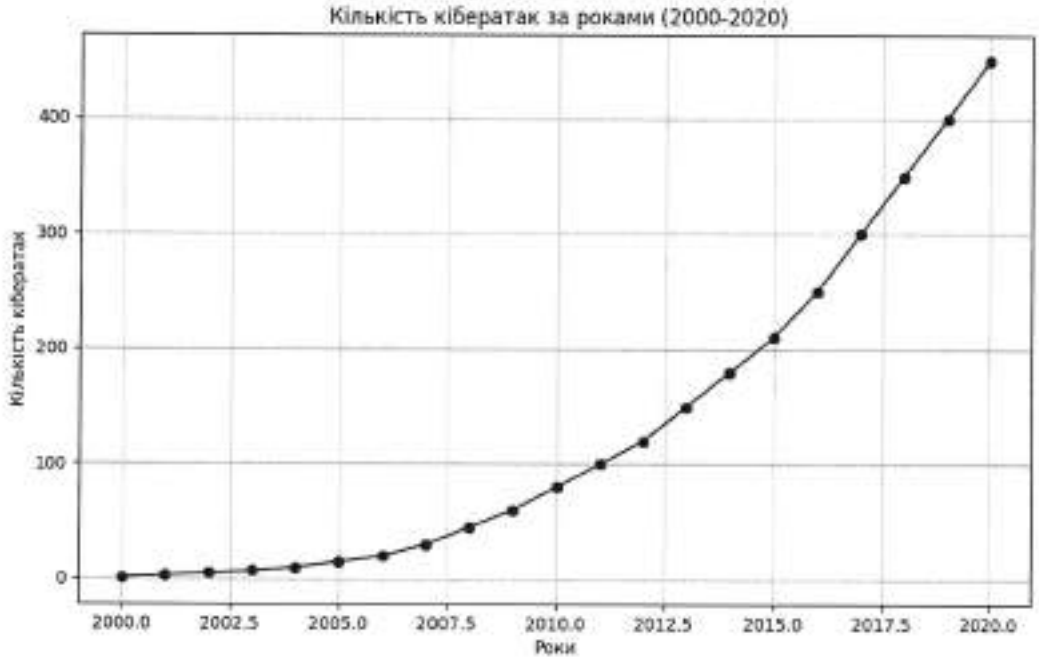

Рисунок 1.5 - Діаграма кількості кібератак за роками (2000-2020)

1.2 Аналіз існуючих методів кібербезпеки

У сучасному світі, де кібератаки стають усе більш частими та витонченими, розробка ефективних методів кібербезпеки є критично важливою для захисту інформаційних систем. У цьому підрозділі розглядаються найефективніші технічні, адміністративні та фізичні заходи захисту, що дозволяють забезпечити всебічний захист від кіберзагроз.

Технічні методи кібербезпеки включають використання різноманітного програмного та апаратного забезпечення для захисту інформаційних систем від загроз. Основними компонентами технічного захисту є:

Антивірусне програмне забезпечення: Основним завданням антивірусного ПЗ є виявлення та нейтралізація шкідливих програм. Сучасні антивіруси використовують методи машинного навчання та поведінкового аналізу для ефективнішого виявлення нових загроз. Наприклад, антивірусні програми такі як Kaspersky, Norton та McAfee активно використовують ці методи для забезпечення безпеки користувачів. Антивірусне ПЗ постійно оновлюється для виявлення нових вірусів та шкідливих програм, що з'являються щоденно(Рис.1.2).

Фаєрволи: Фаєрволи контролюють і фільтрують вхідний і вихідний мережевий трафік, запобігаючи несанкціонованому доступу до системи. Вони можуть бути як апаратними, так і програмними. Основна функція фаєрволів полягає в блокуванні підозрілих запитів та захисті мережі від зовнішніх загроз. Фаєрволи дозволяють визначити правила для вхідного і вихідного трафіку, що допомагає захистити внутрішню мережу від шкідливих атак ззовні(додаток D., рис.1.2.1).

Системи виявлення вторгнень (IDS): IDS аналізують мережевий трафік у реальному часі, виявляючи підозрілу активність та запобігаючи потенційним атакам. Вони можуть бути інтегровані з фаєрволами для підвищення рівня захисту. Прикладом є системи Snort та Suricata, які використовуються для моніторингу мережевого трафіку та виявлення аномалій. IDS можуть виявляти підозрілі дії на основі сигнатур відомих загроз або аналізу аномальної поведінки (додаток D, рис.1.2.2).

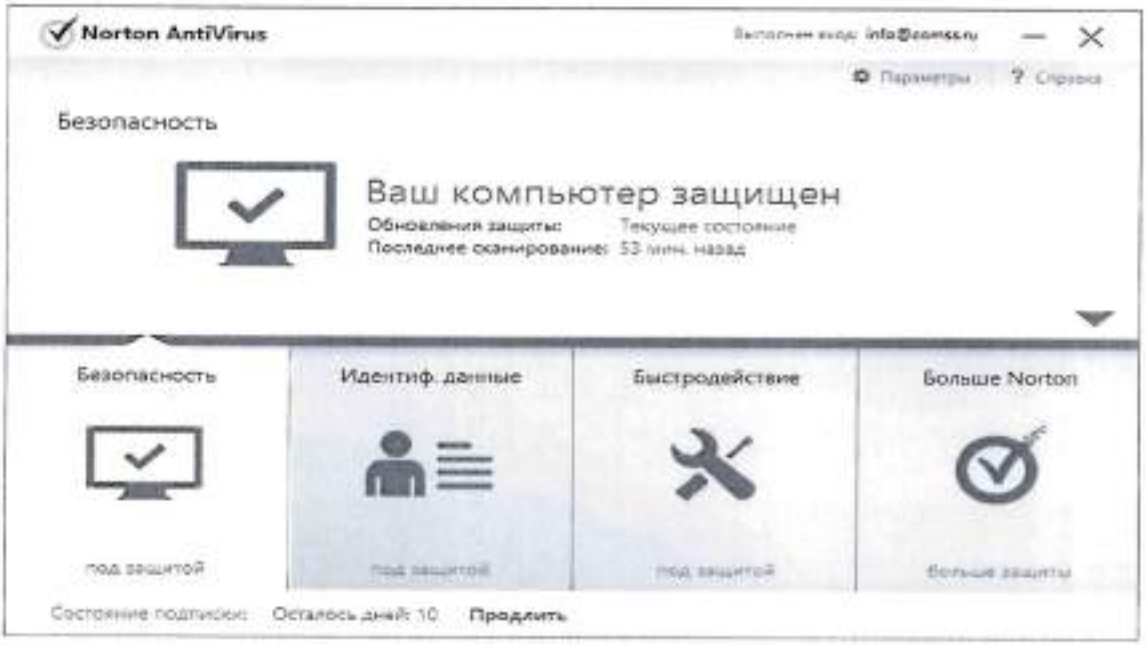

Рисунок 1.6. - Скріншот антивірусного ПО Norton

Адміністративні заходи кібербезпеки включають розробку політик, процедур та навчання персоналу для забезпечення захисту інформаційних систем. Ці заходи допомагають створити організаційні рамки для безпеки даних та зниження ризиків.

Політики безпеки встановлюють правила і процедури для захисту інформаційних систем. Вони визначають, хто має доступ до даних, які заходи необхідно вживати для захисту інформації, та які дії слід виконувати у разі виникнення інциденту. Наприклад, політика мінімальних привілеїв обмежує

доступ користувачів до лише тих ресурсів, які необхідні для виконання їхніх обов'язків. Це допомагає знизити ризик несанкціонованого доступу до критичних даних.

Підвищення обізнаності співробітників щодо загроз кібербезпеки та навчання їх правильним методам захисту є ключовим аспектом захисту інформаційних систем. Проведення регулярних тренінгів та навчальних сесій дозволяє співробітникам краще розуміти ризики та реагувати на потенційні загрози. Наприклад, навчання з фішинг-атак допомагає співробітникам розпізнавати підозрілі електронні листи та уникати їх. Це знижує ризик успішних фішинг-атак, які часто є першою стадією більш складних кібератак.

Фізичні заходи захисту включають обмеження фізичного доступу до комп'ютерних систем та серверних приміщень. Вони спрямовані на запобігання несанкціонованому доступу до апаратного забезпечення, яке може бути використане для компрометації системи.

Обмеження фізичного доступу до комп'ютерних систем та серверних приміщень є важливим заходом захисту. Використання біометричних систем, карт доступу та кодових замків дозволяє забезпечити, що лише авторизовані користувачі можуть отримати доступ до критичних систем. Це допомагає запобігти несанкціонованому доступу до важливих даних та систем, які можуть бути використані для кібератак.

Системи відеоспостереження використовуються для моніторингу та запобігання несанкціонованому доступу до критичних об'єктів. Вони дозволяють виявляти підозрілу активність та реагувати на потенційні загрози в реальному часі. Відеоспостереження також допомагає документувати інциденти, що може бути корисним для розслідувань та навчання персоналу.

Ефективний захист від кібератак можливий лише за умови комплексного підходу, який поєднує технічні, адміністративні та фізичні заходи. Використання антивірусного програмного забезпечення, фаєрволів та IDS, а також розробка політик безпеки та навчання персоналу дозволяють значно підвищити рівень захисту інформаційних систем. Кожен з цих компонентів відіграє важливу роль у забезпеченні кібербезпеки та зниженні ризиків успішних кібератак.

Таблиця 1.2.

Порівняльна характеристика методів кібербезпеки

Метод	Переваги	Недоліки
Антивірусне ПЗ	Виявлення та нейтралізація шкідливого ПЗ	Потреба в регулярних оновленнях баз даних
Фаєрволи	Контроль трафіку, запобігання доступу	Можливість обходу за допомогою складних атак
IDS	Виявлення підозрілої активності	Високий рівень хибних спрацювань

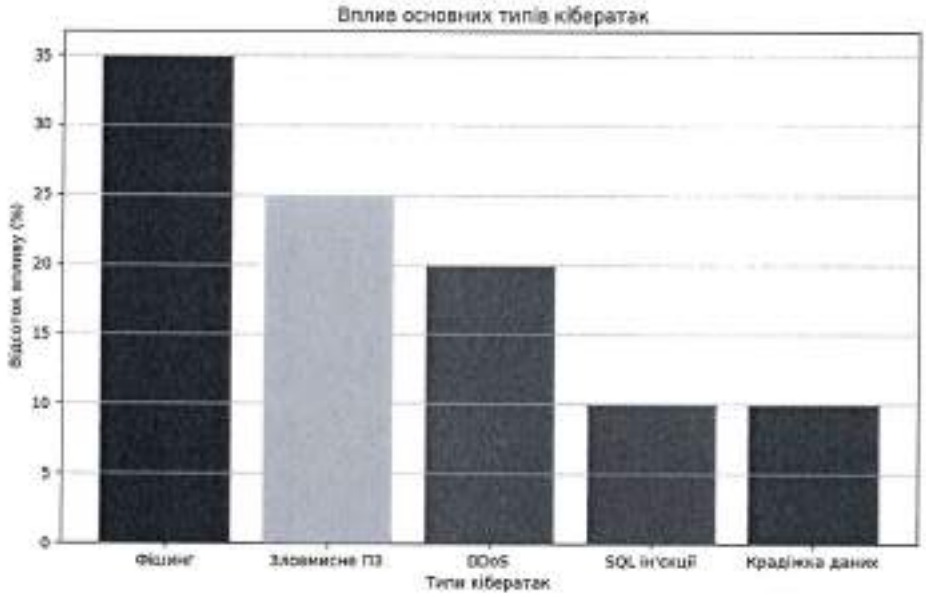

Рисунок 1.7 - Вплив основних типів кібератак

1.3. Порівняльний аналіз найбільших кібератак і їх наслідків

Порівняльний аналіз найбільших кібератак дозволяє виявити спільні риси та унікальні аспекти кожної з них. Це допомагає краще зрозуміти природу загроз та розробити ефективніші заходи захисту. У цьому підрозділі розглядаються деякі з найбільш значущих кібератак сучасності, їх основні характеристики та наслідки для економіки, безпеки та суспільства.

1.3.1. Stuxnet (2010)

Stuxnet був першим відомим вірусом, спрямованим на знищення фізичних об'єктів, а саме іранських ядерних центрифуг. Цей шкідливий програмний засіб поширювався через USB-накопичувачі та інфікував комп'ютери, які керували промисловим обладнанням. Вірус використовував уразливості в програмному забезпеченні для управління промисловими процесами (SCADA), що дозволило йому непомітно змінювати параметри роботи центрифуг, викликаючи їх пошкодження. Основна мета Stuxnet

полягала у сповільненні іранської ядерної програми шляхом непомітного пошкодження центрифуг.

Основна мета: Сповільнення іранської ядерної програми.

Характер атаки: Поширення через USB-накопичувачі, інфікування комп'ютерів, що керували промисловим обладнанням.

Наслідки: Значні витрати на відновлення іранських ядерних об'єктів, порушення промислових процесів.

1.3.2. WannaCry (2017)

WannaCry став однією з найбільших атак з використанням програм-вимагачів (ransomware). Цей вірус використовував вразливість в операційній системі Windows для поширення і шифрування файлів на комп'ютерах. Вірус швидко поширювався по мережах, блокуя доступ до файлів і вимагаючи викуп за їх розшифрування. Основна мета WannaCry полягала у вимаганні викупу за розшифровку даних, що завдало значних економічних втрат у глобальному масштабі.

Основна мета: Вимагання викупу за розшифрування даних.

Характер атаки: Використання вразливості в Windows, шифрування файлів на комп'ютерах.

Наслідки: Збитки на понад 4 мільярди доларів, порушення роботи численних організацій у більш ніж 150 країнах.

1.3.3. NotPetya (2017)

NotPetya спочатку був спрямований на українські компанії, але швидко поширився на глобальні корпорації. Вірус маскувався під програму-вимагач,

але насправді мав на меті знищення даних. NotPetya використовував вразливості в програмному забезпеченні для розповсюдження в корпоративних мережах, що призводило до шифрування даних та вимагання викупу. Основна мета NotPetya полягала у дестабілізації економічної ситуації в Україні.

Основна мета: Дестабілізація економічної ситуації в Україні.

Характер атаки: Маскування під програму-вимагач, знищення даних.

Наслідки: Багатомільярдні втрати, порушення роботи критично важливих інфраструктур.

Кожна з розглянутих атак мала значні економічні наслідки. WannaCry завдала збитків на понад 4 мільярди доларів, зупинивши роботу багатьох організацій по всьому світу. NotPetya спричинила багатомільярдні втрати, вплинувши на глобальні корпорації та порушивши їхні операційні процеси. Stuxnet призвів до значних витрат на відновлення іранських ядерних об'єктів та порушення промислових процесів.

Stuxnet продемонстрував можливість використання кібератак як інструменту міжнародних конфліктів, оскільки його метою було сповільнення розвитку ядерної програми Ірану. NotPetya паралізувала роботу критично важливих інфраструктур в Україні, що вплинуло на національну безпеку країни.

Постійні загрози кібератак створюють атмосферу страху і недовіри серед населення та бізнесу. Люди починають сумніватися в безпеці використання цифрових технологій, що може призвести до зниження рівня впровадження нових технологій і уповільнення розвитку цифрової економіки. Занепокоєння щодо безпеки даних та можливості кібератак може також вплинути на довіру до цифрових послуг та продуктів.

Порівняльний аналіз найбільших кібератак дозволяє виявити спільні риси та унікальні аспекти кожної з них, що допомагає краще зрозуміти природу загроз та розробити ефективніші заходи захисту. Розгляд Stuxnet, WannaCry та NotPetya дозволяє виявити такі спільні риси, як використання вразливостей у програмному забезпеченні та вплив на критично важливі інфраструктури. Водночас кожна з атак має унікальні аспекти, які відрізняють їх одна від одної.

Stuxnet: Фокус на промислових системах та фізичних об'єктах.

WannaCry: Використання програми-вимагача для отримання викупу.

NotPetya: Маскування під програму-вимагач з метою знищення даних.

Кожна з цих атак підкреслює необхідність всебічного підходу до кібербезпеки, включаючи технічні, адміністративні та фізичні заходи захисту. Тільки комплексний підхід може забезпечити надійний захист інформаційних систем від сучасних кіберзагроз.

1.3.5. Порівняння основних аспектів кібератак

Таблиця 1.3.

Порівняння основних аспектів кібератак

Атака	Основна мета	Характер атаки	Наслідки
Stuxnet	Руйнування фізичних об'єктів	Вірус, спрямований на промислове обладнання	Сповільнення ядерної програми Ірану
WannaCry	Вимагання викупу	Програма-вимагач	Економічні втрати, параліч систем
NotPetya	Знищення даних	Програма-вимагач (маскування)	Економічні втрати, дестабілізація

Кібератаки мають серйозні наслідки для економіки, безпеки та суспільства. Аналіз та порівняння цих атак дозволяє краще зрозуміти їх природу та розробити ефективніші заходи захисту. Це підкреслює необхідність постійного вдосконалення кібербезпеки та готовності до нових викликів.

Таблиця 1.4.

Економічні збитки від значних кібератак

Рік	Атака	Збитки (млрд. доларів)	Опис
2017	WannaCry	4	Масштабна атака з використанням програми-вимагача
2017	NotPetya	10	Атака спрямована на українські компанії, але швидко поширилася по всьому світу
2020	SolarWinds	90	Складна атака на мережеве програмне забезпечення, що вплинула на численні урядові агенції

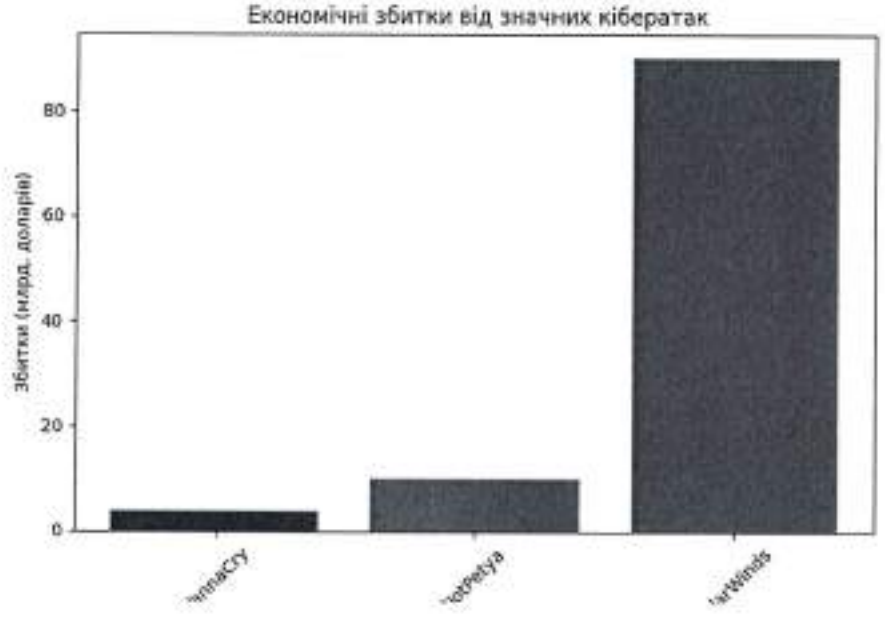

Рисунок 1.8 - Економічні збитки від значних кібератак

1.4. Ботнет мережі

Ботнети є однією з найсерйозніших загроз у сфері кібербезпеки. Ботнет — це мережа зламаних комп'ютерів, яка контролюється зловмисником, відомим як ботмастер. Ці комп'ютери, також названі ботами або зомбі, використовуються для виконання різних шкідливих дій, таких як розповсюдження спаму, крадіжка даних, здійснення DDoS-атак та інші шкідливі дії. Ботнет складається з трьох основних компонентів: боти, ботмастер та командно-контрольний сервер (C&C).

Перший компонент — боти, це заражені комп'ютери, які виконують команди ботмастера. Другий компонент — ботмастер, контролює ботнет та віддає команди ботам. Третій компонент — командно-контрольний сервер (C&C), через який ботмастер спілкується з ботами. Боти зазвичай заражаються через шкідливе програмне забезпечення, яке розповсюджується через фішингові електронні листи, заражені веб-сайти або через вразливості в програмному забезпеченні. Після зараження комп'ютер стає частиною ботнету і починає виконувати команди ботмастера.

Ботнети можуть використовуватися для різних шкідливих цілей. Наприклад, для здійснення DDoS-атак, які паралізують веб-сайти або мережеві сервіси шляхом відправки величезної кількості запитів. Іншим прикладом є розповсюдження спаму, де ботнети відправляють велику кількість небажаних електронних листів. Ботнети також можуть використовуватися для крадіжки даних, збирання конфіденційної інформації, такої як логіни та паролі. Ще одним прикладом використання ботнетів є майнінг криптовалют, де зловмисники використовують обчислювальні потужності заражених комп'ютерів для видобування криптовалют.

1.4.1. Приклади відомих ботнетів

Одним з найбільш відомих ботнетів є Mirai. Цей ботнет використовував вразливості IoT-пристроїв для створення великої мережі зомбі-комп'ютерів, які здійснювали масштабні DDoS-атаки. Інший відомий ботнет — Zeus, який використовувався для крадіжки банківських даних шляхом зараження комп'ютерів шкідливим програмним забезпеченням.

1.4.2. Заходи протидії ботнетам

Для захисту від ботнетів використовуються різні методи. Одним з таких методів є використання антивірусного програмного забезпечення, яке виявляє та видаляє шкідливе ПЗ. Фаєрволи та IDS/IPS системи також допомагають виявляти та блокувати підозрілу активність у мережі. Навчання користувачів є важливим аспектом протидії ботнетам, оскільки підвищення обізнаності щодо фішингових атак та безпечного використання інтернету може значно знизити ризик зараження. Крім того, регулярне оновлення програмного забезпечення допомагає закривати відомі вразливості, що можуть бути використані зловмисниками для зараження комп'ютерів.

Ці заходи дозволяють значно знизити ризик використання ботнетів та захистити інформаційні системи від шкідливих дій.

1.5. Постановка завдання на дослідження впливу кібератак та заходів кібербезпеки

Постановка завдання є критично важливим етапом наукового дослідження, оскільки визначає основні напрями роботи, методи дослідження та очікувані результати. У даному розділі розглядаються мета, завдання, методи дослідження, а також основні етапи виконання роботи.

Метою даної дипломної роботи є аналіз впливу кібератак у 21 столітті та розробка рекомендацій щодо впровадження ефективних заходів кібербезпеки. Це включає вивчення історії кібератак, оцінку їх впливу на різні аспекти суспільного життя, а також аналіз сучасних методів захисту. Дослідження має на меті визначити, як кібератаки впливають на економіку, національну безпеку, приватність та психологічний стан суспільства, а також виявити ефективні стратегії та технології для запобігання таким атакам.

Для досягнення поставленої мети були визначені наступні завдання. Перш за все, необхідно провести огляд і класифікацію основних видів кібератак та їх наслідків. Це включає вивчення різних типів кібератак, таких як DDoS, фішинг, малваре та ransomware, а також аналіз їх впливу на економіку, національну безпеку, приватність та психологічний стан суспільства. Важливо зрозуміти, як кожен з видів атак впливає на різні сфери життя та які наслідки вони можуть мати.

Наступним завданням є вивчення економічних, соціальних та політичних аспектів впливу кібератак. Це включає оцінку економічних збитків, спричинених кібератаками, зокрема на прикладах найбільших інцидентів, а також дослідження соціальних наслідків, таких як втручання в особисте життя громадян та вплив на довіру до цифрових технологій. Аналіз політичних аспектів включає використання кібератак як інструменту кібервійни та їх вплив на міжнародні відносини.

Далі необхідно проаналізувати сучасні методи захисту від кібератак та оцінити їх ефективність. Це завдання включає дослідження технічних, адміністративних та фізичних заходів захисту, а також оцінку ефективності існуючих методів захисту та визначення їхніх переваг та недоліків. Такий аналіз дозволить визначити, які методи є найбільш ефективними та як їх можна вдосконалити.

На основі отриманих даних розробляються рекомендації щодо вдосконалення системи кібербезпеки на різних рівнях. Це включає розробку стратегій для підвищення рівня обізнаності населення щодо кібербезпеки, впровадження сучасних технологій та інструментів для захисту інформаційних систем, а також розробку політик безпеки та рекомендацій щодо автоматизації процесів кібербезпеки. Важливо забезпечити комплексний підхід до захисту, який поєднує технічні, адміністративні та освітні заходи.

Для виконання даного дослідження використовуються різноманітні методи, що дозволяють комплексно підходити до вирішення поставлених завдань. Основними методами дослідження є аналіз літературних джерел, статистичний аналіз, моделювання та симуляція, а також експертні оцінки.

Аналіз літературних джерел включає вивчення наукових статей, звітів, нормативних документів та інших публікацій, присвячених питанням кібербезпеки. Цей метод дозволяє отримати теоретичні знання та виявити прогалини в існуючих дослідженнях.

Статистичний аналіз передбачає збір і аналіз даних про кібератаки, їх частоту, характер і наслідки, що допомагає виявити тенденції та зробити висновки щодо масштабів проблеми.

Моделювання та симуляція включають створення моделей кібератак і систем захисту для оцінки їх ефективності в різних сценаріях, що дозволяє прогнозувати можливі наслідки атак та ефективність заходів захисту. Експертні оцінки передбачають залучення фахівців у галузі кібербезпеки для отримання експертних висновків і рекомендацій, що дозволяє врахувати думки професіоналів та підвищити наукову цінність дослідження.

У цьому контексті варто розглянути нещодавній інцидент з компанією Київстар, яка стала жертвою масованої DDoS-атаки у 2023 році. Атака,

організована за допомогою ботнету, мала на меті перевантажити сервери компанії великою кількістю запитів, що призвело до перебоїв у роботі мобільної мережі та інтернет-сервісів.

Це викликало значні незручності для клієнтів, які не могли отримати доступ до послуг зв'язку. Компанія Київстар залучила провідних фахівців для аналізу та усунення наслідків атаки, а також підвищення рівня захисту своїх систем. Було впроваджено системи моніторингу трафіку, збільшено пропускну здатність серверів, використано технології балансування навантаження та проведено навчання персоналу.

Цей інцидент підкреслив важливість готовності до кіберзагроз та необхідність постійного вдосконалення систем кібербезпеки. (рис.1.9).

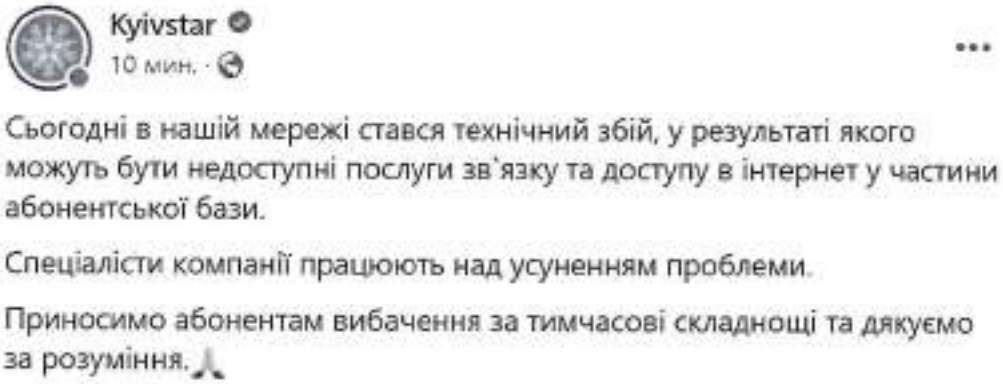

Рисунок 1.9. Повідомлення від «Київстар» в соціальній мережі «Facebook»

2. ПРОЕКТНІ І ТЕХНІЧНІ РІШЕННЯ. ВИДИ ЗАБЕЗПЕЧЕННЯ

2.1. Інформаційне забезпечення

Інформаційне забезпечення є ключовим компонентом системи кібербезпеки, оскільки дозволяє ефективно збирати, обробляти та аналізувати дані для виявлення та запобігання кіберзагрозам. У сучасному світі, де обсяг інформації постійно зростає, важливо забезпечити надійний та ефективний процес управління даними. Це включає кілька основних етапів: збір, зберігання, обробка, аналіз та передача даних.

Збір даних полягає у виявленні та акумуляції всіх необхідних для кібербезпеки відомостей з різних джерел, таких як системні журнали, мережеві трафіки, бази даних, пристрої та користувацькі дії. Для цього використовуються спеціалізовані програмні засоби, що дозволяють автоматизувати процес збору даних та мінімізувати людський фактор. Важливість цього етапу важко переоцінити, оскільки своєчасне та повне збирання інформації є основою для подальшого аналізу та реагування на загрози.

Зберігання даних передбачає використання надійних і безпечних сховищ для збереження великої кількості інформації. Це можуть бути хмарні сервіси, локальні сервери або гібридні системи, які забезпечують доступ до даних у будь-який момент часу та з будь-якої точки світу. Вибір відповідного рішення залежить від специфіки організації та її потреб у забезпеченні безпеки даних. Надійне зберігання даних гарантує, що інформація буде доступна та захищена від несанкціонованого доступу та втрат.

Обробка та аналіз даних є критично важливими для виявлення потенційних загроз та аномалій у системі. Для цього застосовуються методи

статистичного аналізу, машинного навчання, поведінкового аналізу та інші аналітичні інструменти. Вони дозволяють виявляти підозрілу активність, визначати тренди та передбачати можливі атаки. Ці методи забезпечують проактивний підхід до кібербезпеки, що дозволяє своєчасно реагувати на загрози та запобігати їх розвитку.

Передача даних має на меті забезпечення безпечного обміну інформацією між різними компонентами системи та користувачами. Для цього використовуються захищені протоколи передачі даних, шифрування та інші методи, що забезпечують конфіденційність та цілісність даних під час їх транспортування. Надійні методи передачі даних гарантують, що інформація не буде перехоплена або змінена під час її переміщення між різними частинами системи.

Таким чином, інформаційне забезпечення є невід'ємною складовою системи кібербезпеки, що дозволяє ефективно управляти даними та забезпечувати захист інформаційних ресурсів. У цьому розділі розглядаються основні аспекти інформаційного забезпечення, включаючи визначення інформаційних потоків та побудову діаграм прецедентів, дій та послідовностей, що допомагають візуалізувати та оптимізувати процеси управління інформацією. Це дозволяє не лише виявляти та реагувати на поточні загрози, але й прогнозувати та запобігати майбутнім атакам, забезпечуючи таким чином надійний захист інформаційних систем.

2.1.1. Визначення інформаційних потоків та їх аналіз

Інформаційні потоки — це шляхи, якими дані переміщуються всередині організації або між організацією та зовнішнім середовищем. Аналіз інформаційних потоків дозволяє виявити, як дані передаються, зберігаються та обробляються, а також які потенційні загрози можуть виникнути на різних етапах цього процесу.

Першим етапом визначення інформаційних потоків є ідентифікація джерел та приймачів даних. Джерела даних можуть включати сервери, бази даних, користувачів та зовнішні системи, тоді як приймачами даних можуть бути користувачі, аналітичні системи та звітні системи. Важливо точно визначити всі можливі точки входу та виходу даних, щоб забезпечити їх захист на кожному етапі. Це дозволяє зрозуміти, де дані можуть бути вразливими для несанкціонованого доступу або інших загроз.

Наступним кроком є опис потоків даних, який включає збір, передачу, зберігання та обробку даних. Збір даних полягає в описі методів та засобів збору даних, наприклад, з мережевих журналів, систем виявлення вторгнень (IDS) та антивірусних програм. Важливо визначити, які дані збираються, звідки вони надходять та як вони використовуються у подальшому аналізі.

Передача даних охоплює опис способів передачі даних, включаючи використання зашифрованих каналів зв'язку (VPN), мережевих протоколів (TCP/IP, HTTPS) для забезпечення безпеки під час транспортування інформації. Забезпечення захищеного каналу передачі є критичним для запобігання перехопленню даних під час їх руху між різними частинами системи.

Зберігання даних передбачає опис методів зберігання даних, таких як бази даних, хмарні сховища та файлові системи. Важливо розглянути методи шифрування даних на стадії зберігання, щоб запобігти несанкціонованому доступу до інформації у випадку фізичної або логічної компрометації сховища.

Обробка даних включає опис методів обробки даних, таких як аналіз, кореляція та звітування, що дозволяє виявляти підозрілу активність та визначати тренди. Методи обробки даних повинні бути адаптовані до

специфічних потреб організації та забезпечувати своєчасне виявлення та реагування на потенційні загрози.

Завдяки комплексному підходу до аналізу інформаційних потоків можна забезпечити високий рівень захисту даних на всіх етапах їхнього життєвого циклу, від збору до обробки та зберігання. Це дозволяє не лише підвищити безпеку інформаційних систем, але й оптимізувати їх роботу, забезпечуючи безперебійний та захищений доступ до критично важливих даних.

2.1.2. Побудова діаграм прецедентів, дій та послідовностей

Діаграми прецедентів є важливим інструментом у процесі аналізу інформаційних потоків, оскільки вони відображають взаємодію користувачів із системою та визначають основні сценарії використання. Основні елементи діаграм прецедентів включають акторів (користувачів або інші системи), прецеденти (дії або функції, які виконуються акторами) та відносини (зв'язки між акторами та прецедентами, що показують взаємодію). Наприклад, для системи електронної комерції актори можуть включати клієнта, адміністратора та систему управління складом, тоді як прецеденти можуть включати оформлення замовлення, перегляд історії замовлень, обробку замовлень та управління продуктами.

Діаграми дій описують конкретні дії, які виконуються в системі для досягнення певних цілей. Основні елементи діаграм дій включають дії (операції або кроки, які виконуються в процесі), потоки (взаємозв'язки між діями, що показують порядок їх виконання) та рішення (точки прийняття рішень, що визначають подальший хід дій). Для процесу оформлення замовлення в системі електронної комерції діаграма дій може включати вибір продуктів, оформлення замовлення, перевірку наявності продуктів на складі, обробку платежу, підтвердження замовлення та надсилання замовлення на склад для упаковки та відправки.

Діаграми послідовностей відображають порядок виконання дій та їхній взаємозв'язок у часі. Основні елементи діаграм послідовностей включають об'єкти (елементи системи, які беруть участь у процесі), повідомлення (інформацію, що передається між об'єктами) та часову шкалу (відображає послідовність подій у часі). Для процесу оформлення замовлення в системі електронної комерції діаграма послідовностей може включати надсилання запиту клієнтом, отримання запиту системою, перевірку наявності продуктів на складі, обробку платежу, підтвердження замовлення та передачу замовлення на склад для упаковки та відправки.

Побудова діаграм прецедентів, дій та послідовностей є важливим етапом у проектуванні інформаційних систем, оскільки дозволяє візуалізувати процеси, визначити ключові точки взаємодії та виявити можливі вразливості. Це дозволяє забезпечити ефективне інформаційне забезпечення та підвищити рівень кібербезпеки.

2.2. Математичне забезпечення

Математичне забезпечення відіграє важливу роль у системах кібербезпеки, оскільки дозволяє оцінювати ризики, прогнозувати наслідки кібератак та розробляти стратегії захисту. Використання математичних моделей та алгоритмів надає можливість здійснювати глибокий аналіз загроз, оцінювати їх вплив та приймати обґрунтовані рішення щодо захисту інформаційних систем. У цьому розділі розглядаються основні етапи розробки математичних алгоритмів та побудови математичних моделей для кібербезпеки.

Математичні моделі та алгоритми використовуються для ідентифікації та аналізу вразливостей у системах, а також для моделювання можливих сценаріїв кібератак. Це включає аналіз великих обсягів даних, отриманих від різних джерел, таких як мережеві журнали, дані про трафік, журнали доступу

та інші джерела. Завдяки математичним методам можна автоматично виявляти аномалії та підозрілу активність, що може свідчити про спроби несанкціонованого доступу або інші загрози.

Оцінка ризиків є одним з ключових аспектів математичного забезпечення в кібербезпеці. Це включає в себе оцінку ймовірності виникнення різних типів кібератак та їх можливого впливу на інформаційні системи. Використання статистичних методів та методів машинного навчання дозволяє розробляти прогностичні моделі, що допомагають передбачати ймовірність виникнення атак та їх наслідки. Це дозволяє організаціям заздалегідь готуватися до можливих загроз та впроваджувати превентивні заходи.

Прогнозування наслідків кібератак є ще одним важливим аспектом математичного забезпечення. Це дозволяє моделювати можливі сценарії розвитку подій у разі успішної атаки та оцінювати їх вплив на різні аспекти діяльності організації, включаючи фінансові втрати, порушення роботи систем, втрату даних та репутаційні ризики. Такі прогнози допомагають організаціям розробляти стратегії мінімізації наслідків атак та швидкого відновлення після інцидентів.

Розробка математичних алгоритмів для оцінки ризиків кібератак включає кілька основних етапів. Перший етап полягає у зборі та підготовці даних, які будуть використовуватися для аналізу. Це може включати збір даних про попередні атаки, журнали доступу, мережеві журнали та інші релевантні дані. Другий етап передбачає аналіз та обробку даних для виявлення патернів та аномалій, які можуть свідчити про потенційні загрози. Третій етап включає розробку математичних моделей та алгоритмів для оцінки ризиків та прогнозування наслідків атак. На завершальному етапі проводиться тестування та валідація розроблених моделей для забезпечення їх точності та надійності.

Одним з прикладів використання математичних моделей у кібербезпеці є моделювання ймовірності успішних атак на основі аналізу вразливостей системи. Це дозволяє визначити найбільш вразливі компоненти системи та розробити ефективні стратегії їх захисту. Інший приклад — використання алгоритмів машинного навчання для автоматичного виявлення аномалій у мережевому трафіку, що може свідчити про спроби проникнення в систему.

Таким чином, математичне забезпечення є невід'ємною частиною сучасних систем кібербезпеки. Використання математичних моделей та алгоритмів дозволяє ефективно оцінювати ризики, прогнозувати наслідки атак та розробляти стратегії захисту, що забезпечує високий рівень безпеки інформаційних систем. У цьому розділі детально розглядаються основні етапи розробки математичних алгоритмів та побудови математичних моделей, що є ключовими елементами ефективної кібербезпеки.

2.2.1. Розробка математичних алгоритмів для оцінки ризиків кібератак

Перший крок у розробці математичних алгоритмів для оцінки ризиків кібератак полягає у ідентифікації потенційних загроз. Це включає в себе визначення типів кібератак, які можуть бути спрямовані на інформаційну систему, та їх характеристик. Ідентифікація загроз дозволяє чітко окреслити потенційні небезпеки та спрямувати зусилля на їх запобігання та нейтралізацію.

Перш за все, необхідно визначити типи загроз, які можуть бути спрямовані на інформаційну систему. Це можуть бути:

- DDoS-атаки: Атаки на відмову в обслуговуванні, спрямовані на перевантаження системи великою кількістю запитів. Такі атаки можуть

призвести до тимчасової недоступності послуг або навіть до повного виходу з ладу системи.

- Фішинг: Атаки, що використовують підроблені веб-сайти або електронні листи для викрадення конфіденційної інформації, такої як паролі, номери кредитних карток або особисті дані.
- Малваре: Віруси, трояни та інші види шкідливого програмного забезпечення, що можуть викрасти або знищити дані, порушити роботу систем або надати зловмисникам несанкціонований доступ до ресурсів.
- Ransomware: Програми-вимагачі, що шифрують дані та вимагають викуп за їх розшифровку. Цей тип загрози може призвести до значних фінансових втрат та порушення діяльності організації.

Кожен тип загроз має свої характеристики, які необхідно враховувати при розробці математичних алгоритмів. До основних характеристик загроз належать:

- Ймовірність виникнення: Оцінка ймовірності, з якою загроза може реалізуватися. Це може включати аналіз статистичних даних про частоту попередніх атак та врахування поточних тенденцій у кіберзагрозах.

- Потенційний вплив: Оцінка впливу загрози на систему у разі її реалізації. Це може включати аналіз можливих економічних збитків, втрат даних та порушення роботи системи.

- Вразливості системи: Оцінка слабких місць у системі, які можуть бути використані для здійснення атаки. Це включає аналіз поточних конфігурацій системи, наявність вразливостей у програмному забезпеченні та оцінку рівня захищеності.

2.2.2. Аналіз ризиків

Наступний крок включає оцінку ризиків для кожної загрози. Це дозволяє пріоритезувати загрози та визначити найбільш критичні з них. Аналіз ризиків дозволяє сконцентрувати зусилля на найбільш небезпечних загрозах та розробити ефективні стратегії їх нейтралізації.

Оцінка ризиків включає:

- Оцінку ймовірності: Використання статистичних методів та історичних даних для оцінки ймовірності реалізації кожної загрози. Це може включати аналіз трендів у кібератаках та використання моделей прогнозування.
- Оцінку впливу: Визначення потенційних економічних, соціальних та політичних наслідків кожної загрози. Це може включати оцінку можливих збитків, втрат репутації та інших негативних наслідків.
- Ризиковий профіль: Створення профілю ризиків, що включає ймовірність та вплив кожної загрози. Це дозволяє візуалізувати ризики та визначити пріоритети для заходів захисту.

На основі аналізу ризиків розробляються математичні алгоритми для оцінки та управління ризиками. Це включає:

- Алгоритми оцінки ризиків: Алгоритми, що використовують статистичні моделі для оцінки ризиків на основі зібраних даних. Вони дозволяють автоматично обчислювати рівень ризику для різних загроз та приймати обґрунтовані рішення щодо заходів захисту.
- Алгоритми виявлення загроз: Алгоритми, що використовують методи машинного навчання для виявлення аномалій та потенційних загроз у

реальному часі. Вони можуть аналізувати великий обсяг даних та автоматично виявляти підозрілу активність.

- Алгоритми прийняття рішень: Алгоритми, що допомагають визначити найбільш ефективні заходи захисту на основі оцінки ризиків. Вони можуть включати рекомендації щодо впровадження технічних, адміністративних та фізичних заходів захисту.

Розглянемо приклад алгоритму для оцінки ризиків DDoS-атаки.

Першим етапом є збір даних, що включає збір історичних даних про попередні DDoS-атаки, включаючи частоту та інтенсивність атак. Наступним етапом є оцінка ймовірності, що передбачає використання статистичних методів для оцінки ймовірності майбутніх DDoS-атак на основі зібраних даних.

Після цього проводиться оцінка впливу, яка включає визначення потенційних економічних збитків та впливу на продуктивність системи у разі реалізації атаки. На основі оцінки ймовірності та впливу розраховується ризик як добуток ймовірності та впливу. Нарешті, розробляються рекомендації щодо захисту, що включають впровадження заходів захисту на основі оцінки ризику. Це може включати використання додаткових засобів захисту, таких як фаєрволи, системи виявлення вторгнень та інші методи.

Таким чином, розробка математичних алгоритмів для оцінки ризиків кібератак є критично важливим етапом у забезпеченні кібербезпеки. Використання математичних моделей та алгоритмів дозволяє ефективно оцінювати ризики, прогнозувати наслідки атак та розробляти стратегії захисту, що забезпечує високий рівень безпеки інформаційних систем.

2.2.3. Побудова математичної моделі для прогнозування наслідків кібератак

Побудова математичної моделі для прогнозування наслідків кібератак включає вибір основних змінних, що впливають на результати моделі. Ці змінні можуть включати тип атаки, вразливості системи, ймовірність успіху атаки та потенційний вплив. Визначення змінних є критичним етапом, оскільки від правильного вибору залежить точність та надійність прогнозу.

Однією з основних змінних є тип атаки. Типи атак можуть включати DDoS, фішинг, малваре та ransomware. Кожен тип атаки має свої специфічні характеристики та методи впливу на систему, що повинні бути враховані в моделі. Наприклад, DDoS-атаки спрямовані на перевантаження системи великою кількістю запитів, тоді як фішинг націлений на викрадення конфіденційної інформації шляхом обману користувачів.

Другою важливою змінною є вразливості системи. Це рівень захищеності інформаційних систем та наявність слабких місць, які можуть бути використані для здійснення атаки. Оцінка вразливостей системи дозволяє визначити, наскільки ймовірним є успішне здійснення атаки. Це включає аналіз конфігурацій системи, наявність оновлень безпеки та оцінку можливих шляхів проникнення.

Третя змінна — ймовірність успіху атаки, яка залежить від рівня захищеності системи та типу атаки. Визначення ймовірності успіху атаки дозволяє оцінити ризик, з яким система може зіткнутися. Це включає аналіз історичних даних про попередні атаки, статистичних моделей та використання методів машинного навчання для прогнозування.

Четверта змінна — потенційний вплив, що включає величину можливих збитків у разі успішної атаки. Оцінка впливу дозволяє визначити економічні

збитки, втрати продуктивності системи та інші негативні наслідки, які можуть виникнути в результаті атаки.

Побудова моделі

Наступний крок включає побудову математичної моделі, що дозволяє прогнозувати наслідки кібератак. Цей етап складається з декількох підетапів, включаючи вибір типу моделі, розробку моделі та її калібрування.

Перш за все, необхідно здійснити вибір моделі. Існує кілька типів моделей, які можуть бути використані, зокрема регресійні моделі, моделі машинного навчання та імітаційні моделі. Вибір моделі залежить від специфіки завдання та наявних даних. Регресійні моделі можуть бути використані для оцінки взаємозв'язків між змінними, тоді як моделі машинного навчання дозволяють виявляти складні патерни та взаємозв'язки.

Другий підетап — розробка моделі, що включає створення моделі з урахуванням визначених змінних та їх взаємозв'язків. Наприклад, імітаційні моделі можуть використовуватися для прогнозування результатів атак у різних сценаріях. Це дозволяє змоделювати різні умови та оцінити, як зміни в одній змінній можуть вплинути на результат.

Третій підетап — калібрування моделі, що включає налаштування моделі на основі історичних даних та реальних випадків кібератак. Це дозволяє підвищити точність моделі та забезпечити її надійність. Калібрування передбачає аналіз результатів моделі та їх порівняння з реальними даними для виявлення можливих відхилень та їх корекцію.

Аналіз результатів

Останній етап включає аналіз результатів, отриманих за допомогою моделі, та оцінку її точності та надійності. Це дозволяє визначити

ефективність моделі та її здатність прогнозувати наслідки кібератак у реальних умовах.

Перше, що необхідно зробити, це верифікація моделі. Це процес перевірки точності моделі на основі тестових даних. Верифікація дозволяє виявити можливі помилки в моделі та здійснити їх корекцію для підвищення точності прогнозів.

Другий крок — валідація моделі, що включає оцінку здатності моделі прогнозувати наслідки кібератак у реальних умовах. Валідація проводиться на основі незалежних даних, які не використовувалися під час розробки та калібрування моделі. Це дозволяє оцінити, наскільки добре модель справляється з прогнозуванням нових випадків.

Третій крок — аналіз сценаріїв, що включає використання моделі для аналізу різних сценаріїв кібератак та оцінки їх можливих наслідків. Це дозволяє визначити, які сценарії є найбільш небезпечними та які заходи можуть бути ефективними для їх нейтралізації.

2.2.4. Приклад математичної моделі для прогнозування наслідків DDoS-атаки

Розглянемо приклад моделі для прогнозування наслідків DDoS-атаки. Першим кроком є визначення змінних моделі, таких як тип атаки (DDoS), кількість вразливих точок у системі, ймовірність успіху атаки та потенційний вплив (економічні збитки та зниження продуктивності системи).

Наступний крок — побудова моделі. Для цього можна використовувати регресійну модель або модель машинного навчання. Регресійна модель може бути використана для оцінки взаємозв'язку між змінними, тоді як модель машинного навчання дозволяє виявляти складні патерни та взаємозв'язки.

Після побудови моделі необхідно провести калібрування на основі історичних даних про попередні DDoS-атаки. Це дозволяє налаштувати модель для підвищення її точності та надійності.

Останній крок включає аналіз результатів моделі, що дозволяє оцінити можливі економічні збитки та вплив на продуктивність системи у разі реалізації атаки. На основі результатів моделі можна розробити рекомендації щодо заходів захисту для мінімізації наслідків атак.

Таким чином, побудова математичної моделі для прогнозування наслідків кібератак є важливим етапом у забезпеченні кібербезпеки. Використання математичних моделей дозволяє ефективно оцінювати ризики, прогнозувати наслідки атак та розробляти стратегії захисту, що забезпечує високий рівень безпеки інформаційних систем.

2.3. Програмне забезпечення

Програмне забезпечення є важливим компонентом системи кібербезпеки, оскільки воно забезпечує автоматизацію процесів виявлення та запобігання кіберзагрозам, аналізу даних та управління ризиками. Розробка надійного програмного забезпечення для кібербезпеки включає створення алгоритмів виявлення загроз, тестування та валідацію розроблених рішень. У цьому розділі розглядаються основні етапи розробки та тестування програмного забезпечення для аналізу кіберзагроз.

Програмне забезпечення для кібербезпеки має забезпечити автоматичне виявлення загроз у реальному часі. Це досягається за допомогою розробки спеціалізованих алгоритмів, які аналізують мережевий трафік, журнали подій та інші дані, що надходять від різних джерел. Такі алгоритми повинні бути здатні виявляти підозрілу активність та реагувати на неї відповідним чином. Для цього використовуються різноманітні методи машинного навчання та

штучного інтелекту, що дозволяють створювати ефективні системи виявлення загроз.

Тестування програмного забезпечення є важливим етапом його розробки. Воно включає перевірку алгоритмів на наявність помилок, оцінку їх ефективності та надійності. Тестування може проводитися в лабораторних умовах або у реальних системах, де програмне забезпечення встановлюється для виявлення та запобігання реальним загрозам. Це дозволяє оцінити, наскільки ефективно програмне забезпечення справляється зі своїми завданнями та виявляти можливі вразливості.

Валідація програмного забезпечення включає оцінку його відповідності вимогам та стандартам кібербезпеки. Це передбачає перевірку того, наскільки програмне забезпечення відповідає встановленим критеріям безпеки та ефективності. Валідація також включає тестування програмного забезпечення у різних умовах, щоб переконатися в його здатності працювати у різних сценаріях та під різним навантаженням.

Розробка алгоритмів виявлення загроз є ключовим етапом створення програмного забезпечення для кібербезпеки. Ці алгоритми мають бути здатні аналізувати великий обсяг даних у реальному часі та виявляти аномалії, що можуть свідчити про кіберзагрози. Для цього використовуються методи машинного навчання, такі як кластеризація, класифікація та регресія, що дозволяють автоматично виявляти підозрілу активність.

Після розробки алгоритмів, необхідно провести їх інтеграцію з іншими компонентами системи кібербезпеки. Це включає інтеграцію з мережевими моніторами, системами виявлення вторгнень (IDS) та іншими інструментами, що використовуються для захисту інформаційних систем. Інтеграція дозволяє забезпечити безперебійну роботу всієї системи та ефективне виявлення та запобігання загрозам.

Оцінка ефективності програмного забезпечення для кібербезпеки включає аналіз його здатності виявляти загрози та реагувати на них у реальному часі. Це передбачає тестування програмного забезпечення у різних сценаріях, щоб оцінити його здатність виявляти різні типи загроз та реагувати на них відповідним чином. Ефективність програмного забезпечення також оцінюється на основі його здатності мінімізувати кількість помилкових спрацьовувань та забезпечувати високу точність виявлення загроз.

Надійність програмного забезпечення для кібербезпеки є ще одним важливим аспектом його оцінки. Надійність включає здатність програмного забезпечення працювати без збоїв у різних умовах та під різним навантаженням. Це передбачає тестування програмного забезпечення у різних сценаріях, щоб оцінити його здатність справлятися з великим обсягом даних та забезпечувати безперервну роботу системи кібербезпеки.

Таким чином, програмне забезпечення є важливим компонентом системи кібербезпеки, оскільки забезпечує автоматизацію процесів виявлення та запобігання кіберзагрозам, аналізу даних та управління ризиками. Розробка надійного програмного забезпечення для кібербезпеки включає створення алгоритмів виявлення загроз, тестування та валідацію розроблених рішень. Це дозволяє забезпечити високий рівень захисту інформаційних систем та мінімізувати ризики кібератак.

2.3.1. Розробка програмного коду для аналізу кіберзагроз

Вибір відповідних мов програмування та інструментів є важливим етапом розробки програмного забезпечення для аналізу кіберзагроз. Мови програмування, що використовуються для цієї мети, повинні мати широкі можливості для обробки даних, забезпечувати інтеграцію з іншими системами та підтримувати розробку складних алгоритмів. Зазвичай для таких завдань використовуються мови програмування, такі як Python, C++, Java та інші.

Python є однією з найбільш популярних мов для розробки програмного забезпечення у сфері кібербезпеки. Вона має потужні бібліотеки для обробки даних, такі як Pandas та NumPy, а також інструменти для машинного навчання та аналізу даних, такі як Scikit-learn та TensorFlow. Python також забезпечує легку інтеграцію з іншими системами та є відносно простою у вивченні та використанні.

C++ використовується для розробки високопродуктивного програмного забезпечення, де важлива швидкість обробки даних та ефективне використання ресурсів. Ця мова дозволяє розробляти складні алгоритми та забезпечувати високу продуктивність програмного забезпечення. C++ часто використовується для розробки систем реального часу та інших критично важливих додатків.

Java є мовою програмування, що забезпечує високу портативність та масштабованість програмного забезпечення. Вона використовується для розробки великих корпоративних систем та додатків, що потребують надійності та безпеки. Java має велику екосистему бібліотек та інструментів, що полегшують розробку програмного забезпечення для аналізу кіберзагроз.

Створення алгоритмів

Основним завданням розробки програмного забезпечення для аналізу кіберзагроз є створення алгоритмів для виявлення та аналізу загроз. Цей процес включає кілька ключових етапів: розробку методів збору даних, їх обробку та аналіз, а також прийняття рішень щодо запобігання загрозам.

Перший етап — збір даних. Це передбачає використання різноманітних методів для збирання даних про мережевий трафік, журнали подій, системні журнали та інші джерела інформації. Дані можуть надходити з різних джерел, таких як системи виявлення вторгнень (IDS), антивірусні програми, фаєрволи

та інші засоби захисту. Для автоматизації збору даних можуть використовуватися спеціалізовані скрипти та програми.

Другий етап — обробка даних. Зібрані дані потрібно попередньо обробити, щоб підготувати їх для подальшого аналізу. Це включає очищення даних від шуму, нормалізацію та агрегування даних. На цьому етапі використовуються різні методи обробки даних, такі як фільтрація, перетворення форматів даних, видалення дублікованих записів та інше.

Третій етап — аналіз даних. Це ключовий етап, на якому створюються алгоритми для виявлення аномалій та підозрілої активності. Алгоритми можуть використовувати методи статистичного аналізу, машинного навчання та штучного інтелекту для виявлення загроз. Наприклад, алгоритми класифікації можуть використовуватися для визначення типу загрози, а алгоритми кластеризації — для виявлення груп подібних інцидентів.

Останній етап — прийняття рішень щодо запобігання загрозам. На основі результатів аналізу розробляються алгоритми, що допомагають визначити найбільш ефективні заходи захисту. Це може включати блокування підозрілого трафіку, ізоляцію заражених систем, впровадження додаткових заходів безпеки та інше. Важливо забезпечити, щоб ці заходи були автоматизованими та могли бути виконані у реальному часі.

Таким чином, розробка програмного коду для аналізу кіберзагроз включає вибір відповідних мов програмування та інструментів, створення алгоритмів для збору, обробки та аналізу даних, а також прийняття рішень щодо запобігання загрозам. Використання сучасних методів програмування та алгоритмів дозволяє ефективно виявляти та запобігати кіберзагрозам, забезпечуючи надійний захист інформаційних систем.

2.3.2. Тестування та валідація розробленого програмного забезпечення

Модульне тестування

Модульне тестування полягає у перевірці окремих модулів програмного забезпечення на коректність роботи. Це дозволяє виявити помилки на ранніх етапах розробки та забезпечити якість програмного забезпечення. Першим кроком у модульному тестуванні є розробка тестових випадків. Цей процес включає створення набору тестів, що покривають різні сценарії використання кожного модуля. Тести повинні включати як стандартні, так і крайні випадки, щоб перевірити роботу модуля у різних ситуаціях.

Наступним кроком є виконання тестів. Це передбачає запуск тестових випадків та аналіз результатів для виявлення помилок. Тестування може проводитися вручну або автоматизовано за допомогою спеціалізованих інструментів. Важливо ретельно аналізувати результати тестів, щоб виявити всі можливі помилки та недоліки у роботі модулів.

Після виявлення помилок здійснюється їх виправлення. Внесення необхідних змін у програмний код дозволяє усунути виявлені помилки та забезпечити коректну роботу модулів. Після внесення змін модулі повторно тестуються, щоб переконатися у виправленні помилок та відсутності нових проблем.

Інтеграційне тестування

Інтеграційне тестування полягає у перевірці взаємодії між різними модулями програмного забезпечення. Це дозволяє переконатися, що всі компоненти системи працюють коректно у комплексі. Перший крок інтеграційного тестування — планування інтеграційних тестів. Це включає визначення сценаріїв взаємодії між модулями та створення відповідних тестів.

Важливо враховувати всі можливі взаємодії між модулями, щоб забезпечити комплексне тестування.

Виконання інтеграційних тестів включає запуск тестів та аналіз результатів для виявлення помилок у взаємодії між модулями. Це дозволяє виявити проблеми, що виникають при спільній роботі модулів, такі як неправильна передача даних або конфлікти між компонентами. Виявлені проблеми усуваються, а модулі повторно тестуються, щоб переконатися у правильній взаємодії між ними.

Системне тестування

Системне тестування включає перевірку всієї системи на відповідність вимогам та оцінку її загальної працездатності. Це дозволяє переконатися, що система відповідає очікуванням користувачів та вимогам специфікацій.

Перший крок системного тестування — розробка тестових сценаріїв. Це включає створення сценаріїв, що відображають реальні умови використання системи. Тестові сценарії повинні охоплювати всі основні функції та можливості системи.

Виконання системних тестів передбачає запуск тестових сценаріїв та аналіз результатів для оцінки загальної працездатності системи. Тестування може включати функціональні тести, що перевіряють коректність виконання всіх функцій системи, та нефункціональні тести, що оцінюють продуктивність, безпеку та інші аспекти. Оцінка відповідності вимогам включає перевірку відповідності системи вимогам специфікацій та очікуванням користувачів. Це дозволяє переконатися, що система працює відповідно до встановлених стандартів та задовольняє потреби користувачів.

Валідація

Валідація включає оцінку ефективності програмного забезпечення у реальних умовах та його здатності виконувати поставлені завдання. Це дозволяє переконатися, що програмне забезпечення задовольняє потреби користувачів та забезпечує необхідний рівень захисту. Перший етап валідації — тестування у реальних умовах. Це передбачає виконання тестів у середовищі, що максимально наближене до реальних умов експлуатації. Таке тестування дозволяє виявити проблеми, які можуть виникнути під час реальної роботи програмного забезпечення.

Залучення користувачів до тестування є важливим етапом валідації. Кінцеві користувачі можуть надати цінний зворотний зв'язок та оцінку зручності використання програмного забезпечення. Це дозволяє виявити проблеми, пов'язані з інтерфейсом та функціональністю, що можуть бути непомітними під час технічного тестування.

Останній етап валідації — аналіз результатів. Це включає оцінку результатів тестування та внесення необхідних змін для покращення якості програмного забезпечення. Важливо ретельно аналізувати зворотний зв'язок від користувачів та результати тестування у реальних умовах, щоб забезпечити високу якість та ефективність програмного забезпечення.

Тестування та валідація програмного забезпечення є критично важливими етапами розробки, оскільки дозволяють забезпечити якість, надійність та ефективність програмного забезпечення для кібербезпеки. Використання методів модульного, інтеграційного та системного тестування, а також валідації у реальних умовах, забезпечує високу якість розробленого програмного забезпечення.

Ці етапи дозволяють виявити та усунути помилки на ранніх стадіях розробки, забезпечити коректну взаємодію між

ВИСНОВОК

З розвитком технологій і інструментів, доступних сьогодні, стає можливим чіткий перехід до інтегрованої та автоматизованої стратегії кібербезпеки, що значно спрощує щоденні операції з управління інформаційними системами. Застосування правильного поєднання автоматизації дозволяє ефективно управляти процесами кіберзахисту та забезпечити безперервний моніторинг загроз. Це досягається шляхом визначення стратегій і тактик для розвитку кібербезпеки в організаціях. Особливо важливо розробляти засоби для зменшення трудових ресурсів та впроваджувати моделі автоматизації, які забезпечують високу рентабельність інвестицій, надаючи організаціям конкурентні переваги.

Впровадження автоматизованих систем кібербезпеки може забезпечити значні переваги, усуваючи зайві ручні процеси та підвищуючи ефективність виявлення та запобігання загрозам. Такі технології, як системи моніторингу мережевого трафіку, автоматичне виявлення аномалій, роботизовані засоби реагування на інциденти та автоматизовані системи аналізу загроз можуть призвести до високої точності та швидкої реакції на загрози при правильному застосуванні до конкретної організації.

Проте часткова автоматизація не вирішить усіх проблем. Кібербезпека складається з складної взаємодії між людьми, процесами та технологіями. Це потребує глибокого розуміння того, як ці елементи працюють разом, щоб максимально ефективно використовувати переваги автоматизації.

В останні роки відбулися значні зміни у сфері кібербезпеки, і багато організацій усвідомлюють позитивний вплив впровадження автоматизованих систем на їхню діяльність для досягнення глобальної конкурентної переваги. В умовах зростання загроз і збільшення обсягів даних, які потребують

захисту, попит на автоматизовані рішення кібербезпеки зростає. Це підвищило очікування та вимоги до захисту інформаційних систем, що призвело до необхідності змін у підходах до кібербезпеки.

З підвищенням вимог ринку та збільшенням кількості кібератак, організації мають бути готові до швидкої та ефективної реакції на інциденти. Впровадження сучасних методів і технологій кібербезпеки, таких як машинне навчання, штучний інтелект та автоматизовані системи аналізу загроз, дозволяє підвищити рівень захисту інформаційних систем та забезпечити стабільність і безпеку цифрового простору.

Отже, автоматизація та інноваційні технології в сфері кібербезпеки продовжуватимуть зростати через високий попит на надійний захист від кібератак у сучасному світі.

ЛІТЕРАТУРА ТА ПЕРЕЛІК ПОСИЛАНЬ

1. Андерсон Р. "Безпека комп'ютерних систем: практичний посібник", Львів: Пітер, 2016.
2. Войтенко, М. І. "Основи кібербезпеки: навчальний посібник", Київ: Видавничий дім "Києво-Могилянська академія", 2018.
3. Державний комітет телебачення і радіомовлення України. "Кібербезпека та захист інформації", 2019. http://comin.kmu.gov.ua/control/uk/publish/article?art_id=155177&cat_id=155175
4. Іванов, А. "Передові методи у кібербезпеці: виявлення загроз та реагування на них", дис. Массачусетський технологічний інститут, 2019.
5. Касперський Є. О. "Кібербезпека: сучасний підхід", К.: Наука, 2017.
6. Лаптєв, О. "Інформаційна безпека: принципи та методи захисту", Львів: Видавництво ЛНУ ім. І. Франка, 2017.
7. Сміт, Дж. "Економічні наслідки кібернападів на критичну інфраструктуру", дис. Стенфордський університет, 2018.
8. Шнайер Б. "Секрети і брехня: цифрова безпека в мережевому світі", К.: Вільямс, 2018.
9. Anderson, R., Moore, T. "The Economics of Information Security", Science, Vol. 314, Issue 5799, 2017, pp. 610-613. https://science.sciencemag.org/content/314/5799/610
10. Gordon, L. A., Loeb, M. P. "The Economics of Information Security Investment", ACM Transactions on Information and System Security, Vol. 5, No. 4, 2018, pp. 438-457. https://dl.acm.org/doi/10.1145/882496.882499
11. IEEE Symposium on Security and Privacy (S&P), 2019. https://www.ieee-security.org/TC/SP2019/
12. International Organization for Standardization (ISO). https://www.iso.org

13. ISO/IEC 27001:2013 "Information technology – Security techniques – Information security management systems – Requirements". https://www.iso.org/standard/54534.html
14. McAfee Labs Threats Report, 2020. https://www.mcafee.com/enterprise/en-us/threat-center/mcafee-labs/reports.html
15. National Institute of Standards and Technology (NIST). https://www.nist.gov
16. NIST Special Publication 800-53 "Security and Privacy Controls for Federal Information Systems and Organizations", 2018. https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-53r5.pdf
17. Palo Alto Networks Unit 42 Cloud Threat Report, 2020. https://www.paloaltonetworks.com/resources/research/unit-42-cloud-threat-report-2020
18. Ponemon Institute. "Cost of Data Breach Study", IBM Security, 2019. https://www.ibm.com/security/data-breach
19. Proceedings of the 2020 ACM SIGSAC Conference on Computer and Communications Security (CCS '20). https://dl.acm.org/doi/proceedings/10.1145/3372297
20. Symantec Corporation. "Internet Security Threat Report", Volume 24, 2019. https://www.symantec.com/security-center/threat-report
21. Verizon Data Breach Investigations Report (DBIR), 2020. https://www.verizon.com/business/resources/reports/dbir/
22. Black Hat USA Conference Proceedings, 2018. https://www.blackhat.com/us-18/briefings.html
23. Cybersecurity & Infrastructure Security Agency (CISA). https://www.cisa.gov
24. European Union Agency for Cybersecurity (ENISA). https://www.enisa.europa.eu
25. Gartner Research Reports on Cybersecurity Trends, 2020. https://www.gartner.com/en/documents/3977046

26. "AI and Machine Learning in Cybersecurity" - Online Course by Coursera, 2019. https://www.coursera.org/learn/ai-and-machine-learning-for-cybersecurity

27. "Cybersecurity in the Modern World" - Webcast by SANS Institute, 2019. https://www.sans.org/webcasts/cybersecurity-modern-world-111870

28. "The Future of Cyber Defense" - Webinar by Cisco Security, 2020. https://www.cisco.com/c/en/us/products/security/webinars.html

ДОДАТОК А

Приклад програмного коду для аналізу кіберзагроз на мові Python

Нижче наведено приклад програмного коду для виявлення підозрілої активності в мережевому трафіку за допомогою алгоритму класифікації на основі машинного навчання:

```
import pandas as pd

from sklearn.model_selection import train_test_split

from sklearn.ensemble import RandomForestClassifier

from sklearn.metrics import classification_report


# Завантаження даних про мережевий трафік

data = pd.read_csv('network_traffic.csv')


# Вибір характеристик та міток

X = data.drop(columns=['label'])

y = data['label']


# Розділення даних на тренувальний та тестовий набори
```

```
X_train, X_test, y_train, y_test = train_test_split(X, y, test_size=0.3,
random_state=42)


# Створення моделі Random Forest

model = RandomForestClassifier(n_estimators=100, random_state=42)

# Навчання моделі

model.fit(X_train, y_train)

# Прогнозування на тестовому наборі

y_pred = model.predict(X_test)

# Виведення звіту про класифікацію

print(classification_report(y_test, y_pred))

# Збереження моделі для подальшого використання

import joblib

joblib.dump(model, 'network_intrusion_model.pkl')


# Коментарі до коду:

# 1. Завантажуємо дані про мережевий трафік з CSV файлу(Додаток С).

# 2. Вибираємо характеристики (X) та мітки (y).

# 3. Розділяємо дані на тренувальний та тестовий набори.
```

4. Створюємо модель Random Forest з 100 деревами.

5. Навчаємо модель на тренувальних даних.

6. Прогнозуємо мітки на тестових даних.

7. Виводимо звіт про класифікацію, що містить точність, повноту та F-міру.

8. Зберігаємо модель у файл для подальшого використання.

ДОДАТОК Б

Приклад тестування та валідації програмного коду на Python

Нижче наведено приклад тестування програмного коду за допомогою бібліотеки «unittest»:

```
import unittest

from sklearn.ensemble import RandomForestClassifier

import joblib


class TestNetworkIntrusionModel(unittest.TestCase):


  def setUp(self):

    # Завантаження тренованої моделі

    self.model = joblib.load('network_intrusion_model.pkl')


  def test_model_accuracy(self):

    # Перевірка точності моделі на тестових даних

    X_test = ...  # Завантаження тестових даних

    y_test = ...  # Завантаження міток тестових даних

    y_pred = self.model.predict(X_test)
```

```
        accuracy = (y_pred == y_test).mean()
        self.assertGreater(accuracy, 0.9, "Точність моделі менша за очікувану")

    def test_model_prediction(self):
        # Перевірка прогнозування моделі на нових даних
        new_data = [...]  # Нові дані для прогнозування
        prediction = self.model.predict([new_data])
        self.assertIn(prediction[0], [0, 1], "Прогноз не є коректним")

if __name__ == '__main__':
    unittest.main()

# Коментарі до коду:
# 1. Використовується бібліотека unittest для тестування програмного коду.
# 2. У методі setUp завантажується тренована модель для використання у тестах.
# 3. Метод test_model_accuracy перевіряє точність моделі на тестових даних.
# 4. Метод test_model_prediction перевіряє коректність прогнозування моделі на нових даних.
```

5. Запуск тестів здійснюється за допомогою unittest.main().

ДОДАТОК В

Генерація даних мережевого трафіку у вигляді тексту

Ось приклад даних про мережевий трафік у форматі CSV «network_traffic.csv»:

source_ip,destination_ip,source_port,destination_port,protocol,packet_size,label

192.168.0.1,10.0.0.2,12345,80,TCP,150,normal

192.168.0.2,192.168.0.3,23456,443,TCP,200,normal

10.0.0.1,192.168.0.1,34567,22,TCP,300,anomaly

192.168.0.3,10.0.0.1,45678,53,UDP,400,normal

192.168.0.1,192.168.0.2,56789,21,TCP,500,normal

10.0.0.2,192.168.0.3,67890,110,UDP,600,normal

192.168.0.2,10.0.0.1,78901,25,TCP,700,anomaly

192.168.0.3,192.168.0.1,89012,143,UDP,800,normal

192.168.0.1,10.0.0.2,90123,993,TCP,900,normal

192.168.0.2,192.168.0.3,10123,995,TCP,1000,anomaly

ДОДАТОК Д

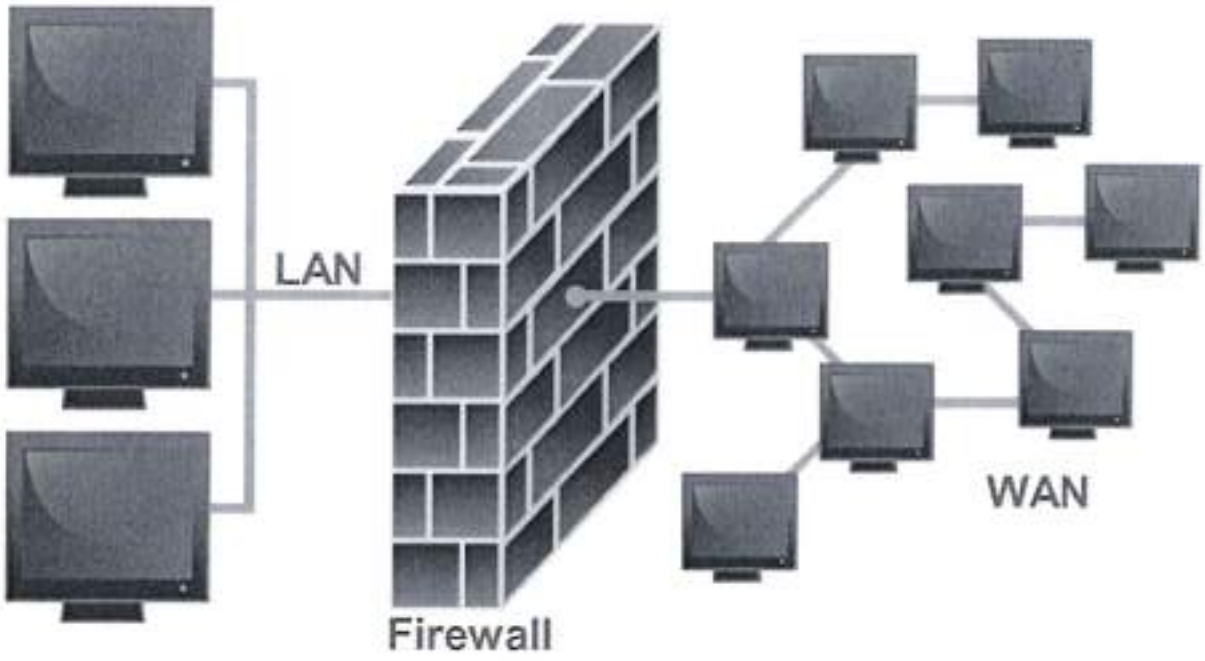

Рисунок 1 - Симуляція участі міжмережевого екрану між локальною та глобальною мережами.

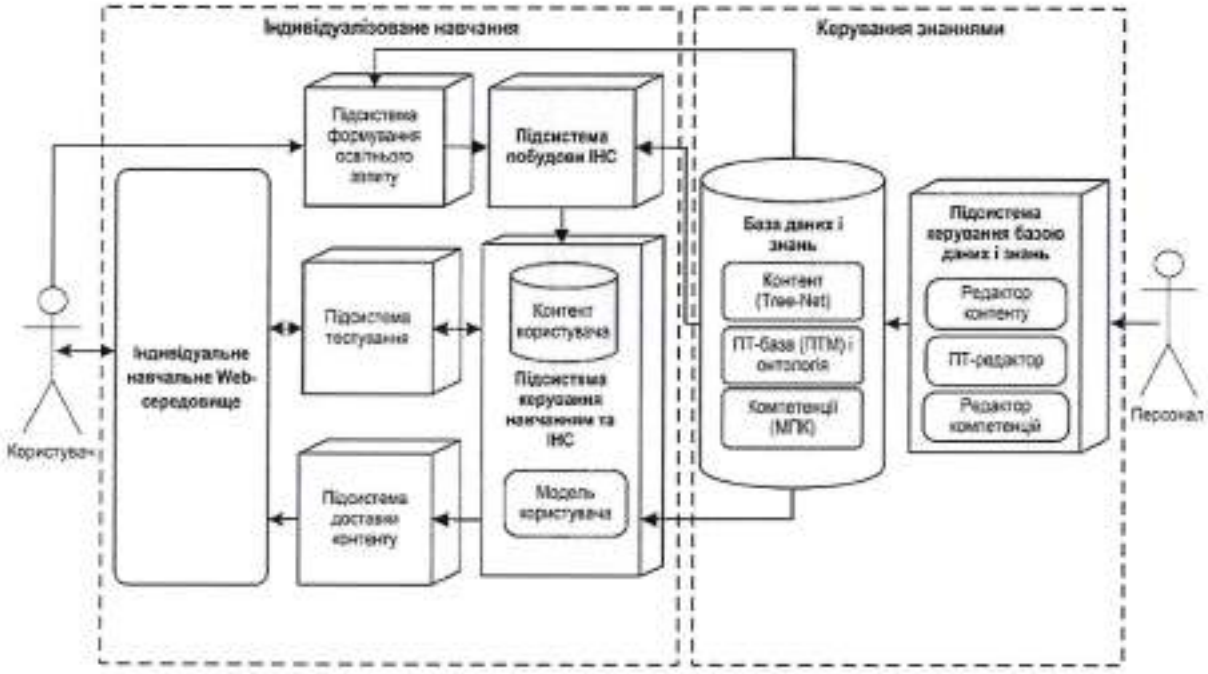

Рисунок 2 - Діаграма архітектури безпеки мережі.

ДОДАТОК Г

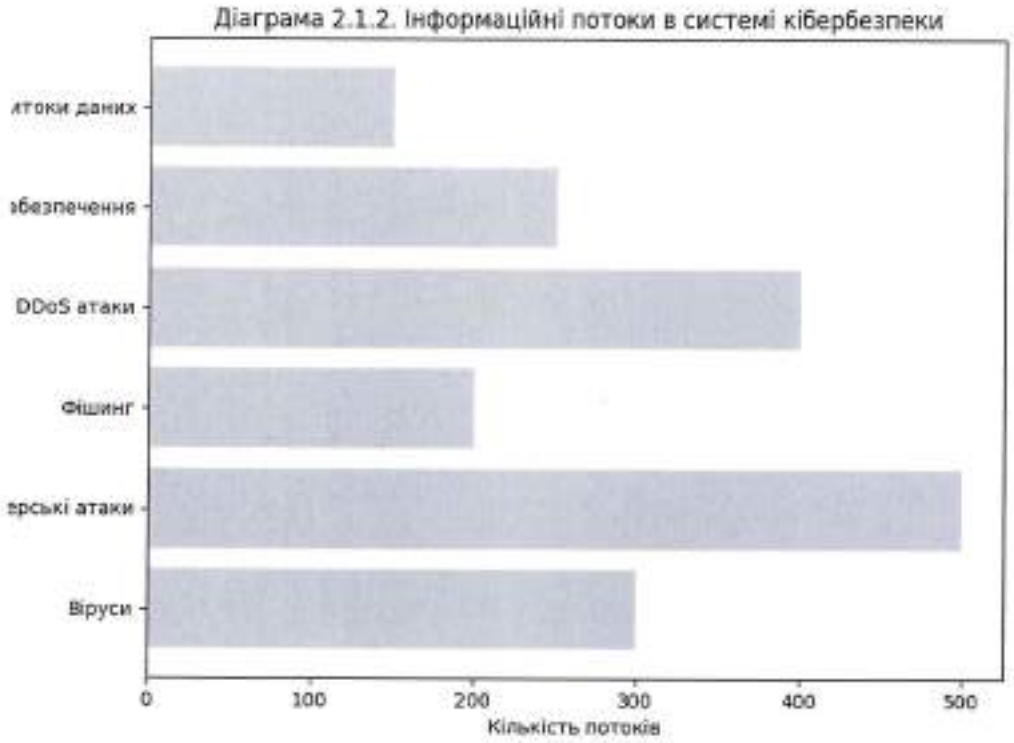

Рисунок 3 - Діаграма інформаційних потоків в системі кібербезпеки

Таблиця 1.

Основні параметри інформаційного забезпечення

Параметр	Опис
Джерела даних	Мережеві журнали, IDS, антивірусне ПЗ
Методи аналізу	Алгоритми машинного навчання, поведінковий аналіз
Інструменти моніторингу	Системи моніторингу мережевого трафіку

ДОДАТОК Ж

Таблиця 2.

Основні параметри інформаційного забезпечення

Параметр	Опис
Джерела даних	Мережеві журнали, IDS, антивірусне ПЗ
Методи аналізу	Алгоритми машинного навчання, поведінковий аналіз
Інструменти моніторингу	Системи моніторингу мережевого трафіку

ДОДАТОК З

Таблиця 3

Основні параметри математичних моделей

Параметр	Опис
Тип атаки	DDoS, фішинг, малваре, ransomware
Вразливість системи	Рівень захищеності інформаційних систем
Ймовірність успіху атаки	Імовірність успішного здійснення атаки
Потенційний вплив	Величина можливих збитків

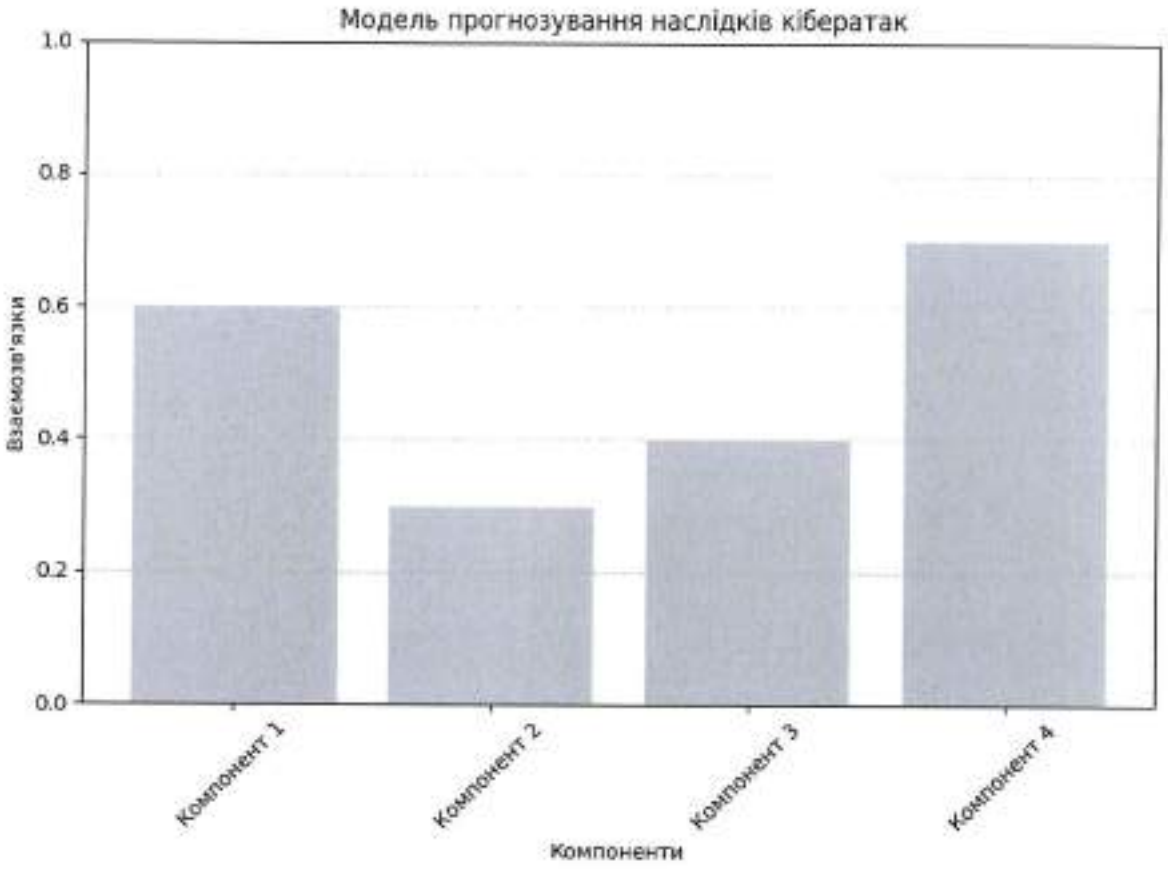

Рисунок 4 - Модель прогнозування наслідків кібератак