Міністерство освіти і науки України
Тернопільський національний технічний університет імені Івана Пулюя
(повне найменування вищого навчального закладу)
Факультет комп'ютерно-інформаційних систем і програмної інженерії
(назва факультету)
Кафедра кібербезпеки
(повна назва кафедри)

КВАЛІФІКАЦІЙНА РОБОТА

на здобуття освітнього ступеня

бакалавр
(освітній рівень)

на тему: " Система захисту комп'ютерної мережі підприємства "

Виконав: студент (ка)
Спеціальності:
125 «Кібербезпека»
(шифр і назва напряму підготовки, спеціальності)
.... Цалко Мирослав Віталійович
.....підпис..... (прізвище та ініціали)

Керівник ... Муж В.В.
.....підпис..... (прізвище та ініціали)

Нормоконтроль .....Тимощук Д. І.....
підпис..... (прізвище та ініціали)

Завідувач кафедри .....Загородна Н.В.
підпис..... (прізвище та ініціали)

Рецензент .....Баран. І.О.
підпис..... (прізвище та ініціали)

м. Тернопіль – 2024

Міністерство освіти і науки України
Тернопільський національний технічний університет імені Івана Пулюя

Факультет комп'ютерно-інформаційних систем і програмної інженерії
(повна назва факультету)

Кафедра Кібербезпеки
(повна назва кафедри)

ЗАТВЕРДЖУЮ
Завідувач кафедри
_____ Загородна Н.В.
(підпис) (прізвище та ініціали)
«__» _____ 2024 р.

ЗАВДАННЯ
НА КВАЛІФІКАЦІЙНУ РОБОТУ

на здобуття освітнього ступеня Бакалавр
(назва освітнього ступеня)

за спеціальністю 125 Кібербезпека
(шифр і назва спеціальності)

Студенту Цалку Мирославу Віталійовичу
(прізвище, ім'я, по батькові)

1. Тема роботи Система захисту комп'ютерної мережі підприємства

Керівник роботи Муж Валерій Вікторович, к.ю.н., доцент
(прізвище, ім'я, по батькові, науковий ступінь, вчене звання)

Затверджені наказом ректора від «15» 04 2024 року № 4/7-350

2. Термін подання студентом завершеної роботи 26.06.2024

3. Вихідні дані до роботи Розглянути питання захисту інформації в комп'ютерних мережах Визначити методи захисту периметра мережі підприємства. Дослідити заходи захисту комп'ютерної мережі від розподілених атак

4. Зміст роботи (перелік питань, які потрібно розробити)
Стан захисту інформації в підприємствах.
Методи забезпечення безпеки мережевого периметра.
Стратегії захисту комп'ютерних мереж від розподілених атак.
Безпека життєдіяльності, основи охорони праці
Висновки

5. Перелік графічного матеріалу (з точним зазначенням обов'язкових креслень, слайдів)
Презентація PowerPoint .

6. Консультанти розділів роботи

Розділ	Прізвище, ініціали та посада консультанта	Підпис, дата	
		завдання видав	завдання прийняв
Безпека життєдіяльності, основи хорони праці	Мариненко С.Ю., к.т.н., доцент		

7. Дата видачі завдання 29.01.2024 р.

КАЛЕНДАРНИЙ ПЛАН

№ з/п	Назва етапів роботи	Термін виконання етапів роботи	Примітка
1.	Ознайомлення з завданням до кваліфікаційної роботи	29.01 – 30.01	Виконано
2.	Опрацювання джерел в галузі дослідження	06.02 – 20.02	Виконано
3.	Провів аналіз методів захисту	22.02 – 12.03	Виконано
4.	Оформлення розділу «Стан проблеми захисту інформації підприємства»	10.02 – 05.03	Виконано
5.	Оформлення розділу «Захист мережевого периметра комп’ютерної мережі підприємства»	26.03 – 04.05	Виконано
6.	Оформлення розділу «Захист комп’ютерної мережі від розподілених атак»	12.04-20.04	
7.	Виконання завдання до підрозділу «Безпека життєдіяльності, основи охорони праці»	25.04 – 10.05	Виконано
8.	Оформлення кваліфікаційної роботи	23.05 – 24.06	Виконано
9.	Нормоконтроль	24.06 – 26.06	Виконано
10.	Перевірка на плагіат	26.06 – 27.06	Виконано
11.	Захист кваліфікаційної роботи	28.06.2023	

Студент _____ Цалко.М.В.
(підпис) (прізвище та ініціали)

Керівник.роботи _____ Муж В.В.
(підпис) (прізвище та ініціали)

АНОТАЦІЯ

Система захисту комп'ютерної мережі підприємства // Кваліфікаційна робота ОР «Бакалавр» // Цалко Мирослав Віталійович // Тернопільський національний технічний університет імені Івана Пулюя, факультет комп’ютерно-інформаційних систем і програмної інженерії, кафедра кібербезпеки, група СБс-43 // Тернопіль, 2023 // С. 67 , рис. – 9, табл. – - , кресл. – - , додат. – -.

КЛЮЧОВІ СЛОВА: IoT, дані, мережа, VPN, шифорування, атака

Актуальність теми: У зв'язку з постійними загрозами кібербезпеки в.сучасному світі, де діджиталізація підприємств зростає, важливість забезпечення безпеки комп'ютерних мереж також збільшується. Основні аспекти цієї теми включають захист від кібератак, захист конфіденційності інформації, забезпечення безперебійності роботи мережі підприємства.

Об'єкт та предмет дослідження: Корпоративна комп'ютерна мережа підприємства, стан проблем захисту інформації, захист мережевого периметра, захист комп'ютерної мережі від розподілених атак. Система захисту комп'ютерної мережі підприємства

Мета кваліфікаційної роботи: Розв'язання проблем захисту комп'ютерних мереж підприємств, класифікація комп'ютерних атак і систем їх виявлення, розробка проактивної системи захисту інформації, вибір розподіленої системи виявлення вторгнень.

Для досягнення поставленої мети використовуються метод аналітичного огляду, аналіз вихідних даних для розробки рішень та базова структура системи захисту периметра мережі. Також розглядається технологія "Медова пастка" як приманка в системі безпеки промислового підприємства. Проаналізовано стратегії конфлікту та динамічний характер його розвитку, який взаємодіє з "медовою пасткою".

Рекомендується використовувати матеріали кваліфікаційної роботи під час розробки системи захисту комп’ютерної мережі підприємства.

ANNOTATION

The enterprise computer network protection system // Qualification work of OR "Bachelor" // Tsalko Myroslav Vitaliyovych // Ivan Pulyuy Ternopil National Technical University, Faculty of Computer Information Systems and Software Engineering, Department of Cyber Security, SBc-43 Group // Ternopil, 2023 // P. 67, fig. - 9, table – - , chair. – - , add. – -.

KEY WORDS: IoT, data, network, VPN, encryption, attack

Relevance of the topic: In connection with the constant threats of cyber security in the modern world, where the digitization of enterprises is growing, the importance of ensuring the security of computer networks is also increasing. The main aspects of this topic include protection against cyber-attacks, protection of information confidentiality, ensuring uninterrupted operation of the enterprise network.

Object and subject of research: Corporate computer network of the enterprise, state of information protection problems, network perimeter protection, computer network protection from distributed attacks. System of protection of the computer network of the enterprise

The purpose of the thesis: Solving the problems of protecting computer networks of enterprises, classifying computer attacks and their detection systems, developing a proactive information protection system, choosing a distributed intrusion detection system.

To achieve the goal, the method of analytical review, the analysis of initial data for the development of solutions and the basic structure of the network perimeter protection system are used. The "Honey Trap" technology is also considered as a bait in the security system of an industrial enterprise. The strategies of the conflict and the dynamic character of its development, which interacts with the "honey trap", are analyzed.

It is recommended to use the materials of the thesis during the development of the computer network protection system of the enterprise.

ЗМІСТ

ПЕРЕЛІК УМОВНИХ ПОЗНАЧЕНЬ

EOM	—	Електронно - обчислювальна машина
SRTOS	—	Система м'яких часових обмежень
HRTOS	—	Система жорстких часових обмежень
NPS	—	Захист периметру мережі
NT	—	Мережевий трафік
CA	—	Кібернетична атака
ACL	—	Список доступу
IDS	—	Система для виявлення вторгнень
DA	—	Розподілена атака
HTT	—	Honeypot технологія
AAAD	—	Аналіз стратегій нападу та оборони

ВСТУП

Системи захисту комп’ютерної мережі підприємства мають вирішальне значення для ефективної роботи мереж підприємства.

Останнім часом існує великий інтерес до системного аналізу та методів оптимізації для захисту комп’ютерів і мереж від атак і несанкціонованих вторгнень.

Наведено велику кількість прикладів таких систем, розробки різноманітних протоколів, технологій, проектів і пов’язаних з ними міркувань, висновків і прогнозів.

Враховуючи різноманітність загроз і складність сучасних мереж, впровадження рішення.захисту вимагає великих знань і досвіду в.ряді вузькоспеціалізованих областей.

В цій кваліфікаційнії поставлено за мету:

- провести аналіз стану захисту інформаційної мережі підприємства;
- пизначити методи забезпечення безпеки мережевого периметра;
- дослідити заходи захисту комп'ютерних мереж від розподілених атак;
- розробити проактивну систему захисту інформації;
- використати технологію "Медова пастка" для підвищення безпеки;
- провести модернізацію існуючих моделей захисту;

Поширені загрози включають навмисне використання коду зловмисного програмного забезпечення (віруси, хробаки, троянські програми), а також атаки.DoS (відмова в обслуговуванні) і DDoS (розподілена відмова в обслуговуванні). canopy).

Є кілька важливих елементів.безпеки, які повинні бути відображені в створюваній інфраструктурі безпеки управління доступом. управління загрозами. управління конфіденційністю. Вести журнали контролю та моніторингу.

Дослідження в області виявлення атак на мережі та комп'ютерні.системи проводяться протягом тривалого часу.

Вивчаються ознаки атак, розроблені та використовуються методи та засоби виявлення спроб несанкціонованого проникнення через системи безпеки, як мережеві, так і локальні – на логічному і навіть.фізичному рівнях.

Фактично, це також може включати дослідження в області наведення та горизонтального електромагнітного випромінювання, оскільки електромагнітні атаки безпосередньо впливають на середовище комп’ютерної мережі.

Не менш глибокі дослідження проводяться.в області захисту від комп'ютерних атак, розробки систем виявлення вторгнень тощо.

Сьогодні системи виявлення атак і вторгнень часто являють собою програмні або апаратні рішення, які автоматизують процес моніторингу подій, що відбуваються в комп’ютерних системах або мережах, а також незалежний аналіз подій для пошуку ознак інциденту безпеки.

Оскільки за останні роки кількість.типів і способів організації несанкціонованого проникнення в чужі комп'ютерні мережі.значно зросла, системи виявлення атак стали необхідним елементом рівня безпеки інфраструктури будь-якого агентства, організації та компанії.

Системи для виявлення аномальної поведінки (виявлення аномалії) покладаються на той факт, що відома деяка сигнатура, яка характеризує правильну або прийнятну поведінку спостережуваного об'єкта.

"Природна" поведінка відноситься до дій об'єкта, які відповідають політиці безпеки. Системи виявлення недоброзичливої поведінки (виявлення зловживань) ґрунтуються на тому, що конкретні ознаки, що описують поведінку порушника, відомі заздалегідь. Найпоширенішими методами виявлення недоброзичливої поведінки є технічні та статистичні підходи. Системи виявлення атак, як і більшість сучасних програмних продуктів, повинні відповідати ряду вимог. Це інноваційні технології розробки, орієнтовані на характеристики сучасних інформаційних мереж і сумісність з іншими програмами. При побудові системи захисту комп’ютерної мережі необхідно враховувати такі фактори комп’ютерна мережа за визначенням – це система, розподілена за територією та функціями. - атаки на комп'ютерні мережі дуже різноманітні. більшість атак і вторгнень, здійснених зловмисниками, також мають розподілений і скоординований характер. - найнебезпечніші атаки на системи захисту інформації абсолютно випадкові та некорельовані в часі та просторі. заходи протидії розподіленим атакам від автономних кінцевих вузлів мережі, як правило, не вдаються. Перераховані

вище фактори, що впливають на природну роботу комп'ютерних мереж загального призначення, однаково важливі для комп'ютерних мереж і систем підприємства. Однак комп'ютерні мережеві системи, спрямовані на захист бізнесу, мають принципові відмінності в плані побудови, що випливає з характеристик комп'ютерних мереж і систем, які забезпечують можливість автоматизації та роботизації технологічної роботи бізнесу. Найбільш істотною відмінністю є фактор часу. Комп’ютерні мережі та бізнес-системи завжди повинні бути системами реального часу. Крім того, лише системи реального часу використовуються в критично важливих додатках.

Значущу роль в цьому відіграють організаційні заходи, які потребують особливої уваги. Виходячи з вищесказаного, розглянемо основне завдання кваліфікаційної роботи.

Проведення детального аналізу стану інцидентів і невирішених проблем у сфері захисту комп'ютерної мережі компанії.

Опис основних напрямків розвитку компонентів системи захисту:

- периметр мережі вузлів і каналів передачі даних;
- браундтмауери та маршрутизатція із фільтрацією пакетів. - транслятори мережевих адрес;
- транслятори адрес основного та альтернативного портів;
- Розробка підсистем захисту від розподілениих кібератак;
- фейкові сервіси з вказаними вразливими місцями (" медові пастки ");
- сервіс, який видає себе за вразливу мережу (мережні " медові пастки ");

В кваліфікаційнії роботі буде розроблено систему захисту комп'ютерної мережі із різними принципами боротьби з атаками та несанкціонованими вторгнення.

РОЗДІЛ 1. АНАЛІЗ СТАНУ ПРОБЛЕМ ЗАХИСТУ ІНФОРМАЦІЇ НА ПІДПРИЄМСТВІ

Особливості комп'ютерних і керуючих мереж компанії відзначаються відмінністю від інформаційних мереж загального призначення. З метою висвітлення цієї унікальності, розглянемо основні риси бізнес-мереж та надамо перелік термінів і визначень, які будуть використовуватися в подальшому.

Джерела включають законодавство України, рішення адміністративних органів, праці наукових установ, монографії та дисертації.

1.1 Загальні відомості

Для успішного функціонування в сучасному бізнесі важливо відповідати високим стандартам, зокрема, забезпечувати абсолютну безпеку протягом робочого дня чи будь-якого іншого періоду роботи, такого як тиждень чи місяць. Під абсолютною безпекою ми маємо на увазі характеристики, ймовірність відповідності якими прагне досягти одиниці протягом обраного періоду експлуатації.

Це особливо важливо для таких галузей, як авіаційні та аерокосмічні комплекси, металургія, хімія, транспорт, енергетика та інші системні галузі. Живучість системи, її здатність працювати в різних умовах, включаючи хімічне чи бактеріальне зараження, електромагнітний чи радіаційний вплив, є ключовою характеристикою.

Система реального часу – це комплекс апаратного та програмного забезпечення, який реагує на непередбачуваний потік подій у передбачуваний час. Гнучка система реального часу може призвести до збільшення витрат і зниження продуктивності, але часто вона не має критичного значення для часу реакції.

Системи жорсткого реального часу недопускають затримок у відповідях, оскільки це може мати серйозні наслідки, включаючи катастрофічні наслідки та великі витрати. Основна відмінність між жорсткими і м'якими системами реального часу полягає в тому, що жорсткі системи не можуть допускати

затримок у реакції на події.

Інформаційна, обчислювальна та керуюча мережа компанії являє собою комп'ютерну та телекомунікаційну систему, яка може бути як дротовою, так і бездротовою, і повинна працювати в режимі реального часу. Для підприємств загального застосування це може бути м'який режим реального часу, а для критично важливих підприємств – жорсткий режим реального часу.

1.2 Принцип захисту комп'ютерної мережі підприємств

Концепція інформації нерозривно пов'язана з комп'ютерними технологіями, системами та мережами зв'язку. Отже, стає очевидною важливість захисту інформації, що зберігається в них. Чесна конкуренція передбачає змагання, що базується на повазі до закону та загальноприйнятих етичних стандартах.

Незважаючи на це, існують випадки, коли конкуруючі підприємці вдаються до протиправних дій для отримання інформації, що завдає шкоди інтересам іншої сторони. Ця інформація може використовуватися в цілях отримання конкурентної переваги на ринку.

Криміналізація суспільства та неефективність правоохоронної системи змушують представників економіки, виробництва та бізнесу вживати заходів для боротьби з негативними процесами, які призводять до витоку конфіденційної інформації.

Багатофакторний ріст комп'ютерної злочинності пов'язаний із:

- Переходом від традиційної "паперової" технології до електронної, при цьому технології захисту інформації не завжди належним чином розвинені.
- Уніфікацією IT-систем, створенням глобальних мереж та розширенням доступу до інформаційних ресурсів.
- Підвищеною складністю програмних засобів.

Останні дослідження інформаційної безпеки свідчать про зростання кількості порушень у сфері комп'ютерної злочинності. У зв'язку з

різноманітністю загроз і складністю сучасних мереж, розробка систем захисту вимагає глибоких знань і досвіду у ряді вузькоспеціалізованих областей.

Поширені загрози включають навмисне використання шкідливих програмних кодів (вірусів, хробаків, троянських програм), а також розподілені атаки DoS (відмова в обслуговуванні) і DDoS (розподілена відмова в обслуговуванні).

Важливими елементами, які повинні бути враховані при розробці інфраструктури безпеки, є:

- контроль доступу;
- конфіденційність;
- управління загрозами;
- забезпечення контролю та моніторингу;

1.3 Класифікація і виявлення комп'ютерних атак

Захист від можливих кібератак вимагає детальної класифікації, що сприяє виявленню та подоланню цих загроз. В даний момент існує значна кількість різноманітних таксономічних ознак. Наприклад, можливо класифікувати атаки за такими ознаками, як пасивні та активні, зовнішні та внутрішні, свідомі та несвідомі, і так далі.

На жаль, деякі із існуючих класифікацій не завжди практично застосовні, але вони все ще використовуються при виборі та використання систем виявлення атак і вторгнень.

Дослідимо декілька прикладів класифікацій комп'ютерних атак які широко використовуються для захисту конфіденційної інформації в державних організаціях:

1) Локальний доступ. Тип атаки, який призводить до несанкціонованого доступу до вузла, на який вони спрямовані.
2) Віддалений доступ. Вид атаки, що надає можливість дистанційного керування і проникнення на робочу станцію.
3) Атака з використанням зломщика паролів. Атака, базована на

використанні програм для підбору паролів користувачів.

4) Атаки на аналізатор протоколів. Вид атаки, який використовує аналізатори протоколів для перехоплення мережевого трафіку та доступу до конфіденційної інформації.
5) Атака мережевим сканером. Тип атаки, заснований на використанні мережевого сканера для аналізу топології мережі та визначення служб, доступних для атаки.
6) Атака за допомогою сканерів вразливостей (Vulnerability Scanner). Вид атаки, який використовує сканери вразливостей для пошуку уразливостей на вузлах мережі.

На рисунку 1.1 класифікація мережних атак різних рівнів. Є вичерпною з практичної точки зору, оскільки охоплює практично всі можливі дії зловмисника. Проте, для повноцінного захисту від кібератак, необхідно не лише класифікувати, але й визначати вразливі компоненти мережі та можливі наслідки успішного проведення атак.

У цьому випадку.в аналіз не входить найважливіший фактор – модель загрози безпеці, з якої починаються всі заходи щодо забезпечення захисту інформації.

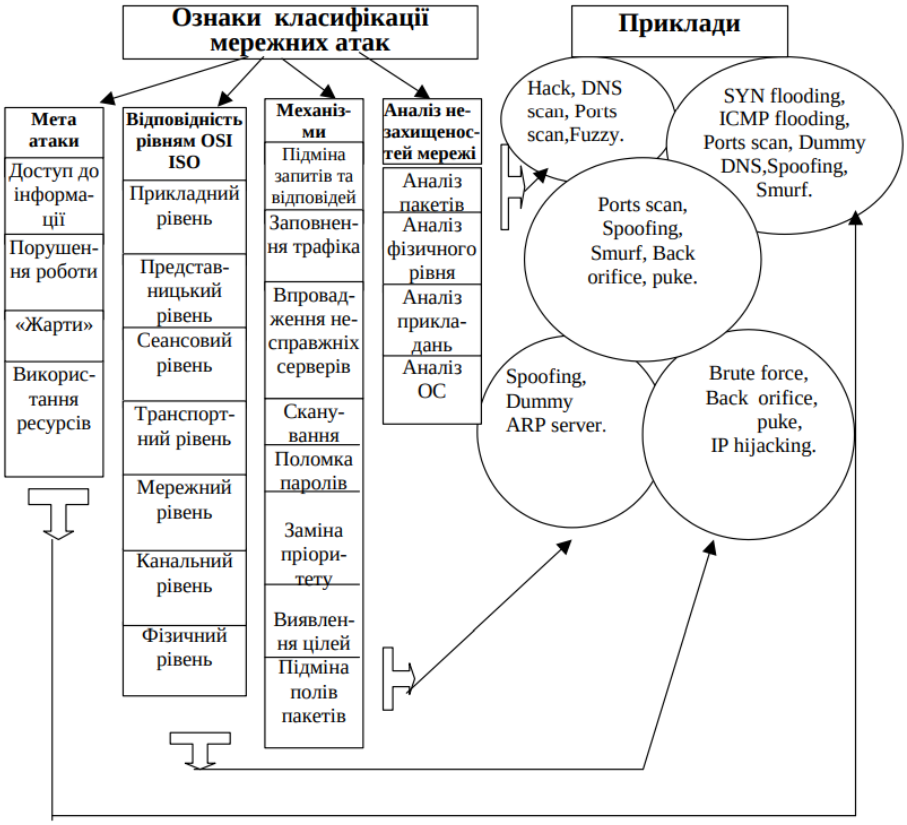

Рисунок 1.1 – Класифікація мережних атак різних рівнів

Можливі загрози для корпоративних мереж включають наступне. Аналіз мережевого трафіку є ефективним методом отримання доступу до логінів та паролів користувача. З цією метою використовується спеціальна програма - аналізатор пакетів, яка займається перехопленням пакетів в мережі та виділяє ті, що містять ідентифікатор і пароль користувача. У багатьох протоколах дані передаються без шифрування взагалі, що робить їх вразливими. Аналіз мережевого трафіку дозволяє отримати доступ до даних, передаваних через протоколи SMTP, FTP, HTTP, POP3, TELNET, IMAP, IRC і NNTP. Це може призвести до блокування паролів для поштових систем, номерів кредитних карток та іншої особистої інформації.

Хоча існують протоколи обміну для захисту мережевих з'єднань та шифрування трафіку, вони ще не стали стандартом через обмеження на експорт крипто інструментів у деяких країнах. Це призводить до того, що реалізації цих протоколів не вбудовані в програмне забезпечення або мають обмежену ефективність.

Аналіз мережевого трафіку може вивчити логіку роботи розподіленої

комп’ютерної системи, забезпечуючи однозначну відповідність між подіями та командами, що відбуваються в системі. Це дозволяє симулювати та виконувати віддалені атаки на практиці, як буде показано в наступних параграфах на прикладі розподілених систем.

Здійснення аналізу мережевого трафіку надає можливість перехоплювати потоки даних, які обмінюються об'єкти в розподіленій системі. Отримання несанкціонованого доступу до інформації, що передається між двома абонентами мережі, є основою віддаленої атаки цього типу. Слід зауважити, що аналіз трафіку можливий лише в межах одного сегмента мережі, і немає можливості змінювати сам трафік.

Наприклад, в ході такої атаки можуть бути перехоплені ім'я користувача та пароль, надіслані без шифрування через мережу. Важливо враховувати пасивний характер аналізу мережевого трафіку та його потенційні наслідки для інформаційної безпеки в сегменті мережі.

Ще однією проблемою безпеки розподіленої комп'ютерної мережі є неадекватна ідентифікація та автентифікація віддалених об'єктів. Для вирішення цієї проблеми у розподілених системах часто використовують створення віртуальних каналів з подальшим обміном інформацією для їх однозначної ідентифікації, що іноді називається "рукостисканням". Проте, цей метод не завжди застосовується для всіх віддалених об'єктів у розподілених комп'ютерних мережах.

Для ідентифікації об'єктів розподіленої системи використовують мережеві адреси, унікальні для кожного об'єкта системи. Однак, варто враховувати, що ці адреси можуть бути піддаватися підробці, що ускладнює їх використання як однозначного ідентифікатора об'єктів.

У рисунку 1.2 наведено основні підходи до створення систем виявлення атак, які включають у себе різні методи та стратегії забезпечення безпеки мереж.

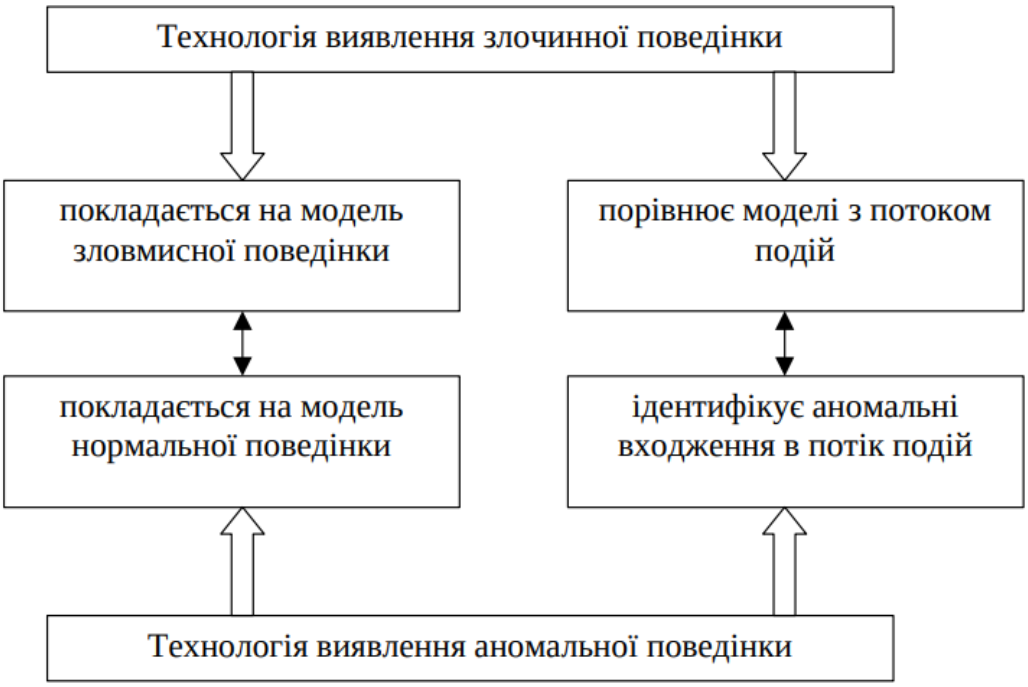

Рисунок 1.2. Основні підходи до створення систем виявлення атак

При побудові системи захисту комп’ютерної мережі необхідно враховувати наступні фактори:

- Комп’ютерні мережі за визначенням є системою, розподіленою відповідно до території та функцій.
- атаки на комп'ютерні мережі красочні.
- більшість атак і вторгнень, здійснених зловмисниками, також мають розподілений і скоординований характер.
- найнебезпечніші атаки на системи захисту інформації – абсолютно випадкові та некорельовані в часі та просторі.
- Примусові заходи протидії розподіленим атакам автономними мережевими термінальними вузлами, як правило, будуть безуспішними.

Перераховані вище чинники, які впливають на ефективну роботу комп'ютерних мереж загального призначення, є однаково важливими для комп'ютерних мереж і систем підприємства. Проте, системи комп'ютерних мереж, спрямовані на захист бізнесу, мають основні відмінності в архітектурному плані, визначені характеристиками мереж та систем, які надають можливість автоматизації та роботизації підприємницької діяльності.

Однією з ключових відмінностей є чинник часу.

Системи комп'ютерних мереж і бізнес-систем повинні завжди працювати в режимі реального часу. Важливо зазначити, що лише системи реального часу використовуються в компаніях з критично важливими додатками.

Ще одним важливим аспектом, що впливає на інформаційну безпеку підприємства, є наявність або відсутність територіально розподілених філій і підрозділів. Згідно з нормативами, якщо головне підприємство має розгорнуту систему захисту інформації, то філії та канали обміну даними можуть бути менш захищеними з різних об'єктивних та суб'єктивних причин.

З іншого боку, можливість існування корпоративних одиниць, розташованих географічно та відповідних стандартам і протоколам, може суттєво поліпшити ефективність всіх вузлів та частини системи захисту. Організаційні заходи грають ключову роль і вимагають особливої уваги.

Аналіз комп’ютерних атак Системи виявлення вторгнень (IDS) став необхідною складовою стратегії кіберзахисту. За останні роки їх популярність значно зросла, оскільки виробники засобів безпеки вдосконалили якість і сумісність своїх програм. Основу IDS складає аналітика, яка в процесі аналізу перевіряє кожен пакет, визначаючи його безпечність, та видає попередження при необхідності. Це є основною метою IDS.

На сьогодні існують два різні підходи до систем виявлення вторгнень (IDS). Обидва методи мають свої прихильників і активно рекламуються за допомогою різноманітних маркетингових матеріалів та прикладів для підтримки їхньої ефективності.

Проте, незважаючи на популярність обох методів, кожен з них має свої недоліки. Давайте зосередимося на порівнянні їх після вивчення детермінованих методів аналізу комп'ютерних атак, таких як аналіз сигнатур та аналіз протоколів [1].

Одним з підходів до IDS є детермінований аналіз, який включає в себе аналіз сигнатур та аналіз протоколів. Основна функція систем виявлення вторгнень полягає в контролі вхідного та вихідного мережевого трафіку. Вони подібні до брандмауерів, але відрізняються тим, що не модифікують потоки

трафіку, але шукають потенційно зловмисний трафік. У разі виявлення аномалій вони надсилають повідомлення адміністраторам системи.

Другий метод включає аналіз форматованих даних мережевого трафіку, відомих як протоколи. Кожен пакет має свій власний протокол, який може бути відкоригований або модифікований авторами IDS відповідно до стандартів RFC. Кожен протокол має набір полів з очікуваними або стандартними значеннями. Якщо виявляється, що яке-небудь значення порушує стандарти, генерується тривога.

Аналіз протоколів передбачає глибоке розуміння очікуваних значень полів пакетів для виявлення потенційно шкідливого трафіку. Цей метод дозволяє ідентифікувати аномалії в будь-якому з поля пакета, такому як IP, TCP та UDP, і вчасно сповіщати про можливі загрози.

Таким чином, обидва методи IDS мають свої плюси та мінуси, і вибір між ними потрібно робити з урахуванням конкретних потреб конкретної системи виявлення вторгнень.

Перші версії цих систем виявилися дуже простими і легко обманюваними. Аналіз протоколу відрізняється від сигнатурного аналізу, який використовує характеристики атаки для сповіщень.

Система аналізу сигнатур має численні переваги. Вона працює швидко, порівняно з повним аналізом пакетів, що є складним завданням. Правила легко створювати, розуміти та налаштовувати, а IT-спільнота швидко створює сигнатури для нових загроз.

Ці системи виявляють хакерів на ранніх стадіях, адже прості атаки зазвичай використовують впізнавані методи. Аналітика на основі сигнатур точно й оперативно підтверджує правильну роботу системи.

Проте IDS, який базується лише на аналізі сигнатур, має свої недоліки. Його швидкість сповільнюється з часом, коли збільшується кількість перевірених підписів. Це критичне, оскільки нові атаки розширюють список підписів, що потрібно перевірити, і ефективні методи обробки даних не завжди допомагають уникнути проблеми.

У випадку аналізу протоколів виникає подібна ситуація система має свої

позитивні та негативні аспекти, але вимагає ретельної попередньої обробки протоколів, що може сповільнити аналіз. Важливо відзначити, що складно сформулювати та зрозуміло викласти правила перевірки протокольної системи. У цьому випадку ми повинні покладатися на добру волю розробників програмного забезпечення, оскільки правила стають відносно складними і їх втілення не завжди є простим завданням.

Додатково, правила стають складнішими, іноді відхиляючись від загальноприйнятих стандартів, протоколів та RFC, що створює додаткові труднощі для розробників систем виявлення вторгнень (IDS) і створює можливості для зловмисників.

На перший погляд, системи IDS, що ґрунтуються на аналізі протоколів, можуть працювати повільніше порівняно з системами, що базуються на сигнатурному аналізі, які мають більший охоплення і результативність.

Крім того, такі системи здатні виявляти "генетичні збої" та часто можуть визначати "експлойти нульового дня", що взагалі недосяжне для систем, ґрунтованих на сигнатурному аналізі.

На жаль, іноді ці системи можуть пропустити неканонічні події, такі як власні сесії Telnet, що не порушують жодних протоколів. З іншого боку, системи, що базуються на аналізі протоколів, мінімізують помилкові тривоги, зафіксовуючи фактичні порушення, але не завжди забезпечують достатньо інформації.

Щодо методів виявлення вторгнень, таких як аналіз сигнатур та аналіз протоколів, на перший погляд вони здаються суттєво відмінними, але при ближчому розгляді можна виявити певну схожість.

Обидва методи виявлення вторгнень зосереджуються на перевірці відформатованих даних для виявлення атак та аномалій. Слабкість обох методів полягає в їхній неспроможності ефективно виявляти нові, щойно створені загрози, так звані експлойти.

Однак існують альтернативні підходи, такі як статистичні методи, що використовують байєсівські, методи мінімальної ймовірності та методи максимальної правдоподібності. Статистичні методи виявлення аномальної

поведінки стали дуже поширеними, де датчики збирають інформацію та формують профілі, що описують типову поведінку об'єкта.

На початковому етапі формування профілю збирається різноманітна інформація про типову поведінку об'єкта, утворюючи набір параметрів, які визначають типову поведінку об’єкта.

Профіль формується на основі аналізу статистичних даних суб'єкта, використовуючи звичайні математичні методи, такі як метод ковзного вікна та метод зваженої суми. У подальшому розглядатимемо статистичні методи виявлення вторгнень, атак і засоби боротьби зі зловмисниками [13].

1.4. Висновки до розділу

У розділі розглянуто стан захисту інформації підприємства, включаючи аналіз інформаційних, обчислювальних та керуючих мереж компанії. Основними компонентами є комп'ютерні та телекомунікаційні мережі, які можуть бути як дротовими, так і бездротовими різних типів. Важливою характеристикою є необхідність роботи всіх мереж в режимі реального часу, який може бути м'яким або жорстким залежно від потреб підприємства.

Проведений огляд принципів захисту корпоративних комп'ютерних мереж включає аналіз класифікації комп'ютерних атак та систем їх виявлення. Детальна класифікація є необхідною для ефективного захисту від потенційних кібератак, полегшуючи їх виявлення та подальшу боротьбу з ними. В наш час відомо велика кількість різних типів таксономічних ознак, що сприяє розвитку ефективних методів захисту.

РОЗДІЛ 2.ЗАХИСТ МЕРЕЖЕВОГО ПЕРИМЕТРА КОМП'ЮТЕРНИХ МЕРЕЖ КОМПАНІЇ

2.1. Основи побудови системи захисту периметра мережі

На рисунку 2.1 показано периметр мережі – це укріплена межа мережі, яка може включати:

- маршрутизатори;
- брандмауер;
- система виявлення вторгнень (IDS);
- пристрій віртуальної приватної мережі (VPN);
- програмне забезпечення;
- демілітаризована зона (DMZ) і захищені підмережі [2];

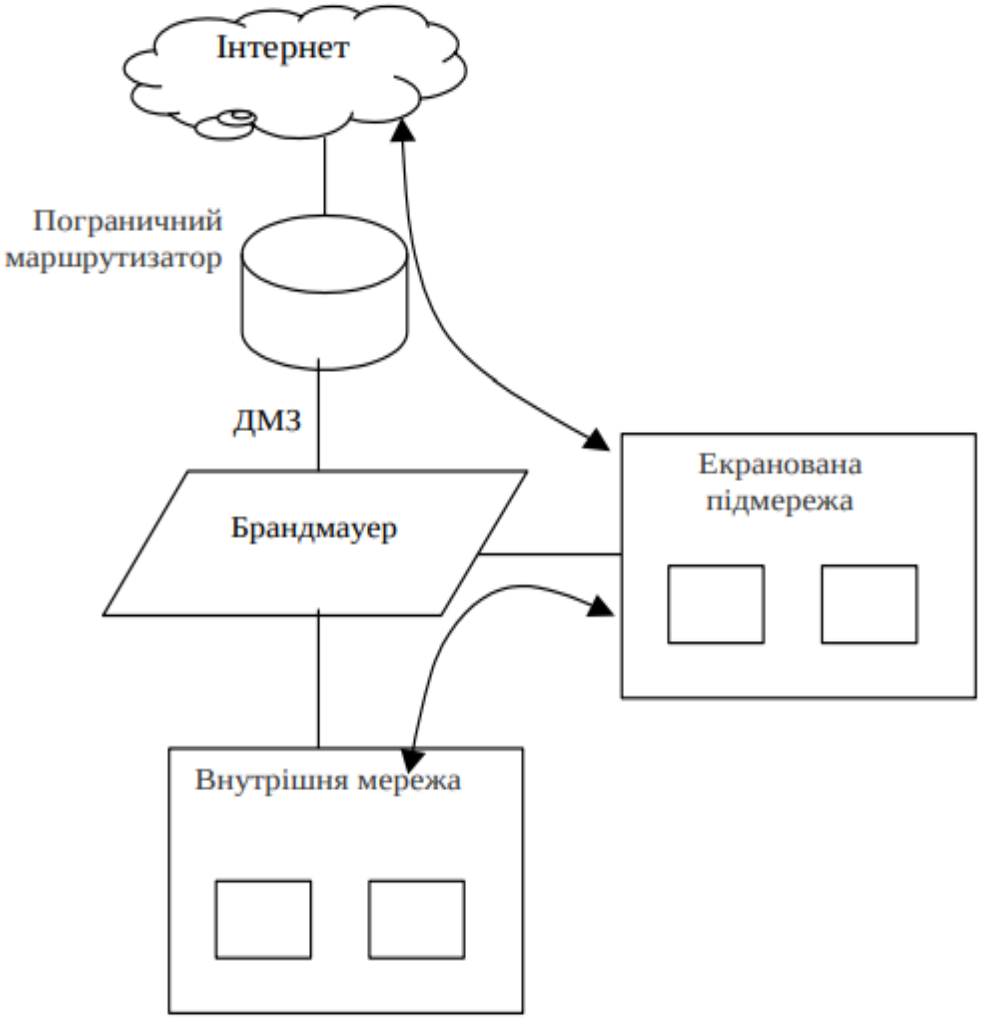

Рисунок 2.1 Компоненти захисту мережного периметра

Демілітаризована зона розташована перед брандмауером, броньована підмережа ізольована від внутрішньої мережі, але все ще потребує захисту, який може забезпечити брандмауер.

Маршрутизатор визначає трафік, що надходить.або виходить з мережі, а також внутрішній трафік, що циркулює в самій мережі, і керує ним. Маршрутизатори прикордонного шлюзу є останніми маршрутизаторами, які знаходяться під контролем безпосередньо перед доступом до Інтернету, і зазвичай діють як перша й остання лінія захисту мережі, фільтруючи вхідний і вихідний трафік.

Брандмауер — це пристрій, який аналізує трафік за допомогою набору правил, щоб визначити, чи можна.цей трафік пропускати через мережу. Сфера дії брандмауера починається там, де закінчується периферійний маршрутизатор, і він виконує глибшу перевірку пакетів під час фільтрації трафіку.

Існує декілька типів брандмауерів, зокрема статичні пакетні фільтри (для блокування доступу до підмереж можна використовувати, наприклад, вбудований статичний пакетний фільтр маршрутизатора Nortel Accellar), -fire Experts (для контролю авторизованих служб, таких як Cisco PIX) і проксі брандмауера (для контролю вмісту, наприклад Sidewinder Secure Computing). Хоча брандмауери не є ідеальними модулями, вони можуть блокувати або дозволяти все, що ви запитаєте.

IDS (Система виявлення вторгнень) — це оповіщення безпеки мережі, яке використовується для виявлення та звітування про всі вторгнення також про потенційно зловмисні. IDS може містити багато різних типів детекторів, розміщених у стратегічних точках мережі, які шукають заздалегідь визначені ознаки небажаних подій і можуть виконувати статистичний і аналітичний аналіз незвичайних подій.

У разі виявлення неочікуваних подій детектор IDS сповіщає адміністратора різними способами за допомогою електронної пошти, пейджінгу або розміщення запису в файлі журналу.

VPN — це безпечний сеанс, який застосовує незахищені канали, такі як

Інтернет, для своєї організації. Як правило, VPN відноситься до периферійного апаратного компонента, який підтримує шифрування сеансу.

Ділові партнери компанії, співробітники, які подорожують у справах або працюють з дому, можуть скористатися доступом до корпоративної мережі через VPN. Підключаючись безпосередньо до внутрішньої мережі компанії, VPN дозволяє віддаленим користувачам працювати там, як ніби вони знаходяться в офісі.

DMZ (демілітаризована зона) — незахищена територія між охоронними зонами. DMZ розміщується перед брандмауером, а захищена підмережа – за брандмауером.

Фільтрована підмережа — це ізольована мережа, підключена до призначеного інтерфейсу брандмауера або іншого пристрою фільтрації трафіку.

Відфільтровані підмережі часто використовуються для ізоляції хостів, до яких необхідно отримати доступ з Інтернету та використовуються лише внутрішніми користувачами даної організації.

Захищені підмережі зазвичай містять служби «загального користування», включаючи DNS, електронну пошту та Інтернет.

Брандмауер — це бар’єр, який захищає від спроб зловмисників, які проникають у мережу,.щоб скопіювати, змінити або видалити інформацію або скористатися пропускною здатністю, пам’яттю чи.потужністю обробки комп’ютерів у цій мережі. Брандмауери встановлюються на межі двох мереж - Інтернет і мережі LOM, тому їх ще називають міжмережевими моніторами. Він фільтрує всі вхідні та вихідні дані, передаючи лише авторизовані пакети.

Брандмауери дозволяє реалізувати політику безпеки, яка визначає авторизовані служби та типи доступу до них.

Він реалізує політики доступу до мережі, змушуючи всі мережеві підключення проходити.через брандмауер, де їх можна сканувати, дозволяти або забороняти як показано на рисунку 2.2.

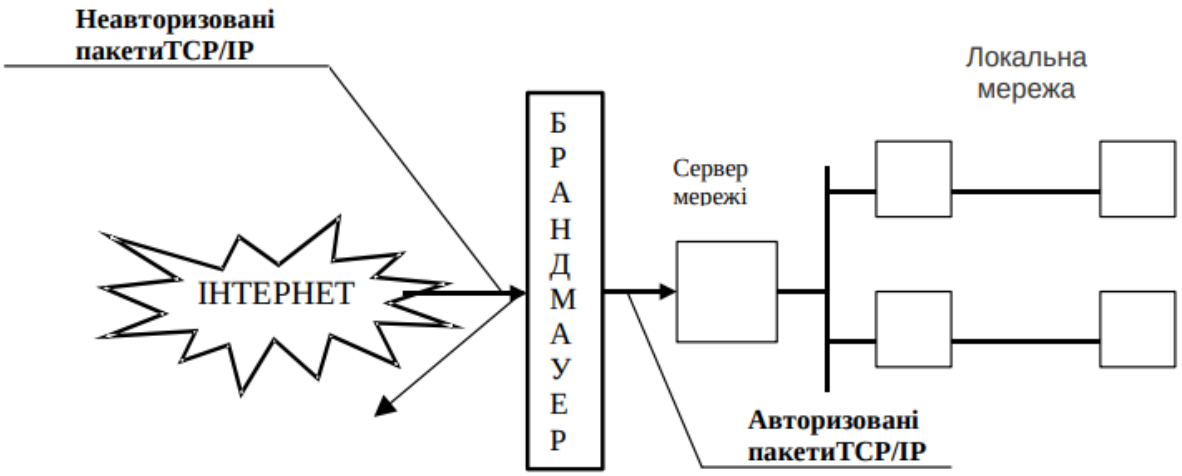

Рисунок 2.2 Умовна схема роботи та розміщення брандмауера

Функцію брандмауера можуть виконувати маршрутизатори, спеціалізовані комп'ютери, сервери або групи серверів, спеціально створені для захисту мережі або підмережі від несанкціонованого використання протоколів і служб машинного хоста поза цією підмережею.

Як правило, система брандмауера побудована на маршрутизаторах верхнього рівня, як правило, на маршрутизаторах, які підключають мережу до Інтернету, хоча вона може бути побудована на різних маршрутизаторах за для захисту лише однієї підмножини хостів або підмережі.

Сучасні брандмауери дуже відрізняються.як за рівнем захисту, так і за використовуваними методами захисту.

Однак більшість брандмауерів, що пропонуються як комерційні продукти, можна (хоча й дещо умовно) класифікувати за одним із трьох типів:

- брандмауер фільтрації пакетів;
- Брандмауер експертного рівня;
- Проксі брандмауер;

Брандмауер фільтрації пакетів – це програма маршрутизатора або сервера, налаштована на фільтрацію вхідних і вихідних пакетів.

Брандмауер пересилає або відкидає пакети на основі інформації в IP-заголовку пакета:

- адреса відправника;
- адреса одержувача;

- інформація про програму або протокол;
- номер вихідного порту;
- номер порту;
- порт одержувача.

Фільтрування пакетів є одним із найстаріших і найпоширеніших інструментів контролю доступу до мережі.

Ідея.фільтрації пакетів полягає в тому, щоб визначити, чи дозволено певному пакету входити в мережу або залишати її. Однак він не може розрізнити різні типи трафіку. Оскільки.фільтри пакетів не аналізують потоки трафіку так глибоко, як.інші технології брандмауера, вони працюють набагато швидше.

Брандмауер, що фільтрує пакети, перед тим, як надіслати пакет одержувачу, порівнює повний зв'язок із таблицею правил, за якими він має пересилати або відхиляти пакет. Брандмауер продовжує перевірку, доки не знайде правило, з яким погоджується вся асоціація пакетів.

Якщо брандмауер отримує пакет, який не відповідає жодному з правил у таблиці, він застосовує правило за замовчуванням, яке також має бути явно визначено в таблиці брандмауера.

З міркувань безпеки це правило зазвичай вказує на необхідність скинути всі пакети, які не відповідають жодному з інших правил. Фільтрування на основі адреси джерела стандартний список контролю доступу Однією з причин, чому технологія фільтрації пакетів продовжує використовуватися, є блокування або дозвіл трафіку на основі IP-адреси вихідної системи. Цей список не можна відфільтрувати за пунктом призначення чи номером порту.

Таким чином, стандартний список доступу є швидким.і йому слід віддавати перевагу, коли лише адреса джерела є критерієм фільтрації. Синтаксис.стандартного списку доступу такий список доступу Номер списку не може перевищувати діапазон 1-99.

Опція маски — це обов'язкова маска групового символу, яка повідомляє маршрутизатору, чи це один хост, який потрібно відфільтрувати, чи весь діапазон.

Можна додати опцію журналювання, щоб маршрутизатор спеціально реєстрував усі збіги цього фільтра. Один із методів уникнення виявлення плагіату полягає в тому, щоб переформулювати текст, зберігаючи його зміст та інформацію, але використовуючи власні слова та конструкції речень.

Загальне використання стандартних списків доступу зазвичай використовується для створення "чорного списку" конкретних хост-мереж, дозволяючи блокувати доступ до своєї мережі для конкретного сервера або всієї мережі. Тобто, ви маєте можливість обмежити доступ до вашої мережі від певних серверів або взагалі від усієї мережі.

Теоретично, ви також можете використовувати стандартні списки доступу для дозволу трафіку з конкретної IP-адреси, але це не рекомендується через можливу вразливість мережі перед атаками та скануванням адрес.

Крім того, стандартні списки доступу використовуються і для регулювання вихідного трафіку, тобто для пакетів, які виходять з вашої мережі і включають мережеву адресу в поле джерела.

Фільтрування за адресою призначення та портом - це розширена технологія фільтрації пакетів, яка дозволяє фільтрувати пакети на основі інформації з заголовка та номерів портів.

Ці приклади можна використовувати як спеціальні "канали", що дозволяють одній системі отримувати доступ до іншої системи (екстранет), дозволяють доступ до визначеної системи відкритого доступу (веб-сервер або DNS), або дозволяють певному типу трафіку входити в вашу мережу (пакет ICMP занадто широкий). Синтаксис.розширеного списку доступу такий список доступу.

Ключове слово protocol визначає протокол, який цікавить фільтр. Компоненти порту джерела або порту призначення визначають тип дозволеного або забороненого трафіку.

У кінець списку доступу можна додати багато параметрів, наприклад журнал (як зазначено в стандартному списку доступу або запис журналу, який також показує вхідний інтерфейс і MAC-адресу джерела) або набір ключових слів, перевірити індикатори визначені у вхідних пакетах.

Корисною функцією розширених списків доступу є фільтрація певних типів трафіку.

Додатковим рівнем захисту може бути блокування трафіку на списку портів, які використовуються звичайними троянськими програмами або програмами, які конфліктують із політикою використання Інтернету.

Ця фільтрація також може використовуватись, щоб дозволити або заборонити певні інформаційні повідомлення ICMP у мережі.

Найкращий спосіб заблокувати ICMP — це дозволити лише необхідний тип трафіку та заборонити всі інші . Використання пакетних фільтрів разом із їхніми перевагами,.також передбачає ряд недоліків. Якщо захист від підробленого та фрагментованого трафіку недостатньо ефективний, можливо уникнути фільтрів пакетів. Наприклад, статичний фільтр пакетів, який завжди відкритий, стає джерелом потенційної "уразливості". У разі використання технології, що не контролює поточний стан трафіку, може виникнути складність у впровадженні зворотного трафіку.

Для часткового вирішення цих проблем можна використовувати технологію динамічної фільтрації пакетів. Ідея полягає в тому, що фільтри активуються за необхідності та автоматично вимикаються при відключенні. Динамічні списки доступу є прикладом такої технології.

У зовнішньому інтерфейсі визначаються критерії для моніторингу певних типів підключень. Коли трафік повертається, його порівнюють з динамічним списком звернень, що формується негайно після виходу трафіку з мережі.

Відображення списків керування доступом покращує функціонал розширених іменованих списків керування доступом. Вони використовують ключові слова "відображати" та "оцінювати". Операція "відображення" дозволяє відновити динамічні ACL шляхом повернення пакета, що відповідає певному запису в ACL. Потім зворотній трафік оцінюється за допомогою цього динамічного ACL за ключовим словом "оцінювати".

Незважаючи на те, що дзеркальні списки не ідеальні, вони виявляються набагато більш ефективними в порівнянні з іншими фільтрами пакетів. Достатньо "скинути" один пакет, щоб повністю видалити рефлективно

згенерований ACL. Проте є проблема у тому, що ці списки не ураховують TCP-прапорці, тому вихідний трафік може виходити без будь-яких попереджень. Брандмауери з експертним рівнем захисту є найбільш розповсюдженими міжмережевими екранами [9]. Окрім фільтрації статичних пакетів, вони також відстежують з’єднання в таблиці стану, яка відображає поточний стан сеансу підключення. Трекер здоров'я подає дані у табличній формі, включаючи деталі IP-адрес джерела та призначення, прапори, номери послідовності та підтвердження тощо.

Кожен запис таблиці стану, створений при ініціації з'єднання, проходить через пристрій експертного керування, який порівнює інформацію пакета з інформацією таблиці стану, коли трафік повертається. Якщо пакет пов’язано з існуючим записом у таблиці, то йому дозволяється переміщуватися.

Витяг з таблиці станів маршрутизатора Cisco виконується за допомогою списку доступу до відображення, наприклад:

1) Дозволяється tcp від хоста xx.yy.zz.45 з портом 36204 до хоста 192.168.1.1 з портом smtp
   (10 відповідностей) (час залишку 295).
2) Дозволяється tcp від хоста xx.yy.zz.99 з портом www до хоста 192.168.1.1 з портом 2151
   (8 відповідностей) (час залишку 294)
3) Дозволяється tcp від хоста xx.yy.zz.247 з портом www до хоста 192.168.1.1 з портом 2149
   (10 відповідностей) (час залишку 294)
4) Дозволяється udp від хоста xx.yy.zz.34 з портом domain до хоста 192.168.1.1 з портом 2150 з журналуванням
   (3 відповідностей) (час залишку 293)
5) Дозволяється tcp від хоста xx.yy.zz.247 з портом www до хоста 192.168.1.1 з портом 2148
   (16 відповідностей) (час залишку 296)
6) Дозволяється udp від хоста xx.yy.zz.34 з портом domain до хоста 192.168.1.1 з портом 2146 з журналуванням

(3 відповідностей) (час залишку 292).

Всі динамічно створені списки доступу, що формуються вихідними з’єднаннями, надають функціональність, подібну до таблиці стану, відстежуючи інформацію про поточні сеанси зв’язку. Це дозволяє зворотньому трафіку успішно пройти через маршрутизатор. Кожен запис починається з ключового слова "License", а далі йде інформація про стан сесії, підтримку TCP та UDP, а також протокол відстеження адреси та порту призначення.

Забезпечення високого рівня безпеки для бізнес-мереж сучасності вимагає комплексного моніторингу та захисту. Один із методів - використання брандмауерів експертного рівня, які здатні блокувати невизначений трафік завдяки таблиці встановлених з'єднань.

База правил брандмауера визначає IP-адреси відправника та отримувача, а також номери портів для дозволу з'єднань. Виявлені аномалії відразу аналізуються для виявлення можливих загроз.

Існують два основних підходи до класифікації брандмауерів експертного рівня Expert Filtering і Expert Control. Експертна фільтрація використовується для оцінки статусу потоків пакетів на основі різноманітної інформації про транспортний рівень.

Засоби контролю експертного рівня відстежують інформацію рівня 4 і забезпечують захист від нестандартних потоків трафіку TCP/IP. Експертне тестування, незважаючи на вищу продуктивність порівняно з брандмауерами проксі, надає безпечніше середовище, оскільки аналізує всі аспекти зв’язку на рівні програми.

Хоча брандмауери експертного рівня можуть забезпечити високий рівень захисту, важливо розуміти, що абсолютна безпека завжди залишається недосяжною метою.

Проксі-брандмауери представляють собою альтернативу або комбінацію брандмауерів експертного рівня, використовуючи складні та нешироко поширені технології. Вони здійснюють функції професійних брандмауерів, блокуючи невстановлені та неавторизовані з'єднання.

База правил проксі-брандмауера порівнює IP-адреси джерела та

призначення, а також кількість портів, що дозволяють підключення. Це забезпечує високий рівень безпеки, оскільки внутрішні та зовнішні сервери не підключаються безпосередньо, а брандмауер діє як посередник.

Брандмауер проксі перевіряє кожен пакет, щоб переконатися, що він відповідає протоколу, вказаному в номері порту призначення. Це дозволяє побудувати ефективну систему захисту, зменшуючи ризик входу та виходу зловмисного трафіку.

Переваги проксі-брандмауерів включають захист внутрішніх IP-адрес від зовнішнього доступу, можливість відстеження порушень політик безпеки за допомогою журналів аудиту, та включення захисту на основі користувачів.

Проксі-сервіси надійно захищають від несанкціонованого використання користувачами та підтримують надійну автентифікацію. Завдяки керуванню з'єднаннями на рівні служб, брандмауери проксі-сервера не піддаються IP-спуфінгу.

Основні переваги включають кращі можливості журналювання порівняно з іншими типами брандмауерів, а також забезпечують єдину точку перевірки та керування для мережі.

Кілька додаткових особливостей включають можливість блокування підключення користувача до проксі-сервера, відсутність облікового запису на сервері bastion, роботу проксі-сервісів від імені користувачів та надання централізованої точки для мережі, що дозволяє детально моніторити трафік.

Існує потенціал перевантаження мережевого трафіку внаслідок застосування внутрішньої мережевої топології, захищеної брандмауером проксі та прихованої від публічного доступу. Деякі проксі надають розширені можливості контролю трафіку за допомогою інструментів моніторингу.

Брандмауер проксі-сервера забезпечує надійну автентифікацію та журналювання. Трафік програм можна попередньо автентифікувати перед його досягненням внутрішніх серверів, що забезпечує ефективніше журналювання, порівняно зі стандартним серверним журналюванням. Правила фільтрації брандмауера проксі-сервера менш складні, ніж у брандмауера фільтрації пакетів.

Хоча брандмауери проксі-серверів мають вищий рівень безпеки порівняно з брандмауерами фільтрації пакетів, вони також мають кілька недоліків, таких як зниження продуктивності через додаткову обробку, потрібну для обслуговування програм.

Проксі-сервери програм працюють повільніше, ніж фільтри пакетів, і вимагають розробки нових проксі для кожної нової програми або протоколу. Поміж внутрішніх проблем можуть виникнути проблеми з операційними системами та їх компонентами, що можуть впливати на безпеку сервера брандмауера.

Проксі-сервіси також можуть бути чутливими до помилок операційних систем та помилок програмного рівня, а операційна система сервера, що містить проксі, може залишатися вразливою до зовнішніх загроз. Крім того, параметри проксі-сервера можуть бути складними для налаштування для кожної програми, яка використовує певний порт.

З урахуванням можливості проксі-сервера стати вузьким місцем у мережі та єдиною точкою збою, важливо також враховувати роль маршрутизаторів у забезпеченні безпеки мережі. Маршрутизатор фільтрує вхідний та вихідний трафік, захищає від атак на відмову в обслуговуванні і може використовуватися як крайовий брандмауер, використовуючи технології, такі як контекстний контроль доступу, мережева трансляція адрес та списки контролю доступу.

В розділі про принципи віртуальних приватних мереж і тунелювання, а також системи виявлення вторгнень розглянуто основні концепції. Отже, в аналізі основних компонентів захисту периметра мережі приходимо до висновку, що для ефективного захисту мережі необхідно використовувати комплексний багаторівневий підхід, розташовуючи компоненти захисту на різних рівнях для максимізації їхньої ефективності.

2.2. Розподілені системи виявлення вторгнень

Система виявлення вторгнень (IDS) відстежує мережевий трафік або маніпуляції з файлами хоста, щоб виявити незвичну поведінку або неналежне

використання.

IDS.веде журнал вторгнень, надсилає сповіщення в реальному часі та в деяких випадках може запобігти атаці. Основними компонентами IDS є мережеві датчики [3].

Датчики служать основним мостом IDS до обчислювального середовища. Вони збирають інформацію, необхідну для виявлення вторгнень, фільтрують їх і передають детекторам.

На наступному кроці зібрані події безпеки аналізуються, в них виявляються вторгнення та генеруються звіти про підозрілу активність. Існує два типи датчиків мережеві та серверні. Мережеві датчики збирають події безпеки з мережевого трафіку та передають їх у підсистему виявлення.

Серверні датчики попередньо фільтрують потік подій у системі. Одночасно відстежуйте системну активність (використання ресурсів, виконання, підключення тощо), аналізуйте протоколи та використовувані системні/службові файли та структури.

У зв’язку з прямим контактом із захищеною системою датчикам часто доручають виконувати контрзаходи (закривати з’єднання, зупиняти процеси, змінювати налаштування мережевих пристроїв тощо).

Виявлення атак виконується детектором відповідно до заданих критеріїв виявлення (сигнатур, шаблонів, правил). Атаки різняться за складністю ідентифікації деякі можна легко виявити за допомогою сигнатур, а для інших потрібні статистичні методи виявлення [4].

У цьому відношенні сучасні IDS мають декілька механізмів виявлення.пошук за сигнатурою, пошук за регулярними виразами та статистичні механізми виявлення вторгнень. Однак, на жаль, системи виявлення вторгнень, розроблені для виявлення та відбиття хакерських атак, можуть піддаватися несанкціонованому втручанню, яке порушує продуктивність цієї системи, спричиняючи те, що система не може виконати призначене завдання.

У загальному випадку датчик системи виявлення атак – це підсистема, яка отримує доступ до.джерела інформації, яким може бути мережевий трафік,

журнали записів або системні визови.

Далі данні передаються до механізму попередньої фільтрації, щоб відфільтрувати те, що датчик не може проаналізувати.

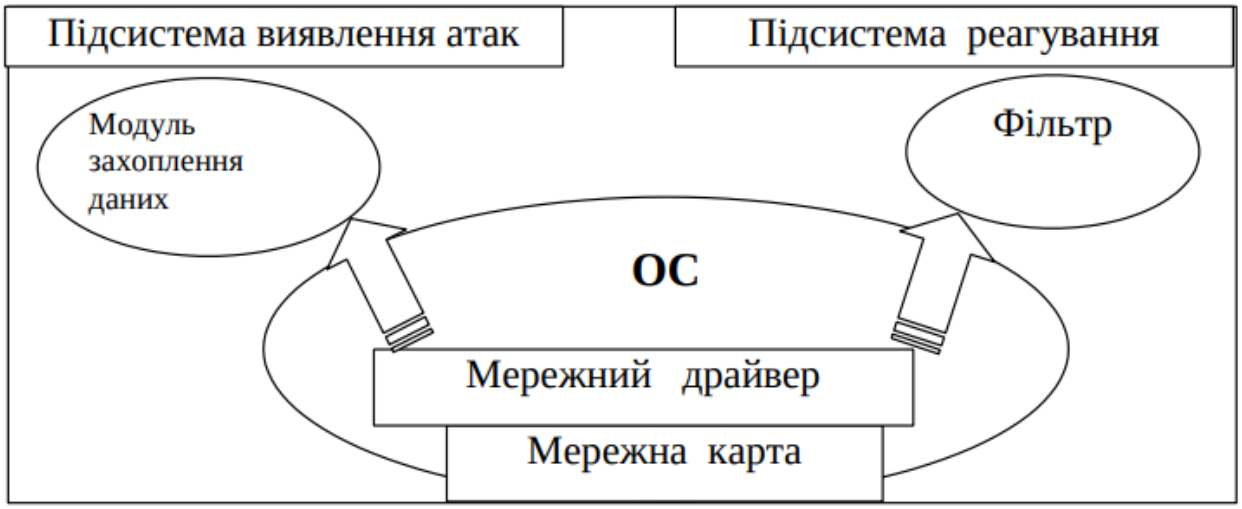

Рисунок 2.3 Схема атак на сенсори

Подивимось можливі варіанти атак на сенсори, починаючи з їх ієрархічного рівня які приведені на рисунку 2.3:

- Мережева плата використовується з двома цілями для перехоплення мережевого трафіку з метою пошуку слідів атак (якщо вони не позначені спеціальними тегами виявлення атак, встановленими в кадрі комутатора або маршрутизатора), і також для передачі на ПК. Враховуючи різні можливості блокування управління мережевими картами (RMON, DMI, ACPI, Wf та ін.), можна припустити, що атаки на мережеві карти цілком можливі.
- Мережевий драйвер – наприклад, на цьому рівні погана реалізація мережевого стеку дозволяє пакетам, сформованим певним чином, надсилатися на датчик, що призводить до «синього екрану».
- Операційна система. – наявність вразливостей в сучасних операційних системах призводить до того, що атак на IDS набагато більше, ніж насправді.
- Модуль імпорту даних. – якщо він працює з мережевими пакетами, достатньо надіслати йому нестандартні пакети (тобто ті, що не

відповідають RFC) або створити великий обсяг трафіку, який датчик не зможе обробити.

Якщо він працює з журналом подій, ви можете переповнити цей журнал, і старі події будуть заміщені новими подіями.

Підсистема виявлення атак включає в себе «сигнатурний» IDS який має серйозне обмеження змініть один байт у коді атаки, і він більше не буде виявлений.

Основні варіанти реагування повідомлення для керування платою, створення SNMP або електронної пошти, відключення засоби захисту, призначені для забезпечення безпеки мережі, також можуть служити інструментами в руках досвідченого зловмисника.

Наприклад, якщо датчик відключений від вузла атаки, можна використовувати адресу компонента IDS як адресу відправника для атаки. IDS таким чином може стати інструментом для здійснення атаки типу DoS. Ще одним способом атаки на систему виявлення вторгнень є вплив на механізм автентифікації. Вилучення ключа автентифікації з компонента IDS призведе до припинення процесу автентифікації і заборонить обмін інформацією між компонентами. Якщо автентифікація взагалі не використовується між компонентами, зловмисник може створити фальшивий датчик або панель керування для обману системи та відправки користувачеві невірних команд.

З метою покращення захисту датчиків системи виявлення вторгнень у мережі рекомендується створити окрему мережу керування. Ця мережа буде використовуватись виключно для зв’язку між датчиками системи виявлення вторгнень, централізованим блоком збору даних і панелями аналітики приведено на рисунку 2.4.

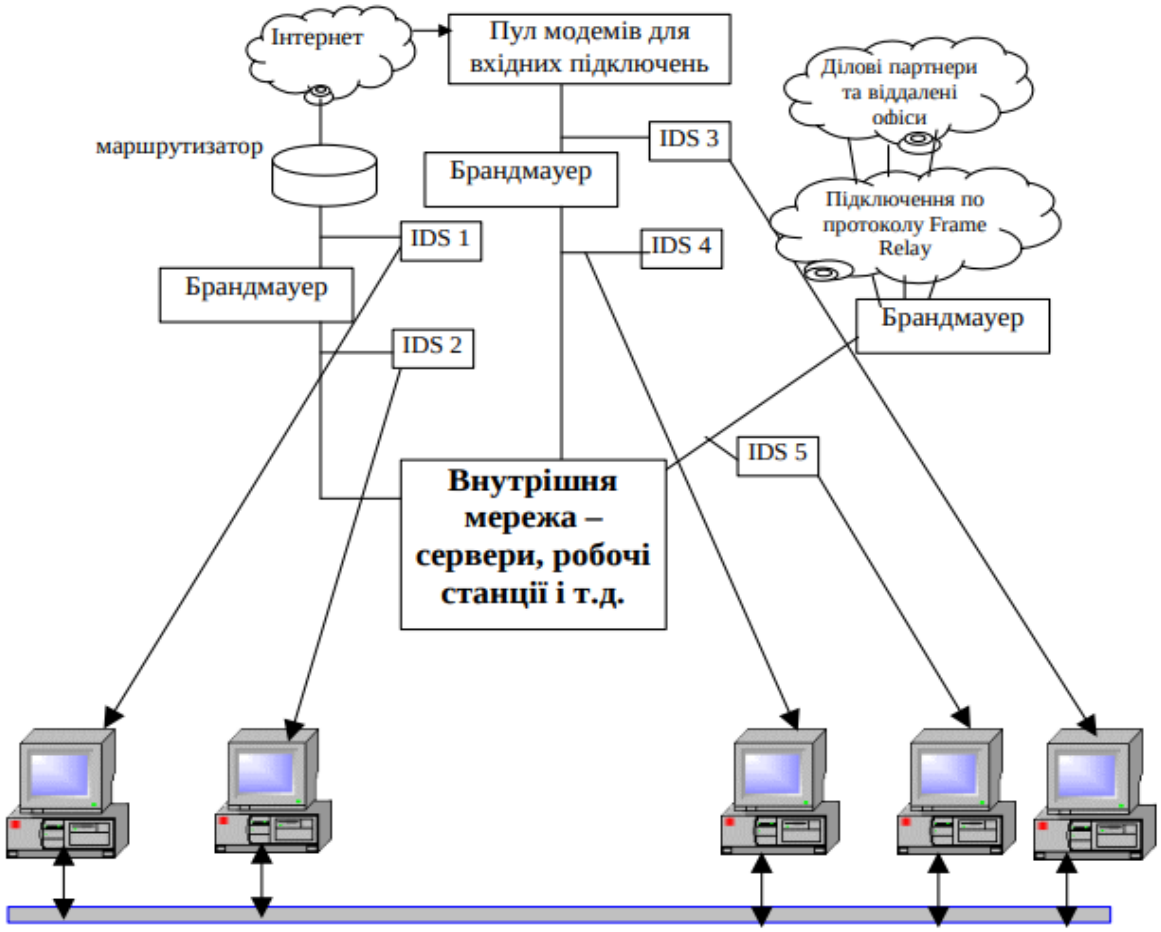

Рисунок. 2.4. Схема мережі управління системою виявлення вторгнень

Тут кожен мережевий датчик у системі виявлення вторгнень має принаймні дві мережеві інформаційні карти.

Одна або кілька з цих інтерфейсних карт лише призначені для моніторингу трафіку у перевіряних мережах і не передають пакети. Замість цього, інша мережева інтерфейсна карта повністю підключена до окремої мережі управління, яка використовується виключно для передачі даних до системи виявлення вторгнень та зміни конфігурацій. Ця архітектура ускладнює для зловмисника пошук і ідентифікацію датчика системи виявлення вторгнень, бо він не відповідає на запити до мережевої інформаційної карти, яка ним керує.

Оскільки мережева інтерфейсна карта знаходиться в ізольованій мережі, зловмисники не матимуть доступу до неї. Деякі теги моніторингу мережевої інформації є чистими інструментами аналізу мережевих пакетів.не використовують IP-адреси. Якщо датчик системи виявлення вторгнень використовує IP-адресу, і зловмисник знає цю адресу, він може завчасно

атакувати цю адресу, щоб спричинити стан відмови в обслуговуванні (DoS), коли датчик не бачить атаку.

Крім того, зловмисник може приховати або ввести в оману трафік, що надходить від датчика, використовуючи інший метод. Побудова окремої мережі керування має й інші переваги.

Він ізолює контрольний трафік, щоб ніхто інший, хто.контролює мережу,.не міг бачити дані датчика.

Це також заважає датчикам контролювати.власний трафік.

Приватні мережі — хороший спосіб уникнути майбутніх проблем під час передачі даних датчиків через брандмауери та незашифровані загальнодоступні мережі. Важливо підвищити безпеку датчиків у системах виявлення вторгнень, щоб мінімізувати ризик компрометації.

Якщо зловмисник бере під контроль систему виявлення вторгнень, він може вимкнути або переналаштувати її так, щоб вона не записувала їх і не сповіщала їх. Зловмисники також можуть використовувати систему виявлення вторгнень для атаки на інші вузли в мережі.

Підтримка високого рівня безпеки датчиків є важливою для створення надійної та корисної системи виявлення вторгнень.

2.3 Проактивна система захисту інформації в комп'ютерній мережі

Архітектура розподілених проактивних систем. Проактивні служби в основному зосереджені не на усуненні, а на запобіганні збоїв і являють собою набір стратегічних заходів, які мають забезпечити ефективну роботу мережі і відсутність перебоїв, враховуючи політику безпеки.

Активні системи базуються на семи фундаментальних принципах такі як[21]:

- зв'язок із фізичним світом;
- «глибинних» мережевих взаємодій;
- обробка макросів;
- робота в умовах невизначеності;
- форсайт;

- замкнутий контур керування;

Орієнтація на системи, в яких люди не виконують функції управління, або на повністю автоматизовані системи – загальна мета проактивних IT-систем для організації безпеки.інформаційних ресурсів компанії.

Таким чином, загрози конфіденційності, цілісності та доступності інтерфейсів, протоколів і послуг є найпоширенішим і поширеним типом загроз систем безпеки.

Розроблений захист може базуватися саме на цьому не конкретно, а в загальних рисах.

Для такої системи, які б конкретні атаки не були організовані проти телекомунікаційної системи - вони не.будуть ефективними заздалегідь.

Кожен протокол має свої особливості, але в контексті конфіденційності, цілісності і доступності для інтерфейсів, протоколів і послуг, ці три аспекти відіграють важливу роль усіх випадках він повинен забезпечувати взаємодію принаймні двох.об’єктів це його концептуальна вдмінність від алгоритму – ланцюжок операцій.

Явна взаємодія призводить до виконання «поставленого завдання» з достатньо великої кількості подібних, але невзаємодіючих завдань.

Отже, для всіх протоколів їх мета – це узагальнення забезпечення взаємодії, а агент безпеки в даному випадку відповідає за конфіденційність, цілісність і доступність цієї взаємодії.

Існує також кілька інтерфейсів, які представляють правила доступу до служби. Тому спільним для них буде забезпечення конфіденційності, цілісності та доступності правил доступу до послуг.

Основна функція всіх сервісів — надати комусь певні ресурси (зокрема можливості).

Безпека – це захист ресурсів від несанкціонованого доступу та/або використання, зміни чи пошкодження/знищення.

В якості основи для підсистеми безпеки слід вибрати агентську технологію. Кожен агент діятиме, враховуючи реальну ситуацію в зоні його/її відповідальності (фоновий моніторинг).

У той же час він розумний, здатний працювати незалежно від інших агентів, незважаючи на підключення до них - якщо буде допущено порушення безпеки,.воно буде негайно усунено агентом безпеки.

Миттєво без необхідності зв'язуватися з іншими агентами або з диспетчерським центром (повне підключення служб безпеки). Під агентом тут розуміється суб’єкт, який здатний формувати цілі, навчатися, планувати та приймати рішення в середовищі, що динамічно змінюється.

Метою агентів є спрощення та покращення взаємодії користувача зі складними програмними системами в слабко структурованих розподілених середовищах, що динамічно змінюються, шляхом адаптації до змінних характеристик, специфічних для конкретного користувача.

Агент відрізняється від традиційних програм тим, що він може взаємодіяти з середовищем, отримуючи інформацію через датчики і впливаючи на середовище через агентів, які його викликають. Крім того, він може змінювати свою поведінку, навчаючись на основі власного досвіду.

Розглянемо особливості побудови запропонованої системи безпеки. Деякі компоненти цієї системи вже існують.

Це демонструють приклади систем безпеки, наведені в першій частині розділу. Крім того, активно захищені системи використовуються, наприклад, у банківській сфері - для банківських переказів через універсальні телекомунікаційні мережі (Інтернет).

Система має бути розподіленою, тобто реалізація інформаційних технологій базується на розподілі інформаційних ресурсів. Розподілені обчислювальні системи включають дані, засоби обробки та операційні компоненти.

Інформаційними ресурсами розподіленої комп'ютерної системи є оброблені дані, програмне забезпечення та інфраструктура обчислювальних ресурсів компоненти апаратного забезпечення та інформація про користувачів і різних агентів, включаючи агентів безпеки, які необхідно включити.

Політика безпеки визначає набір правил, які регулюють обробку інформації, взаємодію підсистем і забезпечують захист в розподіленій

комп'ютерній системі та її архітектурі безпеки. У контексті розподіленої природи IT-систем відбувається збільшення вразливості інформаційних ресурсів і поширення багатьох загроз безпеці. З точки зору акторського підходу, загрози безпеці також слід розглядати як акторів або мультиагентні системи (з розподіленими загрозами), ігноруючи дестабілізуючі фактори різної природи (апаратне забезпечення, програмне забезпечення, користувачі тощо).

Безпека розподілених обчислювальних систем – це стан мультиагентного інформаційного.середовища, в якому під впливом дестабілізуючих факторів (загроз безпеці) виконується обробка даних, взаємодія та захист між агентами (самозахист) гарантований.

Захист є незамінною внутрішньою властивістю ROS.

Система складається з компонентів (інтелектуальних підсистем), які реалізують загальну політику безпеки наведеному на рисунку 2.5.

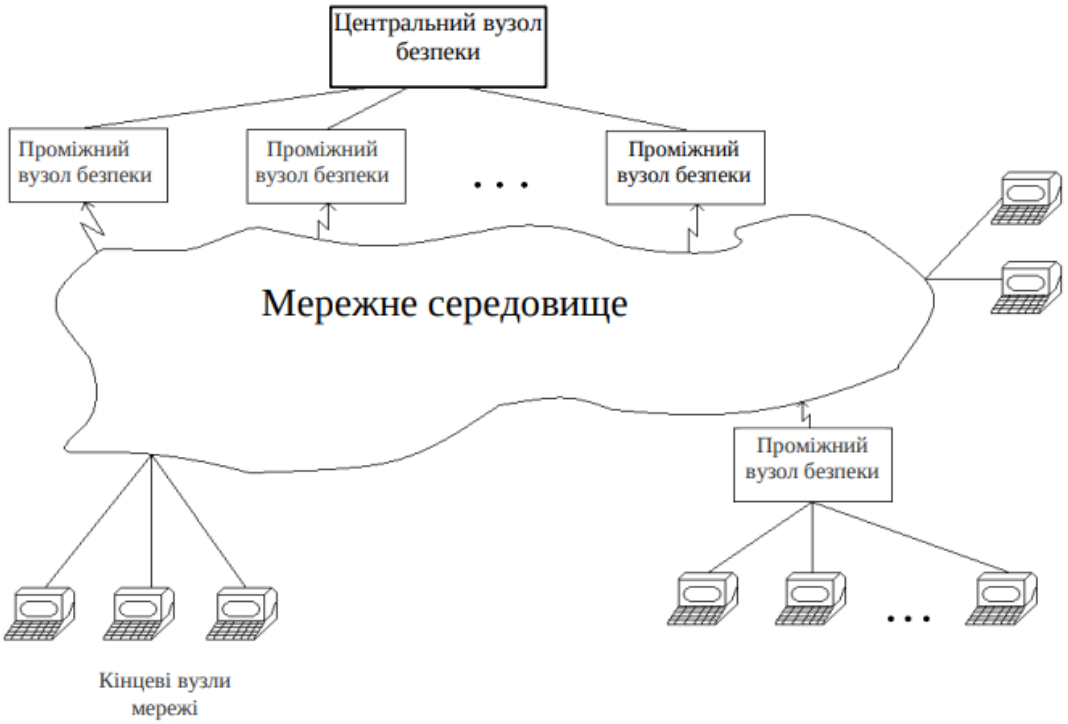

Рис 2.5. Представлення структури підсистеми захисту розподіленої обчислювальної системи

Запропонована архітектура самоподібних систем є інноваційним рішенням

у галузі інформаційних технологій і може вирішувати проблеми балансування ресурсів між функціональними завданнями системи та завданнями забезпечення безпечного виконання.

У той час самоподібність значно спростить і покращить управління складними і погано структурованими системами, одночасно мінімізуючи трафік, необхідний для безпеки[13].

2.4. Висновок до розділу

Розглянуті та проаналізовані основні принципи захисту периметра мережі компанії, базові аспекти побудови системи захисту мережевого периметра. Також розглянуто аналіз динамічної фільтрації пакетів і рефлексивні списки доступу. Багато проблем, що виникають при статичній фільтрації пакетів, можна частково вирішити використовуючи технологію динамічної фільтрації пакетів. Суть цієї технології полягає в тому, що фільтри призначені для роботи «на льоту», коли це необхідно, і припиняють працювати після відключення.

Списки доступу до відображення є прикладом технології динамічної фільтрації пакетів.

У зовнішньому інтерфейсі визначається критерій, на основі якого здійснюється моніторинг певних типів підключень. Якщо трафік повертається, він порівнюється з динамічно створеним списком звернень негайно після того, як покидає мережу. Це частина розподіленої системи виявлення вторгнень.

Система виявлення вторгнень (IDS) моніторить мережевий трафік або маніпуляції з файлами хоста для виявлення незвичної поведінки або недоречного використання. IDS ведуть журнал вторгнень, надсилають сповіщення в реальному часі та в деяких випадках можуть запобігти атакам. Система проактивно захищає інформацію в комп'ютерних мережах.

Архітектура розподіленої проактивної системи орієнтується на запобігання інцидентам, а не лише на їх усунення. Проактивні сервіси представляють собою комплекс стратегічних заходів, спрямованих на забезпечення оптимальної та безперебійної роботи мережі відповідно до політики безпеки.

РОЗДІЛ 3. ЗАХИСТ КОМП'ЮТЕРНОЇ МЕРЕЖІ ВІД РОЗПОДІЛЕНИХ АТАК

Одним із методів, який зазвичай використовують зловмисне програмне забезпечення конфіденційності цільової системи є атака з впровадженням коду на хост.

Це дозволяє зловмисному програмному забезпеченню виконання свого коду у зовнішньому просторі процесу, дозволяючи йому працювати непомітно та отримувати доступ до важливої інформації з інших процесів. Оскільки існує багато різних методів введення та виконання коду у зовнішньому просторі обробки, потрібен загальний підхід, щоб охопити всі можливості.

Підходів, які зосереджені лише на низькорівневих деталей операційної системи (таких як використання API) недостатньо, оскільки набір підозрілих API постійно розширюється. Тому підходи, які зосереджуються на низькорівневих елементах операційної системи, зазвичай, пропускають нові атаки. Крім того, такі підходи обмежуються глибоким знанням.операційної системи.

Оцінюючи результати аналізу багатьох статей, монографій, документів наукових конференцій, завдання захисту інформаційних ресурсів комп'ютерних мереж від атак, як ззовні, так і зсередини, завжди залишатимуться актуальними.

На даний момент опубліковано список тисяч загроз і вразливостей інформаційно-комунікаційних систем. Один з найбільш детальних описів цього типу представлений у відкритому стандарті Європейського Союзу — Basic IT Protection Manual [8], який налічує понад чотири тисячі сторінок.

Проте створення безпеки даних — це не просто систематизація, виявлення та відображення загроз, а головне — це управління ризиками та своєчасне впровадження превентивних заходів для зменшення ризиків загроз через щоденну роботу над безпекою системи [2].

Для вирішення цієї проблеми недостатньо виявлення та реагування на дії порушників.

Треба не тільки передбачити такі дії, усунути вразливості в системі захисту

мережі, а й відвернути увагу зловмисника від вузлів мережі, де зберігаються та обробляються інформаційні ресурси.

Більше десяти років тому було зрозуміло, що безпосереднє протистояння шкідливому впливу Інтернету практично марне.

Зроблено обґрунтований висновок про необхідність застосування методів, що базуються на системному аналізі, оперативних дослідженнях у військовій справі, а також у радіоелектронній боротьбі, радіоелектроніці та радіорозвідці, радіоелектронній протидії, дезінформації та інших аспектах.

Новим підходом для виявлення атак із впровадженням коду на хост є Bee Master [9].

Він застосовує модель honeypot до процесів комп'ютерної системи і тому не покладається на деталі низького рівня.

Основна ідея полягає у виявленні класичних процесорів комп'ютерних систем, які стають жертвами шкідливих програм.

Цей підхід акцентує увагу на концепціях, таких як потоки або сторінки пам'яті, які присутні в кожній сучасній операційній системі. Це дозволяє Bee Master уникнути недоліків, характерних для низькорівневих комп'ютерних систем. Крім того, він забезпечує незалежну відслідковуваність атак із впровадженням коду на хост. Щоб перевірити можливості цього підходу, ми провели якісне та кількісне оцінювання Bee Master у Microsoft Windows і Linux.

Результати показують, що він забезпечує надійне та надійне виявлення багатьох існуючих сімейств шкідливих програм.

Метою даної кваліфікаційної роботи є дослідження методу управління процесом захисту інформаційної системи на основі теорії конфлікту та керованих процесів Маркова.

На основі цього досвіду побудуйте модель алгоритму і вивчіть динаміку боротьби зі зловмисниками за допомогою медових пасток і Bee Master. Конфлікт не можна вважати проблемою оптимізації.

Коли ресурси сторін рівні, «оптимальний» означає, що конфлікт закінчується, а коли ресурси нерівні, слабша сторона зазнає поразки з ймовірністю один.

У той же час вигравати конфлікти можна меншими силами. Однак, щоб отримати вигоду з ймовірністю, більшою за друге найменше значення порядку, необхідно мати ресурси того ж порядку, що й ресурси зловмисника. Конфлікт з раціональним опонентом неможливо вирішити в рамках теорії адаптації. Завдяки його активним діям ворог по відношенню до одного з них, ймовірно, отримає максимальне перевагу. Тому ми, пристосовуючись до подальшого погіршення умов, опинимося у найнесприятливішій ситуації.

Отже, ключовими завданнями, які потрібно вирішити для досягнення поставленої мети, є:

- аналіз можливих стратегій у конфлікті та вибір найбільш перспективних для цього завдання.
- вибір математичного інструменту для опису процесів розвитку конфлікту.
- розробка математичної моделі конфліктів для досягнення асимптотичних оцінок ефективності.

3.1 Технологія " Honeypot "

Технологія Honeypot.є одним із найефективніших і доступних способів виявлення та захисту від атак на мережеві ресурси.

Приваблива та доступна для зловмисника мішень, розташована всередині мережі, що не відрізняється від реальних ресурсів зовні, єдина мета якої – привернути увагу зловмисника, спровокувати його.

Здійснюємо протиправні дії та повідомляємо про вторгнення особу, відповідальну за комп’ютерну безпеку.

Іншими словами, honeypot - це система, яка симулює роботу реальної системи, призначеної для потенційних атак та несанкціонованого доступу. Honeypot привертає увагу і ресурси зловмисника, фіксує кожну його дію і повідомляє службу безпеки про інцидент. При цьому, залежно від типу honeypot,.можуть бути імітовані всі системи, які є потенційними об’єктами атаки сервери, бази даних, мережеві служби, файлові ресурси тощо. Переваги

honeypot систем визначаються.принципом їх роботи.

По-перше, практично відсутні помилкові спрацювання. Оскільки honeypot лише симулює реальну систему і не доступний жодному реальному користувачеві мережі чи законній мережевій програмі, будь-яка діяльність у honeypot і будь-які спроби отримати доступ до системи не є авторизованими та представляють собою атаку або мережевий зонд, спрямований на пошук уразливості на його захист.

Визначення реальності атаки є найважливішим моментом для адміністраторів, оскільки це дозволяє їм швидко вжити контрзаходів.

Але крім того, Honeypot також дозволяє отримати необхідну інформацію для вивчення дій порушників. Суть у тому, що Honeypot дозволяє зберегти слід удару для подальшого дослідження. Зламану систему honeypot можна безпечно вимкнути та направити для аналізу внутрішнім або зовнішнім експертам з інформаційної безпеки, що зазвичай неможливо на реальному сервері, такому як сервер бази даних для бізнес-додатків або поштовий сервер.

За слідами, залишеними агресором, можна дізнатися про.методи та засоби нападу, які він застосовував, і зробити висновки про його цілі.

У той же час, важливою особливістю системи honeypot є відносно невеликий обсяг інформації, який необхідно вивчити під час розслідування інциденту.

Реальні мережеві системи записують величезну кількість інформації,.і дослідження інцидентів IS на основі журналів кількох програм і мережевих систем є досить трудомістким завданням. На відміну від цього, honeypot містить лише необхідну інформацію, пов’язану з фактичним порушенням, оскільки там не вживаються судові дії.

3.2 Місце Honeypot в системі безпеки підприємства

Honeypot є високоефективним і доступним методом виявлення вторгнень і.раннього попередження.

Виходячи з усього вищезазначеного, можна виділити два ключових

напрямки застосування цієї технології. По-перше, це зменшення ризику кібератак на реальні системи. Технологія Honeypot дозволяє сповіщати, виявляти та записувати дії порушників.

Правильно встановлений і.налаштований honeypot відволікає увагу та ресурси зловмисника від реальної системи, дозволяючи виявити спробу проникнення, надавши інформацію для її аналізу та, можливо, додатковий час для реалізації відповідних захисних заходів. Другий напрямок полягає у зборі інформації для дослідження поведінки, методів та інструментів злочинців. Дослідження систем honeypot не зменшує бізнес-ризики, але отриману з його допомогою інформацію можна використовувати для створення більш ефективних надійних систем захисту реальних програм і мереж від потенційних загроз.

На рисунку 3.1 приведена.найпростіша схема Honeypot. Щоб не мати ключових характеристик honeypot, вузол повинен обслуговувати зовнішній трафік, який має конфігурацію, відмінну від стандартної і використовується іншими учасниками мережі на законних підставах і т.д.

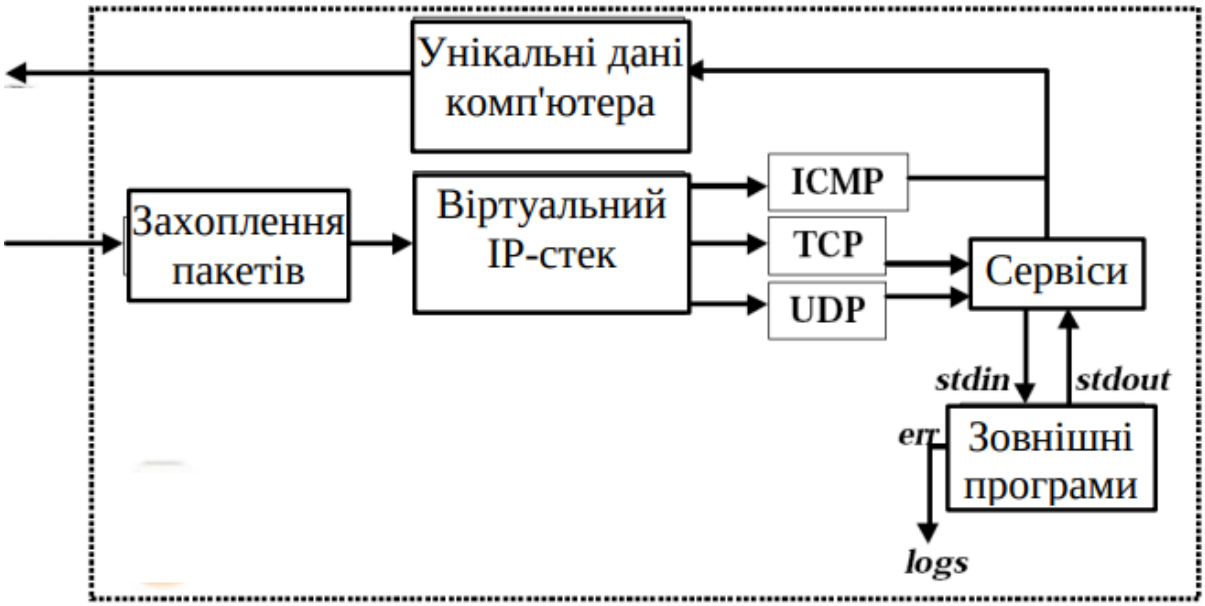

Рисунок 3.1 – Найпростіша схема Honeypot

Приманки можуть існувати як реальні, так і віртуальні. Реальною приманкою є використання виробничого програмного забезпечення на спеціалізованому обладнанні. Справжня наживка є однією з найкращих мет

цілей, яку ви можете запропонувати злодієві. Він виглядає і поводиться як справжній виробничий ресурс, і якщо дані в ньому оновлюються, важко вгадати хакеру, що перед ним приманка. Однак недоліком справжньої приманки є те, що її організація та управління часто вимагають багато зусиль і часу. Інколи встановлення фактичної наживки може зайняти стільки ж часу, скільки й встановлення фактичних виробничих активів. Ще одним серйозним недоліком є складність запобігти нападу зловмисника, який нажився, на інші виробничі ресурси. Багато продуктів UNIX/Linux фактично використовують механізми запобігання викраденню виробничих ресурсів (іноді їх називають механізмами контролю даних), але лише деякі продукти Windows мають такі функції.

Віртуальна приманка – це змодельоване середовище, у якому програмне забезпечення.обмежує можливості зловмисника. Як правило, потенційна шкода для продуктивних ресурсів значно зменшується або навіть повністю усувається. Більшість віртуальних приманок можуть імітувати відкриті порти, закриті порти або порти з відповідями служби.

Віртуальний декодер, який лише відкриває порт і записує початковий запит зловмисника, називається простим слухачем портів. Досконаліші прослуховувачі портів можуть відповідати на прості пакети відкриття або закриття, що робить їх більш реалістичними та привабливими для хакерів. Ці приманки записують інформацію, надіслану хакером, і взаємодіють відповідно до мережевого протоколу, наприклад, надсилають SYN-пакети.

Порівняння систем Honeypod та IDS/IPS:

1. Honeypod
    1.1 Функції Honeypod
        1.1.1 Імітація системи Honeypod імітує справжні мережні ресурси, що привертає увагу зловмисників і дозволяє виявляти їхні методи та наміри.
        1.1.2 Збір інформації Збирає дані про атаки, що допомагає аналізувати їх для покращення загального захисту мережі.
        1.1.3 Неперервний моніторинг Постійно активний для виявлення навіть нових типів загроз.

1.2 Переваги:

1.2.1 Ефективний проти навіть нових та неочікуваних загроз.

1.2.2 Дозволяє зосередитися на виявленні зловмисників, що вже проникли в мережу.

1.2.3 Надає детальні дані для аналізу і покращення стратегій безпеки.

1.3 Обмеження:

1.3.1 Не виявляє атак, які не спрямовані на нього.

1.3.2 Може займати ресурси на підтримку імітації.

2. IDS/IPS (Системи виявлення та запобігання вторгнень):

2.1 Функції IDS:

2.1.1 Виявлення загроз моніторить мережу на предмет аномальних або підозрілих активностей.

2.1.2 Сповіщення про інциденти попереджає адміністраторів про потенційно небезпечні ситуації.

2.2 Функції IPS:

2.2.1 Автоматичне реагування блокує або усуває шкідливий трафік автоматично.

2.2.2 Захист мережі активно запобігає атакам на основі виявлених вразливостей.

2.3 Переваги IDS/IPS:

2.3.1 Ефективне виявлення і блокування специфічних типів атак.

2.3.2 Забезпечення реагування в реальному часі на інциденти.

2.4 Обмеження IDS/IPS:

2.4.1 Може генерувати помилкові спрацьовування.

2.4.2 Потребує постійного оновлення для ефективного виявлення нових загроз.

Порівняння показує, що кожна з розглянутих технологій захисту мережі має свої унікальні переваги та недоліки. Honeypod є надзвичайно корисним для збору інформації про нові та невідомі загрози, що робить його незамінним інструментом для аналітики та дослідження кіберзагроз. Однак, для

ефективного захисту мережі в реальному часі необхідно використовувати інші технології, такі як мережеві екрани, IDS/IPS та антивірусне програмне забезпечення. Використання Honeypod у поєднанні з цими технологіями дозволяє забезпечити багаторівневий захист мережі, що значно знижує ризики та підвищує рівень безпеки організації.

Дуже перспективним напрямком майбутнього розвитку систем.захисту інформації є використання пасток, що імітують боротьбу з ворогом шляхом стохастичного управління змінами вразливостей, такі пастки називаюься ескалаційними. [13].

Також з перспективного оновлення це інтеграція Honeypod з системами штучного інтелекту є одним із найперспективніших напрямків модернізації цієї технології. ШІ здатний аналізувати великі обсяги даних, виявляти складні шаблони та робити прогнози на основі наявної інформації.

Можливості інтеграції Honeypod з ШІ:

- Автоматичний аналіз даних. ШІ може автоматично обробляти дані, зібрані Honeypod, виявляти аномалії та підозрілі активності, що значно спрощує роботу аналітиків з кібербезпеки.
- Прогнозування загроз. Завдяки використанню алгоритмів машинного навчання, ШІ може прогнозувати потенційні загрози на основі аналізу минулих атак та поведінки зловмисників.
- Покращене виявлення аномалій. ШІ здатний виявляти складні та невідомі раніше шаблони атак, що може бути важливим для виявлення нових типів загроз, які традиційні методи можуть пропустити.
- Інтелектуальна класифікація загроз. ШІ може класифікувати виявлені загрози за ступенем небезпеки, що дозволяє пріоритизувати реагування на інциденти та зосереджувати ресурси на найбільш критичних загрозах.
- Автоматизація реагування. Інтеграція з ШІ дозволяє автоматизувати процес реагування на інциденти, включаючи ізоляцію підозрілої активності, блокування шкідливого трафіку та повідомлення персоналу.

3.3 Розробка моделі конфлікту і аналіз стратегій атак та захисту

Відповідно з загальною теорією конфлікту, процес протистояння між нападником і захисником описується диференціальними рівняннями або рівняннями з різними аргументами [11].

Ця гіпотеза справедлива для дискретних систем із затримкою, таких як комп'ютерні мережі та розподілені інформаційні системи.

Продуктивність E_1 системи S_{ids} і продуктивність E_2 системи S_{icm} протягом інтервалу спостереження T у загальному випадку нелінійних функцій станів zids , Zicm і вектори $\xi(t)$, $\eta(t)$ відповідно. Їх взаємозалежність відповідає рівнянню (1).

Якщо врахувати коефіцієнт нормалізації випадкових процесів у великих системах [12], то за допомогою гауссового наближення можна розв'язати рівняння в малому околі екстремумів точок E1 і E2. У цьому випадку це вирази для ефективностей мають вигляд.

Метою кожної системи є максимізація її ефективності шляхом зниження ефективності протилежної сторони. Однак результати зусиль будуть відомі лише в момент часу T.

Протягом періоду спостереження $0 \le t \le T$ можуть забезпечити найкраще управління $u_1^{(t)}$, дія $v_1^{(t)}$ і передбачити кінцевий результат, ґрунтуючись лише на припущеннях про протилежні поведінкові стратегії. Дані Ніка та поточного стану zids і zicm.

Включення в рівняння в функцію $v_1^{(t)}$ означає перенаправлення частини ресурсів на формування оборонних або контрнаступальних впливів.

Тому необхідно вирішувати конфліктну проблему за Додатковим критерієм є мінімізація частки ресурсів, що виділяються на захист, або встановлення обмеження на їх допустимого споживання цієї частки ресурсів.

Діаграма моделі конфлікту [1] між зловмисником S_{icm} та захисником S_{ids}, модифікована на випадок використання стратегії ескалації до підробленого сервісу (пастка, система дезінформації), представлена в роботі [4]. Модель

реального конфлікту зазвичай нелінійна, але для отримання асимптотичних оцінок за досить тривалий період спостереження (з великою кількістю періодів) вона може бути спрощена під час розвитку конфлікту прийнятно виконати ступінчаста лінеаризація моделі шляхом екстраполяції на основі кореляційно-регресійних методів.[13].

Була розроблена модифікована поетапна процедура з примусовою заміною та.включення.не залежних пермінних для знаходження екстрапольованих коефіцієнтів лінеаризованої моделі.

У той же час, видалення відсутніх значень із вибірки незалежної змінної (ресурси діяльності та фіктивні служби).X_i, $1 \leq i \leq p$.не є.необхідним, бо це може призвести до відсутності змінних X_1,.теоретично може оставити цей елемент в зразку і використовувати вимірювання X_1, X_2 ,… X_{i-1}, X_{i+1},… X_p.для знаходження вектора транспортного засобу RX.

У практичній ситуації, щоб отримати ці дані, потрібно використовувати наближені методи видалити елементи, залишивши лише повні елементи, тобто елементи зі значенням повністю присутні замінити середнє замінити відсутнє значення Хі замінено середнє значення всього набору n. x_i , завдяки чому результуючий шаблон завершується до попарного видалення, регресійної заміни.

На жаль, статистичні властивості кожного з наведених методів часто невідомі, тому немає гарантії, що отримані оцінки будуть неупередженими. Отже, вибіркові елементи та/або змінні з відсутніми значеннями слід виключити, щоб забезпечити баланс між кількістю змінних і кількістю залишкових елементів.

Іншими словами, кількість повних елементів у шаблоні максимізовано , Якщо елемент містить багато відсутніх значень, його потрібно видалити.

З іншого боку, якщо більшість елементів не визначають значення змінної, то ця змінна відкидається.Тоді можна застосувати стандартні методи множинного регресійного аналізу [14].

На рисунку 3.2 представлено лінеаризовану модель процесів розвитку конфлікту з прогнозуванням і корекцією хибних гіпотез («модель типу прогноз-

корекція» [15].

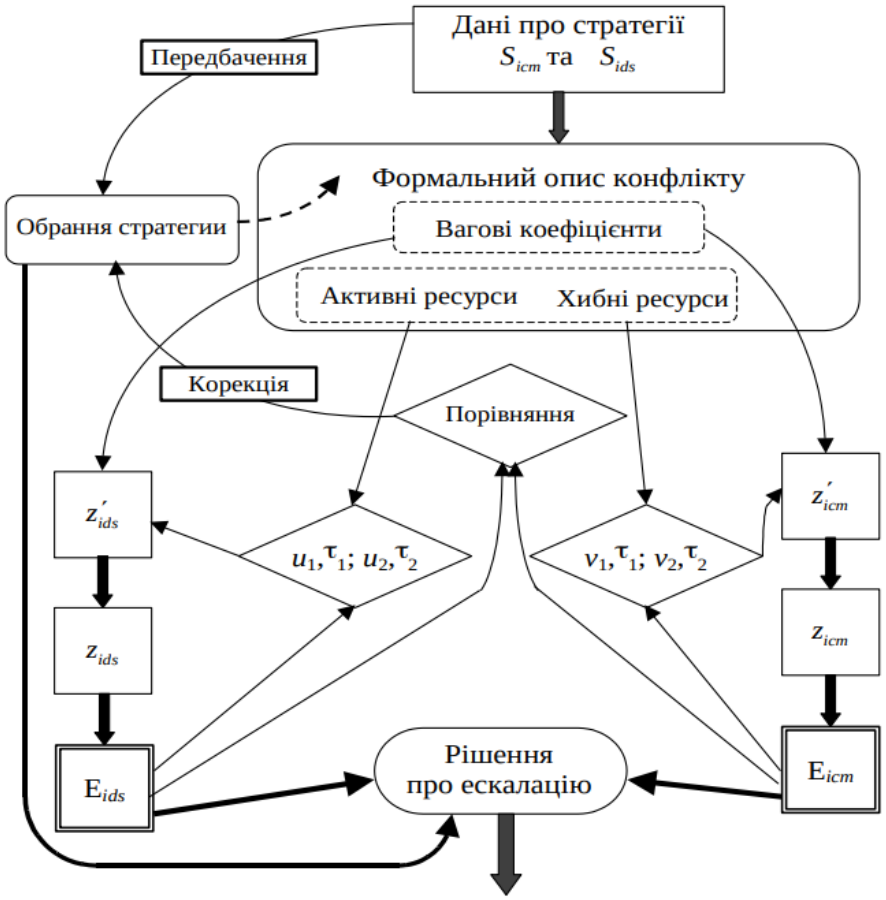

Рисунок 3.2 Лінеаризована модель конфлікту з можливістю ескалації до псевдосервісів

Стратегії контратаки та атаки, розроблена відповідно до класичної теорії конфлікту [9] та модифікована для конкретного завдання, яке розглядається [4].

Ми розглянемо набір основних оборонних стратегій, включаючи:

- Встановлення зон безпеки з рубежами оборони зовнішнім, невійськовим та внутрішнім.
- Відмова у прийомі блокування підозрілого трафіку на етапі вхідних воріт.
- Розподілена відмова у прийомі пересилання підозрілого трафіку на кілька точок і блокування його джерела з усіх цих точок.
- Насичення захисних ліній фейковими сервісами для відтворення відомих вразливостей, що вводить ворогів у пастки.
- Реакція на агресивну поведінку хакера, демонстрація спокою та

впевненості.

- Реакція на втрату інтересу, виявлення розгубленості.
- У системі захисту, заснованій на теорії конфлікту, активні дії розглядаються як відповідь на потенційну атаку. Також розглядаються теоретичні моделі та методи аналізу для прогнозування розвитку конфліктів та оптимізації послідовності захисних заходів. Щодо юридичного аспекту, передбачається, що оцінка ефективності цієї технічної системи може бути проведена достатньо точно й об’єктивно.

3.4 Висновки до розділу

Розглядається та аналізується захист комп’ютерних мереж від розподілених атак.

Одним із методів, який зазвичай використовують зловмисне програмне забезпечення для приховування цільової системи, є атака з впровадженням коду на хост.

Це дозволяє зловмисному програмному забезпеченню виконувати свій код у зовнішньому просторі процесу, дозволяючи йому працювати непомітно та отримувати доступ до важливої інформації з інших процесів.

Оскільки існує багато різних способів введення та виконання коду у зовнішньому просторі обробки, потрібен загальний підхід, щоб охопити всі ці можливості.

Підходів, які зосереджені лише на низькорівневих деталях операційної системи (таких як підключення API), недостатньо, оскільки.набір підозрілих API постійно розширюється.

Тому підходи, які зосереджуються на низькорівневих деталях операційної системи, як правило, пропускають нові атаки. Крім того, такі підходи обмежуються глибоким знанням.операційної системи. Запропонована технологія «Honeypot».

Технологія Honeypot є одним із найефективніших і доступних способів виявлення та захисту від атак на мережеві ресурси.

Приваблива та доступна для зловмисника мішень, розташована всередині

мережі, що не відрізняється від реальних ресурсів зовні, єдина мета якої – привернути увагу зловмисника, спровокувати його.

Здійснюємо протиправні дії та повідомляємо про вторгнення особу, відповідальну за комп'ютерну безпеку. Проаналізовано розташування приманки в системі безпеки промислової компанії. Розроблено модель конфлікту та аналіз стратегій наступу та оборони.

Відповідно до загальної теорії конфлікту, процес протистояння між нападниками та захисниками описується диференціальними рівняннями або.рівняннями з різними аргументами.

Ця гіпотеза справедлива для дискретних систем із затримкою, таких як комп'ютерні мережі та розподілені інформаційні системи.

Сама стратегія оцінюється за її інформаційною цінністю та інтенсивністю за джерелом енергії (наприклад, за кількістю точок, на які здійснюється розподілена атака).

РОЗДІЛ 4 БЕЗПЕКА ЖИТТЄДІЯЛЬНОСТІ, ОСНОВИ ОХОРОНИ ПРАЦІ

4.1 Вимоги пожежної безпеки при гасінні електроустановок

Гасіння пожеж в електроустановках має свою специфіку через наявність електричного струму та високої напруги, що створює додаткові ризики для пожежників.

Основними принципами є:

- Вимкнення електроживлення Це перший і найважливіший крок при гасінні пожежі в електроустановках. Якщо це можливо, слід відключити всі електричні лінії та устаткування, щоб уникнути ризику ураження електричним струмом.
- Використання спеціальних вогнегасників. Для гасіння електроустановок під напругою використовують вогнегасники, які не проводять електричний струм, наприклад, порошкові, вуглекислотні або хладонові.
- Дотримання безпечної відстані. Пожежники повинні триматися на безпечній відстані від електроустановок, щоб уникнути ризику ураження електричним струмом або опіків.

Засоби гасіння пожеж в електроустановках [44]. Для ефективного гасіння пожеж в електроустановках використовуються різноманітні засоби, кожен з яких має свої особливості та сфери застосування:

- Порошкові вогнегасники використовуються для гасіння електроустановок до 1000 В. Вони ефективно гасять пожежі класів A, B, C та E.
- Вуглекислотні вогнегасники застосовуються для гасіння електроустановок до 1000 В. Вуглекислий газ не проводить електричний струм і ефективно знижує температуру, позбавляючи вогонь кисню.

Особливості гасіння пожеж в різних типах електроустановок [45] Кожен тип

електроустановки має свої специфічні особливості, які слід враховувати при гасінні пожежі:

- Трансформаторні підстанції у разі пожежі на трансформаторній підстанції слід спочатку вимкнути живлення і використовувати вогнегасники, призначені для гасіння олійних пожеж, оскільки трансформатори часто заповнені трансформаторною олією.
- Кабельні тунелі та шахти пожежі в кабельних тунелях особливо небезпечні через обмежений доступ та високу концентрацію диму. Для їх гасіння використовують автоматичні системи пожежогасіння з інертними газами або водяні системи тонкорозпиленої води.
- Електрощитові та розподільні установки[47-48].
- При гасінні пожеж в цих установках необхідно використовувати вуглекислотні або порошкові вогнегасники і забезпечити швидке відключення живлення, щоб уникнути пошкодження електрообладнання.

Запобіжні заходи та підготовка до гасіння пожеж в електроустановках [46]. Ефективне гасіння пожеж в електроустановках вимагає ретельної підготовки та дотримання запобіжних заходів:

- Навчання персоналу. Персонал, який обслуговує електроустановки, повинен регулярно проходити навчання з правил пожежної безпеки та практичних навичок користування вогнегасниками.
- Огляд та обслуговування вогнегасників. Всі вогнегасники повинні регулярно перевірятися та обслуговуватися для забезпечення їхньої працездатності у випадку пожежі.
- Системи раннього виявлення пожежі. Встановлення автоматичних систем раннього виявлення пожежі допомагає вчасно виявити загрозу та прийняти відповідні заходи для її ліквідації.

4.2 Правила охорони праці під час експлуатації ЕОМ

Правила охорони праці на робочих місцях з використанням електронно-

обчислювальних машин (далі - Правила) поширюються на робочі місця з використанням електронно-обчислювальних машин (далі - ЕОМ) (у тому числі на робочі місця з використанням ЕОМ, обладнаних відеодисплейними терміналами (далі - ВДТ) та периферійними пристроями (далі - ПЕОМ)) незалежно від форм власності. (Дія цих Правил поширюється на осіб, зайнятих на роботах, пов'язаних з використанням ЕОМ (у тому числі на робочих місцях з використанням ВДТ та периферійних пристроїв - далі - ПЕОМ)). Це Положення встановлює вимоги охорони праці щодо обладнання робочих місць та використання операторами (далі - оператори) електронно-обчислювальних машин (далі - ЕОМ) і периферійних пристроїв (далі - ПЕОМ), які використовують ЕОМ і периферійні пристрої. Вимоги цього Положення є обов'язковими для роботодавців, операторів ЕОМ які використовують у роботі комп'ютери з ВДТ і ПП.

Вимоги цього положення не поширюються на:

- робочі місця студентів та учнів у комп'ютерних кабінетах вищих навчальних закладів, професійно-технічних навчальних закладів та загальноосвітніх навчальних закладів
- робочі місця операторів комп'ютерного набору у сфері управління та експлуатації атомних електростанцій.
- робочі місця пілотів, водіїв або операторів ЕОМ з ВДТ і ПП, комп'ютерів для засобів зв'язку та систем обробки даних, а також комп'ютеризованих засобів у складі машин і устаткування, що рухаються під час їх роботи
- Робочі місця працівників, зайнятих обслуговуванням, ремонтом та налагодженням комп'ютерів з ВДТ та ПП.
- Переносні системи обробки даних (якщо вони не використовуються постійно на робочому місці)
- Комп'ютери, касові апарати та обладнання з невеликими пристроями для відображення даних або результатів вимірювань
- Друкарські машинки класичної конструкції, обладнані DTP (екранними друкарськими машинками).

- Робочі місця повинні відповідати вимогам цього Положення та постанови Головного державного санітарного управління України від 10 грудня 1998 року № 7 (ДСанПіН 3.3.2-007-98)
- дотримуватися вимог Правил роботи з візуальними дисплейними терміналами електронно-обчислювальних машин, затверджених ДСанПіН 3.3.2-007-98

  Навчання та перевірка знань з питань охорони праці на підприємствах мають відповідати вимогам Державних нормативних актів про охорону праці. Необхідно дотримуватися Державних санітарних норм і правил та Правил роботи з електронно-обчислювальними машинами, затверджених Міністерством юстиції України від 15 лютого 2005 року № 231/10511.
- Навчання і перевірка знань з питань пожежної безпеки на підприємствах повинні здійснюватися відповідно до "Типового положення про порядок проведення інструктажів, спеціального навчання та перевірки знань з питань пожежної безпеки на підприємствах, в установах та організаціях України".
- До роботи не допускаються особи, які не пройшли встановленого порядку навчання, інструктаж і перевірку знань з питань охорони праці, пожежної безпеки та цих Правил.

Вимоги до виробничих приміщень та вимоги до освітлення, оптимальних мікрокліматичних умов, ергономічних характеристик основних елементів робочого місця, рівнів шуму, вібрації, електромагнітного, ультрафіолетового, інфрачервоного та електростатичного випромінювання встановлені ДСанПіН 3.3.2-007-98.

Виробничі приміщення повинні відповідати затвердженій у встановленому порядку проектній документації.

Під час експлуатації будівель і споруд, де розташовані робочі місця працівників, необхідно дотримуватися правил пожежної безпеки в Україні № 252/26697 (НАПБ А.01.001-2014), затверджених наказом Міністерства внутрішніх справ України від 30 грудня 2014 року № 1417 та зареєстрованих у

Міністерстві юстиції України 5 березня 2015 року.

Вимоги до мікроклімату:

- Параметри мікроклімату на робочих місцях мають відповідати ДСН 3.3.6.042-99.
- Температура повітря в приміщеннях має бути в межах від 18 до 24 градусів Цельсія.
- Відносна вологість повітря повинна бути від 40 до 60 відсотків.
- Швидкість руху повітря на робочих місцях повинна бути не більше 0,1 м/с.
- Не допускається перевищення допустимих рівнів шуму, вібрації та електромагнітних полів.

Ергономічні вимоги до робочих місць:

- Робоче місце повинно бути обладнане меблями, які відповідають ергономічним вимогам.
- Крісло оператора повинно мати регулювання висоти сидіння і спинки, а також підлокітники.
- Висота робочої поверхні столу повинна бути від 680 до 800 мм.
- Відстань від очей оператора до екрана повинна бути не менше 500 мм.
- Кут нахилу екрана повинен бути від 20 до 50 градусів.
- Клавіатура повинна бути розташована на висоті, що забезпечує зручне положення рук під час роботи.
- Робоче місце повинно забезпечувати вільний простір для ніг оператора.

Вимоги до організації робочого процесу

- Робота на ЕОМ з ВДТ повинна організовуватися таким чином, щоб уникати тривалого неперервного навантаження на органи зору і опорно-руховий апарат.
- Тривалість безперервної роботи на ЕОМ не повинна перевищувати 2 години, після чого повинна надаватися перерва не менше 15 хвилин.
- Протягом робочого дня оператор повинен мати не менше двох перерв тривалістю не менше 15 хвилин кожна.
- Загальна тривалість роботи на ЕОМ не повинна перевищувати 6 годин

на день.

- Під час перерв оператору рекомендується виконувати комплекси вправ для зняття втоми очей та м'язового напруження.
- Роботодавець повинен забезпечити медичне обстеження операторів перед початком роботи та періодично протягом трудової діяльності.
- Роботодавець зобов'язаний забезпечити операторів інструкціями з охорони праці, які містять інформацію про безпечну організацію робочого процесу, правильне використання обладнання, а також заходи першої допомоги при нещасних випадках.

Вимоги до експлуатації та технічного обслуговування ЕОМ:

- ЕОМ повинні відповідати вимогам технічних регламентів та стандартів безпеки.
- Експлуатація ЕОМ повинна здійснюватися відповідно до технічної документації, наданої виробником.
- Технічне обслуговування ЕОМ повинно проводитися згідно з графіками, затвердженими керівництвом підприємства ЕОМ повинні регулярно перевірятися на предмет справності та відповідності вимогам безпеки.

ВИСНОВКИ

У кваліфікаційній роботі досліджено організацію систем захисту інформації у внутрішніх комп'ютерних мережах підприємств. Ця тема має велике значення для сталого розвитку компанії.

До теперішнього часу розробка і впровадження мережевих інформаційних систем є однією з найбільш важливих і хвилюючих завдань в галузі інформаційних технологій.

У процесі розробки роботи було вивчено структуру IT-мережі компанії, проаналізовано інформаційні потоки, що циркулюють у внутрішній мережі компанії, а також інформаційні потоки, що циркулюють між філіями.

Також в ході роботи було виконано такі тези з початкового завдання:

- Аналіз сучасного стану захисту інформації на підприємствах виявив основні загрози, включаючи шкідливе ПЗ та DDoS атаки.
- Розроблено методи захисту мережевого периметра з використанням маршрутизаторів, брандмауерів, VPN та IDS.
- Було виконано порівняння технологій Honeypod та IDS/IPS
- Введено технологію "Медова пастка" для відстеження і аналізу атак.
- Було виконано покращення моделі захисту Honeypod
- Використано розподілені системи виявлення вторгнень для ефективного моніторингу мережевого трафіку.

Проведено аналіз стратегій атак і захисту з використанням моделей конфлікту, що дозволило розробити проактивні заходи для підвищення безпеки мереж.

У кваліфікаційній роботі запропоновано додаткові заходи захисту інформації, розроблено архітектуру системи захисту безпеки та обмеження доступу до комп'ютерної мережі підприємства:.

- периметр мережі вузлів і каналів передачі даних.
- брандмауери та маршрутизатори з фільтрацією пакетів.
- мережа перекладів alres.
- транслятор адрес основного та альтернативного портів.
- підсистема захисту від розподілених кібератак:

- підроблені сервіси з явними вразливими місцями («медові пастки»).
- підроблені мережеві служби з уразливістю безпеки (мережі «медової пастки»).

Як базове рішення для підсистеми захисту від атак розподілених мереж застосовано теорію колізій та адаптацію рівня вразливості до поведінки атакуючого суб'єкта:

- агресивна поведінка - демонструє спокій.
- нейтральна поведінка - виявляє впевненість.

Втрата інтересу є ознакою розгубленості. Такі зміни у стратегії взаємодії системи захисту зі зловмисником дозволяють зловмиснику залишатися в напруженому стані та усувають підозри, що зловмисник потрапив у.пастку.

Для захисту конфіденційної інформації, що передається між філіями, використовується технологія віртуальної корпоративної мережі компанії, яка дозволяє реалізувати захист каналу передачі даних від перехоплення та зміни інформації.

Проксі-сервери можуть приховувати інформацію про джерело запиту або користувача.

У цьому випадку зовнішній сервер бачить лише інформацію про проксі-сервер, наприклад IP-адресу, але не може визначити фактичне джерело запиту.

Існують також підроблені проксі, які передають на сторонні сервери неправдиву інформацію про реальних користувачів.

Для керування використовується інтерфейс, який має кілька наборів інструментів для керування доступом користувачів через протоколи HTTP та FTP.

Також є можливість переглянути статистичні дані, такі як часто відвідувані вузли, кількість «захоплених» вірусів тощо.

Термінальний сервер використовується для взаємодії між філією та центральним офісом через канал VPN. Термінальний клієнт після встановлення з’єднання з термінальним сервером передає вхідні дані (натискання клавіш, рухи миші) останньому та може надавати доступ до локальних ресурсів (наприклад, принтерів, дискових ресурсів, накопичувачів) порт (COM/LPT).

Термінальний сервер забезпечує робоче середовище (термінальний сеанс) для запуску програм користувача.

Результати роботи сервера передаються клієнту, як правило, це зображення для екрану і звук (якщо є).

Переваги програми з використанням термінального сервера більш очевидні:

- Зменшене навантаження на канал зв'язку
- Покращена безпека
- Канали VPN передають дані менш небезпечно.

Отже, кваліфікаційне завдання виконано. Отримані результати можуть бути використані (з відповідними змінами та доповненнями) для захисту інформації в корпоративних комп’ютерних мережах компаній різного розміру та призначення.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. "Розгляд великої дискусії щодо систем виявлення інтрузій: аналіз сигнатур проти аналізу протоколів" - Метт Танасе, 5 лютого 2003 р.
2. "Дебати IDS: Сигнатурний аналіз проти аналізу протоколів" - М. Танасе.
3. Бекер, І., Тимощук, В., Маслянка, Т., & Тимощук, Д. (2023). МЕТОДИКА ЗАХИСТУ ВІД ПОВІЛЬНИХ ТА ШВИДКИХ BRUTE-FORCE АТАК НА IMAP СЕРВЕР. Матеріали конференцій МНЛ, (17 листопада 2023 р., м. Львів), 275-276.
4. "Мережна безпека: Топ-Даун Підхід, 7-е видання" - Джеймс Ф. Куроуз, Кіт В. Росс - Pearson Education, Inc., 2017 - 864 стор.
5. Тимощук, В., & Стебельський, М. (2023). Шифрування даних в операційних системах. Матеріали VI Міжнародної студентської науково-технічної конференції „Природничі та гуманітарні науки. Актуальні питання “, 183-184.
6. "Фреймворки для мережевих пасток та їх застосування: новий підхід" - Чі Кіонг Нг, Лей Пан, Янг Сян - Springer Nature Singapore Pte Ltd., 2018 - 81 стор.
7. Тимощук, В., Долінський, А., & Тимощук, Д. (2024). СИСТЕМА ЗМЕНШЕННЯ ВПЛИВУ DOS-АТАК НА ОСНОВІ MIKROTIK. Матеріали конференцій МЦНД, (17.05. 2024; Ужгород, Україна), 198-200.
8. "Honeypots: Відстеження хакерів" - Ленс Спітцнер - Addison Wesley, 2002 - 480 стор.
9. ZAGORODNA, N., STADNYK, M., LYPA, B., GAVRYLOV, M., & KOZAK, R. (2022). Network Attack Detection Using Machine Learning Methods. Challenges to national defence in contemporary geopolitical situation, 2022(1), 55-61.
10. Tymoshchuk, V., Karnaukhov, A., & Tymoshchuk, D. (2024). USING VPN TECHNOLOGY TO CREATE SECURE CORPORATE NETWORKS. Collection of scientific papers «ΛΌГОΣ», (June 21, 2024; Seoul, South Korea), 166-170.

11. "Кібербезпека - стратегії атак та захисту" - Юрій Діогенес, Ердал Озкая - Packt Publishing Ltd., 2018 - 354 стор.

12. "Практичний посібник з комп'ютерної мережевої безпеки, четверте видання" - Джозеф Мігга Кізза - Springer International Publishing AG, 2017 - 569 стор.

13. Tymoshchuk, V., Dolinskyi, A., & Tymoshchuk, D. (2024). MESSENGER BOTS IN SMART HOMES: COGNITIVE AGENTS AT THE FOREFRONT OF THE INTEGRATION OF CYBER-PHYSICAL SYSTEMS AND THE INTERNET OF THINGS. Матеріали конференцій МЦНД, (07.06. 2024; Луцьк, Україна), 266-267.

14. "Слабкі ланки: Універсальний ключ до стійкості мереж та складних систем" - П. Чсермели - Springer-Verlag Berlin Heidelberg 2009 - 404 стор.

15. Kharchenko, O., Raichev, I., Bodnarchuk, I., & Zagorodna, N. (2018, February). Optimization of software architecture selection for the system under design and reengineering. In 2018 14th International Conference on Advanced Trends in Radioelecrtronics, Telecommunications and Computer Engineering (TCSET) (pp. 1245-1248). IEEE.

16. "Системи обчислень в реальному часі (3-є видання)" - Дж.К. Буттатцо - Springer Science+Business Media, LLC 2011 - 521 стор.

17. Kharchenko, A., Halay, I., Zagorodna, N., & Bodnarchuk, I. (2015, September). Trade-off optimal decision of the problem of software system architecture choice. In 2015 Xth International Scientific and Technical Conference" Computer Sciences and Information Technologies"(CSIT) (pp. 198-205). IEEE.

18. "Аналіз та синтез дискретних стохастичних систем з мережевими складнощами в часі" - Деруй Дінг, Зідонг Ванг, Гуоліанг Вей - CRC Press, 2019 - 249 стор.

19. Ревнюк, О. А., Загородна, Н. В., Козак, Р. О., Карпінський, М. П., & Флуд, Л. О. (2024). The improvement of web-application SDL process to prevent Insecure Design vulnerabilities. Прикладні аспекти інформаційних технологій, 7(2), 162-174.

20. "UML проектування систем реального часу, паралельних та

розподілених додатків" - Х. Гома - М.: ДМК Прес, 2011 - 704 стор.

21. Kuznetsov, A., Karpinski, M., Ziubina, R., Kandiy, S., Frontoni, E., Peliukh, O., ... & Kozak, R. (2023). Generation of nonlinear substitutions by simulated annealing algorithm. Information, 14(5), 259.

22. Stallings W. Wireless Communications and Networks, 2nd Edition. - Pearson Education, Inc., Upper Saddle River, NJ, USA, 2005. - 559 pp.

23. Skorenkyy, Y., Zolotyy, R., Fedak, S., Kramar, O., & Kozak, R. (2023, June). Digital Twin Implementation in Transition of Smart Manufacturing to Industry 5.0 Practices. In CITI (pp. 12-23).

24. Joshi R.C. Honeypots: A New Approach to Information Security / R.C. Joshi, Anjali Sardana. - Science Publishers, P.O. Box 699, Enfield, NH 03748, USA, 2001. - 323 pp.

25. Тимощук , В., Долінський , А., & Тимощук , Д. (2024). ВИКОРИСТАННЯ ТЕХНІКИ ДИНАМІЧНОГО ВІДКРИВАННЯ МЕРЕЖЕВИХ ПОРТІВ ДЛЯ ПІДВИЩЕННЯ БЕЗПЕКИ СЕРВЕРІВ. Collection of Scientific Papers «ΛΌГОΣ», (May 24, 2024; Zurich, Switzerland), 233–234. https://doi.org/10.36074/logos-24.05.2024.051.

26. Schneider B. Applied Cryptography, 2nd Edition. - M.: Dialectics, 2016. - 610 pp.

27. Schneider B. Secrets and Lies. Data Security in the Digital World. SPb: Peter, 2003. - 368 pp.

28. Karnaukhov, A., Tymoshchuk, V., Orlovska, A., & Tymoshchuk, D. (2024). USE OF AUTHENTICATED AES-GCM ENCRYPTION IN VPN. Матеріали конференцій МЦНД, (14.06. 2024; Суми, Україна), 191-193. https://doi.org/10.62731/mcnd-14.06.2024.004.

29. Тимощук, В., Долінський, А., & Тимощук, Д. (2024). ЗАСТОСУВАННЯ ГІПЕРВІЗОРІВ ПЕРШОГО ТИПУ ДЛЯ СТВОРЕННЯ ЗАХИЩЕНОЇ ІТ-ІНФРАСТРУКТУРИ. Матеріали конференцій МЦНД, (24.05. 2024; Запоріжжя, Україна), 145-146.

30. Graham R. Communications, Radar and Electronic Warfare. - John Wiley and Sons, Ltd., The Atrium. Southern Gate, Chichester, West Sussex, PO19

8SQ, United Kingdom. 2011. - 378 pp.

31. Druzhinin V.V., Kontorov D.S., Kontorov M.D. Introduction to the Theory of Conflict. - M.: Radio and Communication, 1989. - 288 pp.

32. Ванца, В., Тимощук, В., Стебельський, М., & Тимощук, Д. (2023). МЕТОДИ МІНІМІЗАЦІЇ ВПЛИВУ SLOWLORIS АТАК НА ВЕБСЕРВЕР. Матеріали конференцій МЦНД, (03.11. 2023; Суми, Україна), 119-120.

33. Marchau V.A.W.J. Decision Making under Deep Uncertainty: From Theory to Practice / Vincent A. W. J. Marchau, Warren E. Walker, Pieter J. T. M. Bloemen, Steven W. Popper - Springer Nature Switzerland AG, Gewerbestrasse 11, 6330 Cham, Switzerland, 2019. - 405 pp.

34. Myers G.J. The Art of Software Testing, 3rd Edition / Glenford J. Myers, Corey Sandler, Tom Badgett. - John Wiley & Sons, Inc., 2012. - 256 pp.

35. Іваночко, Н., Тимощук, В., Букатка, С., & Тимощук, Д. (2023). РОЗРОБКА ТА ВПРОВАДЖЕННЯ ЗАХОДІВ ЗАХИСТУ ВІД UDP FLOOD АТАК НА DNS СЕРВЕР. Матеріали конференцій МНЛ, (3 листопада 2023 р., м. Вінниця), 177-178.

36. Bonaventure O. Computer Networking: Principles, Protocols, and Practice. - Release Sep 07, 2018. - 272 pp.

37. Benslama M. Ad Hoc Networks Telecommunications and Game Theory / Malek Benslama Mohamed Lamine Boucenna Hadj Batatia. - John Wiley & Sons, Inc., 2015. – 141 pp.

38. Демчук, В., Тимощук, В., & Тимощук, Д. (2023). ЗАСОБИ МІНІМІЗАЦІЇ ВПЛИВУ SYN FLOOD АТАК. Collection of scientific papers «SCIENTIA», (November 24, 2023; Kraków, Poland), 130-130.

39. Bensky A. Short-range Wireless Communication, 3rd Edition.- Elsevier, The Boulevard, Langford Lane, Kidlington, Oxford OX5 1GB, United Kingdom, 2019. - 462 pp.

40. Тимощук, В., & Тимощук, Д. (2022). Віртуалізація в центрах обробки даних-аспекти відмовостійкості. Матеріали X науково-технічної конференції „Інформаційні моделі, системи та технології “Тернопільського національного технічного університету імені Івана Пулюя, 95-95.

41. Andrusyak A.I., Demianchuk V.S., Yuriev Y.M. Aviation Electromagnetic Communication Network. – Kyiv: NAU, 2001. – 448 pp.

42. Тимощук, В., Карташов, В., Королюк, Р. І., & Рубен, Т. (2022). Огляд протоколів керування для побудови автоматизованих систем віддаленого управління. Матеріали X науково-технічної конференції „Інформаційні моделі, системи та технології “Тернопільського національного технічного університету імені Івана Пулюя, 143-144.

43. Afifi A. Statistical Analysis: A Computer-Oriented Approach, 2nd Edition / A.A. Afifi, S.P. Azen. - Academic Press. 2nd ed., 1979. - 442 pp.

44. "Класифікація пожеж. Пожежні класи" -.ДСТУ EN 2:2014.

45. "Системи протипожежного захисту" - ДБН В.2.5-56:2014.

46. "Правила пожежної безпеки в Україні, затверджені наказом МВС України від 30 грудня 2014 року № 1417"

47. "Безпека електроустановок: навчальний посібник" - А. В. Бондаренко, Київ: Видавництво НТУУ "КПІ", 2018 - 256 стор.

48. "Пожежна безпека в електроустановках: підручник" - В. А. Кузнєцов, Львів: Видавництво ЛНУ ім. Івана Франка, 2017 - 320 стор.