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

Інститут електроенергетики
Факультет інформаційних технологій
Кафедра безпеки інформації та телекомунікацій

ПОЯСНЮВАЛЬНА ЗАПИСКА
дипломної роботи

магістра
(ступінь підготовки)

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

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

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

ступінь підготовки *магістр*
(назва освітнього рівня)

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

на тему: ***Розробка системи виявлення вторгнень реального масштабу часу***

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

_____ ***Мохнін Микита Ігорович***
(підпис) (прізвище ім'я по-батькові)

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

Рецензент			

Нормоконтроль			

Дніпро
2018

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

Інститут електроенергетики
Факультет інформаційних технологій
Кафедра безпеки інформації та телекомунікацій

ЗАТВЕРДЖЕНО:
завідувач кафедри
безпеки інформації та телекомунікацій
_____ Корнієнко В.І.

«_____»_____20___року

ЗАВДАННЯ
на виконання кваліфікаційної роботи магістра

спеціальності *125 Кібербезпека*
(код і назва спеціальності)

студенту **125м-16-1** **Мохнін Микита Ігорович**
(група) (прізвище ім'я по-батькові)

Тема дипломної роботи ***Розробка системи виявлення вторгнень реального масштабу часу***

1 ПІДСТАВИ ДЛЯ ПРОВЕДЕННЯ РОБОТИ

Наказ ректора Державного ВНЗ «НГУ» від _____№_____

2 МЕТА ТА ВИХІДНІ ДАНІ ДЛЯ ПРОВЕДЕННЯ РОБІТ

Об'єкт досліджень ***процес розробки системи виявлення вторгнень та Порівняння її з аналогами.***

Предмет досліджень ***стійкість системи виявлення вторгнень до існуючих та невідомих мережевих атак.***

Мета НДР ***є підвищення захисту інформації від мережевих атак на основі системи виявлення вторгнень.***

Вихідні дані для проведення роботи ***Система виявлення вторгнень, мережева атака, алгоритм k-ближніх сусідів.***

3 ОЧІКУВАНІ НАУКОВІ РЕЗУЛЬТАТИ

Наукова новизна ***полягає у тому, що дана системи виявлення вторгнень була розроблена на основі синтезу двох фундаментальних систем виявлення вторгнень та алгоритму k- ближніх сусідів.***

Практична цінність ***полягає у гнучкості використання та впровадження системи до різних типів корпоративних мереж.***

4 ВИМОГИ ДО РЕЗУЛЬТАТІВ ВИКОНАННЯ РОБОТИ

Результати повинні надати план дій та алгоритм роботи системи виявлення вторгнень, опис самої системи та результат порівняння її з аналогами.

5 ЕТАПИ ВИКОНАННЯ РОБІТ

Найменування етапів робіт	Строки виконання робіт (початок-кінець)
Збір аналітичних даних	***02.10.2017-28.10.2017***
Вивчення відомих систем виявлення вторгнень	***28.10.2017-20.11.2017***
Порівняння відомих систем виявлення вторгнень	***20.11.2017-14.12.2017***
Сформування ефективнішої системи виявлення вторгнень на основі отриманих даних та алгоритму k-ближніх сусідів.	***14.12.2017-26.12.2017***

6 РЕАЛІЗАЦІЯ РЕЗУЛЬТАТІВ ТА ЕФЕКТИВНІСТЬ

Економічний ефект ***доведено економічну ефективність та розраховано строк окупності затрат. Результати досліджень можуть бути використані в конфігурації серверу та в обслуговувані системи виявлення вторгнень.***

Соціальний ефект _____

7 ДОДАТКОВІ ВИМОГИ

Завдання видав _____ ст.викл. Святошенко В.О.
(підпис) (прізвище, ініціали)

Завдання прийняв до виконання _____ ст Мохнін М.І.
(підпис) (прізвище, ініціали)

Дата видачі завдання: _____

Термін подання дипломної роботи до ДЕК _____

ЗМІСТ

С.

СПИСОК УМОВНИХ СКОРОЧЕНЬ

БД – база даних

ВСВВ – вузлова система виявлення вторгнень

КСЗІ – комплексна система захисту інформації

МСВВ – мережева система виявлення вторгнень

ОС – операційна система

ПЗ – програмне забезпечення

СВВ – система виявлення вторгнень

СВЗВ – система виявлення і запобігання вторгнень

СНД – спроба несанкціонованого доступу

СУБД – система управління базами даних

РЕФЕРАТ

Пояснювальна записка: с.____, рис. ____, табл.___, джерел___, додатків___.

Мета магістерської дипломної роботи: Розробка системи виявлення вторгнень реального масштабу часу.

Предмет дослідження: Стійкість системи виявлення вторгнень до існуючих та невідомих мережевих атак.

Об`єкт дослідження: Процес розробки системи виявлення вторгнень, та порівняння її з аналогами.

У першому розділі проаналізовано різновиди та структури систем виявлення вторгнень, наведено класифікацію та статистику мережевих атак, наведені приклади обходу СВВ та її недоліки, проведено аналіз нормативно-правової бази України та міжнародних стандартів.

У спеціальній частині обґрунтовано необхідність застосування СВВ, проведено аналіз системи виявлення вторгнень, дослідження існуючих СВВ, було проведено порівняння її з аналогом та розроблено модель для подальшого впровадження СВВ.

У економічному розділі було розраховано капіталовкладення для створення системи виявлення вторгнень, вартість її обслуговування, та рентабельність на прикладі інтернет-магазину «Parfum.ua»

Науково новизна роботи полягає у розробці системи виявлення вторгнень, створені подальших правил та методів для впроваджені її на підприємстві.

ІНФОРМАЦІЙНА БЕЗПЕКА, СИСТЕМА ВИЯВЛЕННЯ ВТОРГНЕНЬ, ХМАРНІ СЕРВІСИ, КОМП’ЮТЕРНІ МЕРЕЖІ, ВИЯВЛЕННЯ МЕРЕЖЕВИХ АТАК.

РЕФЕРАТ

Объяснительная записка: с.___, рис. ___, табл.___, источников__, приложений ___.

Цель магистерской дипломной работы: Разработка системы обнаружения вторжений реального масштаба времени.

Предмет исследования: Устойчивость системы обнаружения вторжений в существующих и неизвестных сетевых атак.

Объект исследования: Процесс разработки системы обнаружения вторжений, и сравнение ее с аналогами.

В первой главе проанализированы разновидности и структуры систем обнаружения вторжений, приведена классификация и статистику сетевых атак, приведены примеры обхода СОВ и ее недостатки, проведен анализ нормативно-правовой базы Украины и международными стандартами.

В специальной части обоснована необходимость применения СОВ, проведен анализ системы обнаружения вторжений, исследования существующих СОВ, было проведено сравнение ее с аналогом и разработана модель для дальнейшего внедрения СОВ.

В экономическом разделе было рассчитано капиталовложения для создания системы обнаружения вторжений, стоимость ее обслуживания, и рентабельность на примере интернет-магазина «Parfum.ua»

Научная новизна работы заключается в разработке системы обнаружения вторжений, созданные дальнейших правил и методов для внедрены ее на предприятии.

ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ, СИСТЕМА ОБНАРУЖЕНИЯ ВТОРЖЕНИЙ, ОБЛАЧНЫЕ СЕРВИСЫ, КОМПЬЮТЕРНЫЕ СЕТИ, ОБНАРУЖЕНИЕ СЕТЕВЫХ АТАК.

ABSTRACT

Explanatory note: p.____, figures_____, tables____, supplements_____, sources___.

The purpose of master's thesis: Development of a system for detecting invasions of real time.

Subject of research: Stability of the system of detecting intruders to existing and unknown network attacks.

Object of research: The process of developing a system for detecting intrusions, and comparing it with analogues.

The first section analyzes the varieties and structures of intrusion detection systems, presents the classification and statistics of network attacks, gives examples of the bypass of the SVR and its shortcomings, analyzes the legal framework of Ukraine and international standards.

The special part substantiates the necessity of using IDS, analyzes the system of detecting intrusions, investigates existing IDS, compares them with the analogue and develops a model for the further introduction of IDS.

In the economic section, investments were made to create a system for detecting intrusions, the cost of its maintenance, and profitability on the example of the online store "Parfum.ua"

Scientific novelty of the work is to develop a system for detecting intruders, created further rules and methods for its implementation in the enterprise.

INFORMATION SAFETY, INTRUSION DETECTION SYSTEM, CLOUD SERVISE, COMPUTER NETWORKS, DETECTION OF NETWORK ATTACHES.

ВСТУП

Інтенсивний розвиток Інтернет, повсюдний перехід на електронні форми зберігання і передачі інформації, активне впровадження в повсякденне життя електронних форм платежів і багато інших чинників сьогоднішньої реальності вплинули на те, що безпека мереж і мережевих сервісів стала дійсно нагальною проблемою практично всіх організацій. У невеликих організаціях зі слабо розвиненою інформаційною структурою ця проблема поки що малопомітна, і вирішується вона установкою антивірусного пакета, який, як правило, рідко оновлюється, або намагається обмежити доступ до ресурсів. Але, як показує практика, цього явно недостатньо. Важлива інформація для компанії може бути втрачена, вкрадена зловмисниками, якщо її керівництво абияк ставиться до безпеки своєї корпоративної мережі.

Дані в трьох випадках можуть бути модифіковані, знищені:

- всередині локальної мережі співробітниками навмисно або ненавмисно;
- стороння особа проникне в локальну мережу ззовні;
- стороння особа перехопить інформацію в глобальній мережі по шляху її від одного підрозділу до іншого.

Всі перераховані вище випадки можуть завдати значної шкоди компанії. Тому продумана і добре організована система безпеки дозволяє уникнути або звести до мінімуму втрату важливих даних організації, тим самим виключивши додаткові витрати.

Дана дипломна робота є актуальною, так як:

− Відбувається постійне збільшення інформаційних ресурсів, тому необхідно використовувати засоби захисту для виявлення цих загроз;

− Вже згадана система виявлення вторгнення є популярною і її застосування повинно бути досліджено;

− На ринку інформаційних технологій існує потреба в виявленні раніше невідомих атак, так як вони з'являються з великою швидкістю.

РОЗДІЛ 1
ЗАГАЛЬНІ ВІДОМОСТІ ПРО СИСТЕМИ ВИЯВЛЕННЯ ВТОРНЕНЬ ТА ЇХ ПРИЗНАЧЕННЯ

1.1 Інформаційні загрози

В даний час набули поширення як глобальні, так і локальні мережі. Більшість організацій в тій чи іншій мірі ними користується. Уявімо, що компанія складається з великого числа підрозділів, які розкидані на значні відстані один від одного. Розкид окремих частин компанії може бути в межах міста аж до масштабів всього світу. Для того щоб організація працювала як єдине ціле, все її віддалені офіси повинні взаємодіяти між собою. На допомогу якраз і приходять комп'ютерні мережі. В межах одного офісу комп'ютери зв'язуються за допомогою локальної мережі. Всі локальні мережі організації зв'язуються через глобальну мережу інтернет. З одного боку це зручно і практично, але з іншого породжує проблеми, пов'язані із захистом інформації.

Під загрозами конфіденційної інформації прийнято приймати потенційні або реально можливі дії по відношенню до інформаційних ресурсів, що призводять до неправомірного оволодіння охоронюваними відомостями. Такими діями є:

– Ознайомлення з конфіденційною інформацією різними шляхами і способами без порушення її цілісності;

– Модифікація інформації в кримінальних цілях як часткове або значна зміна складу і змісту відомостей;

– Руйнування (знищення) інформації як акт вандалізму з метою прямого нанесення матеріального збитку.

Таким чином це призводить до порушенню її:

– Конфіденційності;

– Цілісності;

– Доступності.

На рисунку 1.1 зображена мета інформаційної безпеки.

Рисунок 1.1 – Загроза інформіції

1.2 Класифікація мережевих атак

1.2.1 Перехоплення пакетів

Сніффер пакети являє собою прикладну програму, яка використовує мережевий інтерфейс, що працює в «нерозбірливому» режимі (від англ. Promiscuous mode). В цьому режимі мережевий адаптер дозволяє приймати всі пакети, отримані по фізичних каналах, незалежно від того кому вони адресовані і відправляє з додатком для обробки. В даний час сніфери використовуються в мережах на цілком законній підставі. Вони використовуються для діагностики несправностей і аналізу трафіку. Однак через те, що деякі мережеві додатки передають дані в текстовому форматі, за допомогою сніффер можна дізнатися корисну, а іноді і конфіденційну інформацію (наприклад, імена користувачів і паролі) .

Перехоплення логінів і паролів створює велику небезпеку. Якщо додаток працює в режимі «клієнт-сервер», а аутентифікаційні дані передаються по мережі в читається текстовому форматі, то цю інформацію з великою часткою

ймовірності можна використовувати для доступу до інших корпоративних або зовнішніх ресурсів. У найгіршому випадку зловмисник отримає доступ до призначеного для користувача ресурсу на системному рівні і з його допомогою створює нового користувача, якого можна в будь-який момент використовувати для доступу в мережу і до її ресурсів.

1.2.2 IP-спуфінга

IP-спуфинг (від англ. Spoof – шахрайство) відбувається в тому випадку, коли зловмисник, що знаходиться всередині корпорації або поза нею, видає себе за санкціонованого користувача. Цього можна досягти двома способами:

– використання IP-адреси, що знаходиться в межах діапазону санкціонованих IP-адрес;

– використання авторизованого зовнішнього IP-адреси, з яким дозволяється доступ до певних мережевих ресурсів.

Атаки IP-спуфінга часто є початковим етапом для інших атак. Класичний приклад - атака DoS, яка починається з чужого адреси, що приховує справжню особу зловмисника.

Як правило, IP-спуфинг обмежується вставкою помилкової інформації або шкідливих команд у звичайний потік даних, переданих між клієнтським і серверним додатком або по каналу зв'язку між однорангових пристроями. Для двостороннього зв'язку зловмисник повинен змінити все таблиці маршрутизації, щоб направити трафік на помилковий IP-адреса.

Якщо ж зловмисник зумів поміняти таблиці маршрутизації і направити мережевий трафік на помилковий IP-адреса, то він отримає все пакети і зможе відповідати на них так, як ніби є санкціонованим користувачем.

1.2.3 Відмова в обслуговуванні

Відмова в обслуговуванні (від англ. Denial of Service, скорочено DoS), без сумніву, є найбільш відомою формою мережевих атак. Крім того, проти атак такого типу найважче створити стовідсотковий захист. Для організації DoS

потрібно мінімум знань і умінь. Проте саме простота реалізації і величезні масштаби завданої шкоди залучають зловмисників до DoS-атак.

Дана атака істотно відрізняється від інших видів атак. Зловмисники не мають на меті отримання доступу до мережі, а також отримання з цієї мережі будь-якої інформації, але атака DoS робить вашу мережу недоступною для звичайного використання за рахунок перевищення допустимих меж функціонування мережі, операційної системи або програми. У разі використання деяких серверних додатків (таких як Web-сервер або FTP-сервер) атаки DoS можуть полягати в тому, щоб зайняти всі з'єднання, доступні для цих додатків, і тримати їх в зайнятому стані, не допускаючи обслуговування рядових користувачів. В ході атак DoS можуть використовуватися звичайні інтернет-протоколи, такі як TCP і ICMP.

Деякі атаки зводять до нуля продуктивність мережі, переповняючи її небажаними і непотрібними пакетами або повідомляючи помилкову інформацію про поточний стан мережевих ресурсів. Коли атака даного типу проводиться одночасно через безліч пристроїв, ми говоримо про розподіленої атаки DoS (від англ. Distributed DoS, скорочено DDoS).

1.2.4 Парольні атаки

Зловмисники можуть проводити парольні атаки за допомогою цілого ряду методів, таких як простий перебір (brute force attack), троянський кінь, IP-спуфинг і сніффінг пакетів. Не дивлячись на те, що логін і пароль часто можна отримати за допомогою IP-спуфинга і сніффінга пакетів, зловмисники нерідко намагаються підібрати пароль і логін, використовуючи для цього численні спроби доступу. Такий підхід носить назву простого перебору.

Для такої атаки використовується спеціальна програма, яка намагається отримати доступ до ресурсу загального користування (наприклад, до сервера). Якщо в результаті зловмисникові надається доступ до ресурсів, то він отримує його на правах користувача, пароль якого був підібраний. Якщо даний користувач має значні привілеї доступу, зловмисник може створити собі

«прохід» для майбутнього доступу, який буде діяти, навіть якщо користувач змінить свій пароль.

1.2.5 Атаки типу «людина посередині

Для атаки типу людина посередині (від англ. Man-in-the-Middle) зловмисникові потрібен доступ до пакетів, що передаються по мережі. Такий доступ до всіх пакетів, що передаються від провайдера в будь-яку іншу мережу, може, наприклад, отримати співробітник цього провайдера. Для атак даного типу часто використовуються сніфери пакетів, транспортні протоколи і протоколи маршрутизації. Атаки проводяться з метою крадіжки інформації, перехоплення поточної сесії і отримання доступу до приватних мережевих ресурсів, для аналізу трафіку і отримання інформації про мережу та її користувачів, для проведення атак типу DoS, спотворення переданих даних і введення несанкціонованої інформації в мережеві сесії.

1.2.6 Атаки на рівні додатків

Атаки на рівні додатків можуть проводитися кількома способами. Найпоширеніший з них - використання добре відомих слабкостей серверного програмного забезпечення (sendmail, HTTP, FTP). Використовуючи ці слабкості, зловмисники можуть отримати доступ до комп'ютера від імені користувача, що працює з додатком (зазвичай це буває не простий користувач, а привілейований адміністратор з правами системного доступу). Відомості про атаки на рівні додатків широко публікуються, щоб дати адміністраторам можливість виправити проблему за допомогою корекційних модулів (патчів). На жаль, багато хакерів також мають доступ до цих відомостей, що дозволяє їм удосконалюватися.

Головна проблема при атаках на рівні додатків полягає в тому, що зловмисники часто користуються портами, яким дозволений прохід через міжмережевий екран (firewall). Наприклад, зловмисник, який експлуатує відому слабкість Web-сервера, часто використовує в ході атаки TCP порт 80. Оскільки

web-сервер надає користувачам Web-сторінки, то міжмережевий екран повинен забезпечувати доступ до цього порту. З точки зору брандмауера атака розглядається як стандартний трафік для порту 80.

1.2.7 Віруси і додатки типу «троянський кінь»

Робочі станції кінцевих користувачів дуже уразливі для вірусів і троянських коней. Вірусами називаються шкідливі програми, які впроваджуються в інші програми для виконання певної небажаної функції на робочій станції кінцевого користувача. Як приклад можна привести вірус, який прописується у файлі command.com (головному інтерпретаторі систем Windows) і стирає інші файли, а також заражає всі інші знайдені ним версії command.com.

Троянський кінь – це не програмна вставка, а справжня програма, яка на перший погляд здається корисним додатком, а на ділі виконує шкідливу роль. Прикладом типового троянського коня є програма, яка виглядає, як проста гра для робочої станції користувача. Однак поки користувач грає в гру, програма відправляє свою копію електронною поштою кожному абоненту, занесеному в адресну книгу цього користувача. Всі абоненти отримують поштою гру, викликаючи її подальше поширення [1].

1.3 Статистика мережевих атак

Очевидно, що в першу чергу зловмисники намагаються застосувати найбільш прості атаки, які не потребують особливих умов для виконання. В основному нижчий відсоток виявлення атаки свідчить про більш високому рівні складності або необхідність спеціальних умов для її реалізації, наприклад, наявності функції завантаження файлів в веб-додатку або вчинення певних дій з боку користувачів. На рисунку 1.2 показаний рейтинг найбільш популярних атак.

Більшість атак в цьому рейтингу експлуатують критично небезпечні уразливості і можуть привести до повної компрометації веб-додатка і сервера, що може дозволити зловмиснику отримати доступ до ресурсів локальної мережі.

Рисунок 1.2 – Рейтинг найбільш популярних атак

Співвідношення типів атак, і їх кількість змінюються в залежності від галузі, до якої відноситься досліджувана система. Зловмисники переслідують різні цілі, при цьому рівень кваліфікації і технічні можливості порушників також різняться. На наведених діаграмах представлені середня кількість атак в день на одну систему, а також співвідношення кількості атак, які виконуються вручну і з використанням утиліт для автоматизованого сканування. На рисунку 1.3 зображені середня кількість атак в день на одну систему.

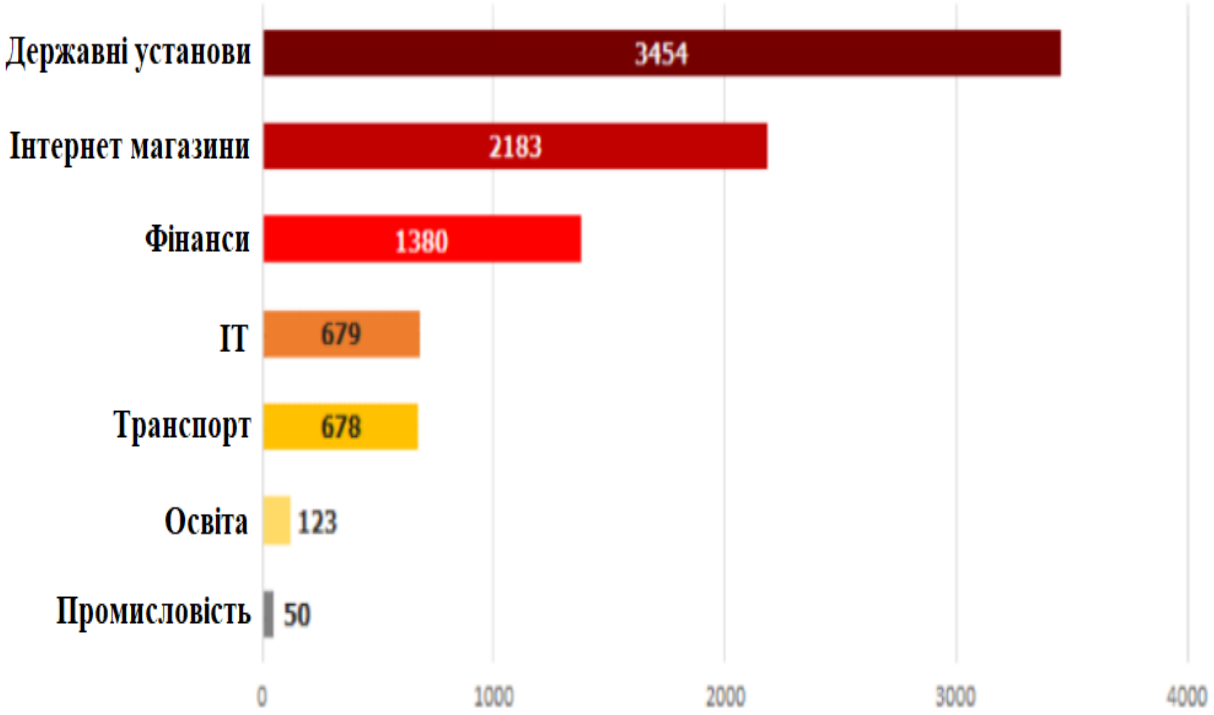

Рисунок 1.3 – Середня кількість атак в день на одну систему

На рисунку 1.4 показана співвідношення автоматизованого сканування і атак, які виконуються вручну.

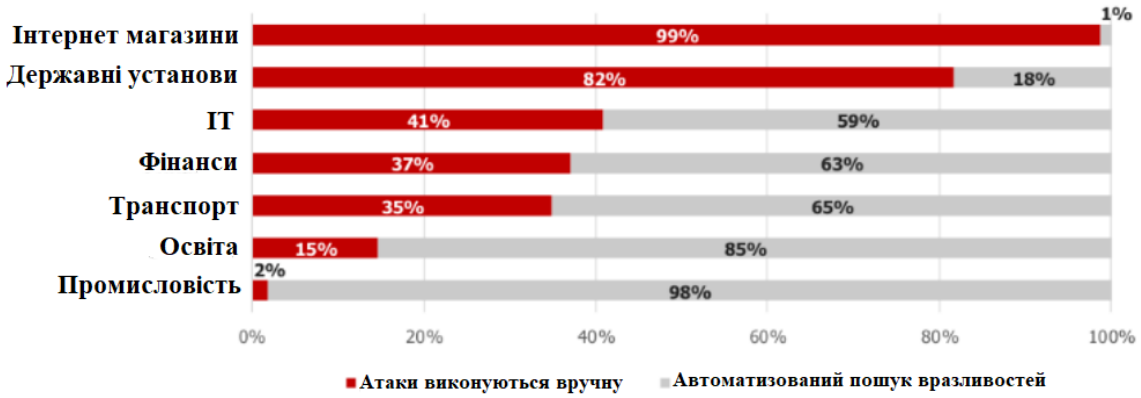

Рисунок 1.4 – Співвідношення атак

Більшу частину атак для всіх галузей, крім державних установ та інтернет-магазинів, складають атаки, що виконуються за допомогою спеціалізованого ПЗ для пошуку вразливостей. Автоматизоване сканування включає в себе спроби виконання різних видів атак, наприклад, впровадження операторів SQL, Path Traversal, з використанням готових програмних засобів інструментального аналізу захищеності. Результати сканування можуть бути використані зловмисником для експлуатації вразливостей і подальшого розвитку вектора

атаки до отримання доступу до чутливої інформації, ресурсів локальної мережі, критично важливих систем або для проведення атак на користувачів.

Найбільше середня кількість атак в день – чином, 3500 атак – зафіксовано в ході пілотних проектів в державних установах. Автоматизований пошук вразливостей становить всього 18% від загального числа атак. Інтернет-магазини займають другий рядок в цьому рейтингу: в день реєструвалося близько 2200 атак, при цьому практично всі вони проводилися без використання автоматизованих засобів сканування.

У фінансовій сфері було зареєстровано близько 1400 атак в день, серед яких переважав автоматизований пошук вразливостей. На транспортні ресурси та IT-компанії доводиться в середньому близько 680 атак в день, більшу частину яких також становить автоматизований пошук вразливостей.

З розрахунків середньої кількості атак в день для сфери освіти був виключений інформаційно-аналітичний центр, в функції якого входить обробка результатів державних іспитів. Пілотний проект для цього центру проходив улітку, коли учні шкіл здавали екзамени, в зв'язку з чим спостерігалося надзвичайно велике число атак на веб-додаток - більше 20 000 атак в день. При цьому найпоширенішими були атаки з використанням інструментальних засобів сканування на наявність вразливостей. Учні, володіючи базовими знаннями про інформаційну безпеку і способах обходу механізмів захисту, могли використовувати загальнодоступне ПЗ для сканування системи. Цим пояснюється і той факт, що більша частина атак даного типу виходила з боку США: ймовірно, публічні утиліти або онлайн-сервіси використовували проксі-сервери, розташовані на території США. Метою атак на інформаційно-аналітичний центр, швидше за все, був доступ до результатів іспитів і екзаменаційним матеріалами. Можливо, учні вважали, що таким чином зможуть змінити свої бали, отримані за іспит. Крім того, можна припустити, що зловмисники намагалися знайти уразливості, експлуатація яких дозволила б отримати доступ до баз екзаменаційних матеріалів для подальшого нелегального поширення.

Для промислових систем зафіксували близько 50 атак в день, практично всі представляли собою автоматизований пошук вразливостей, і лише 1% проводився вручну.

Для державних установ понад 70% склали атаки Path Traversal, за допомогою яких зловмисники намагалися вийти за межі поточного каталогу файлової системи і отримати доступ до файлів, що знаходяться на сервері, з метою розкрадання чутливої інформації.

Близько 17% атак є спробами впровадження операторів SQL. Невелику частину (близько 8%) складають атаки «міжсайтовий виконання сценаріїв», спрямовані на користувачів порталів державних послуг. Виконати команди ОС зловмисники намагалися в 2% випадків.

Майже три чверті атак на інтернет-магазини склали атаки Path Traversal. Так само, як і на порталах, що надають державні послуги, зловмисники робили спроби вийти за межі поточного каталогу файлової системи. Істотну частину (14%) складають атаки на відмову в обслуговуванні. Для інтернет-магазину загроза порушення доступності веб-додатки є критичною. Атаки на користувачів («міжсайтовий виконання сценаріїв» і «Підробка міжсайтових запитів») в сумі складають 4%. У 4% випадків зустрічається і впровадження операторів SQL.

У фінансовій сфері близько 65% в сукупності склали атаки «міжсайтовий виконання сценаріїв» і «Підробка міжсайтових запитів», спрямовані на користувачів систем. Такі атаки широко поширені у фінансовій галузі і становлять особливу небезпеку, оскільки дозволяють викрадати значення Cookie та облікові дані користувачів (за допомогою фішингу), а також здійснювати дії від імені легітимних користувачів.

Зловмисники намагалися отримати доступ до чутливої інформації за допомогою атаки Path Traversal (15% від загального числа) і впровадження операторів SQL (7% від загального числа). Частка атак «Завантаження довільних файлів» склала 7%. Подібні атаки часто використовуються для отримання доступу до виконання команд ОС, при цьому безпосереднє виконання команд ОС було зареєстровано в 3% випадків. В цілому, характер і складність атак

свідчать про вищий рівень технічної підготовки зловмисників в порівнянні з іншими розглянутими галузями.

У сфері IT більше половини зафіксованих атак є спробами впровадження операторів SQL. Присутні також атаки Path Traversal (20% від загального числа). Крім того, 16% є спробами виконання команд ОС, а 12% атак на веб-додатки IT-компаній націлені на користувачів систем.

Для веб-додатків транспортних компаній кількість атак «Впровадження операторів SQL» перевищує 50%, близько 38% становить витік інформації, і 6% – виконання команд ОС.

У сфері освіти приблизно 70% атак, які виконуються вручну, склало «Впровадження операторів SQL». Ця атака часто є досить простий у виконанні, її можна використовувати для отримання доступу до особистих кабінетах користувачів або вмісту баз даних. Близько 30% атак є експлуатацію вразливості

Витік інформації», яка може дозволити зловмиснику отримати чутливі дані або потрібна додаткова інформація про систему.

Аналіз джерел атак проводився тільки в відношенні українських систем, які брали участь в пілотних проектах. Найбільше число зафіксованих атак виходять з російськомовних країн, на перших позиціях перебувають Росія і Україна. Досить високий відсоток атак, джерелом яких є Нідерланди і США, оскільки на території цих країн знаходиться велика кількість провайдерів, що надають послуги проксі-серверів. На рисунку 1.5 зображена статистика походження атак.

Джерела зовнішніх атак на українські організації розрізняються залежно від галузі. Велика частина атак на державні установи здійснюється з російських IP-адрес, близько третини відбуваються з IP-адрес, що належать українським провайдерам, в 6% випадків джерелом є Нідерланди.

Джерелом атак для інтернет-магазинів приблизно в рівних частках (близько чверті від загального числа) є Росія і Україна. Більше третини атак проходить через IP-адреси Нідерландів.

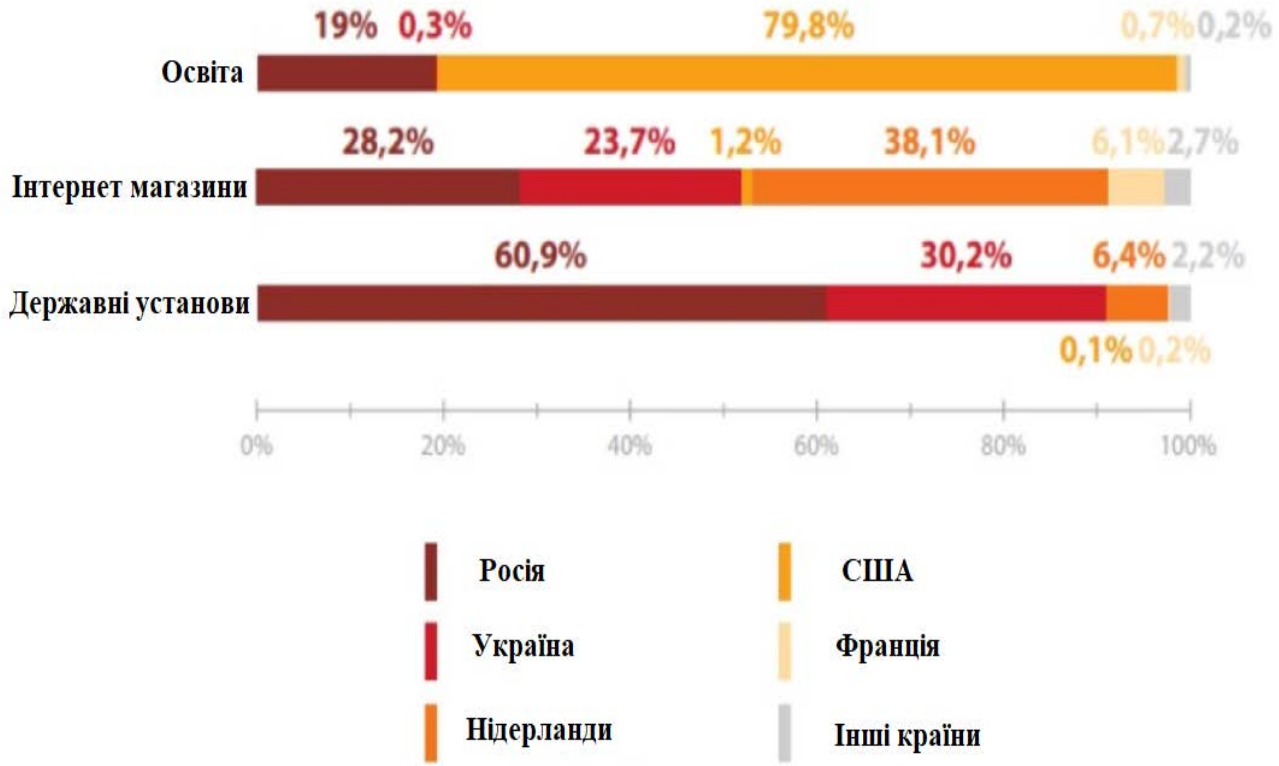

Рисунок 1.5 – Статистика походження атак

Для атак на сферу освіти, як було показано вище, широко використовуються публічні сервіси та утиліти для сканування веб-додатків на наявність вразливостей. Для приховування дійсного IP-адреси джерела атаки таке ПЗ, в основному, задіє сервери, розташовані на території США. П'ята частина атак виходить від російських IP-адрес.

Цікаво відзначити, що джерелом більше третини атак на веб-додатки університетів є внутрішні зловмисники (в середньому для сфери освіти цей показник дорівнює 8%). Ймовірно, це учні, які мають доступ до бездротових мереж освітнього закладу, а також доступ до локальної мережі в навчальних аудиторіях.

На рисунку 1.6 зображено співвідношення зовнішніх і внутрішніх порушників.

У фінансовій сфері від внутрішніх порушників виходить близько 10% атак. Не виключається також варіант, що порушником в ряді випадків може бути адміністратор системи, який проводить тестування захисних механізмів.

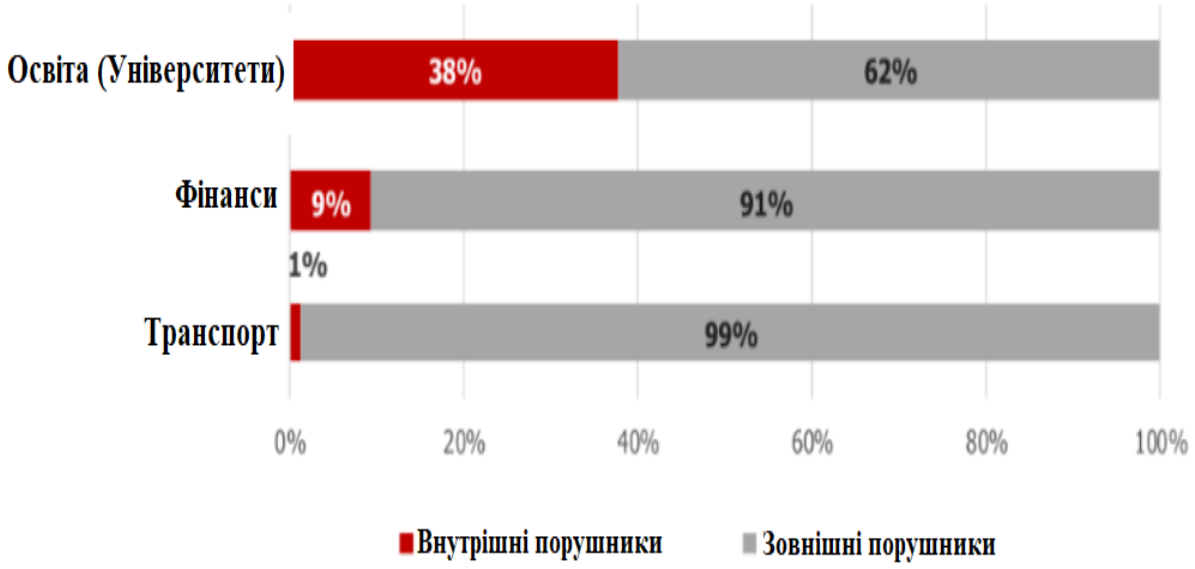

Рисунок 1.6 – Співвідношення зовнішніх і внутрішніх порушників.

Незважаючи на велику кількість простих атак, слід також враховувати, що рівень технічної підготовки сучасних зловмисників дозволяє реалізувати атаки високого рівня складності, що вимагають здійснення низки дій, які відбуваються в різний час і на перший погляд не пов'язані між собою. Для виявлення ланцюжків таких атак, в тому числі для виявлення тривалих цільових атак і при розслідуванні інцидентів, необхідно використовувати інструменти кореляційного аналізу [2].

1.4 Методи виявлення аномалій

Статистичний аналіз: Дана група методів заснована на побудові статистичного профілю поведінки системи протягом деякого періоду «Навчання», при якому поведінка системи вважається нормальним [3]. Для кожного параметра функціонування системи будується інтервал допустимих значень, з використанням деякого відомого закону розподілу. Далі, в режимі виявлення, система оцінює відхилення спостережуваних значень від значень, отриманих під час навчання. Якщо відхилення перевищують деякі задані значення, то фіксується факт аномалії (атаки). для статистичного аналізу характерний високий рівень помилкових спрацьовувань при використанні в

локальних мережах, де поведінка об'єктів не має гладкого, усередненого характеру. Крім того, даний метод стійкий тільки в межах конкретної системи, тобто побудовані статистичні профілі не можна використовувати на інших аналогічних системах.

Кластерний аналіз: Суть даної групи методів полягає в розбитті безлічі спостережуваних векторів-властивостей системи на кластери, серед яких виділяють кластери нормальної поведінки [4]. У кожному конкретному методі кластерного аналізу використовується своя метрика, яка дозволяє оцінювати приналежність спостережуваного вектора властивостей системи одному з кластерів або вихід за межі відомих кластерів. Кластерний аналіз є адаптивним, але не верифіковані і стійким в межах конкретної системи, в якій збиралися дані для побудови кластерів. Нейронні мережі: нейронні мережі для виявлення аномалій навчаються протягом деякого періоду часу, коли все спостерігається поведінка вважається нормальним [5]. Після навчання нейронна мережа запускається в режимі розпізнавання. У ситуації, коли у вхідному потоці не вдається розпізнати нормальне поведінку, фіксується факт атаки. У разі використання репрезентативною навчальної вибірки нейронні мережі дають хорошу стійкість в межах заданої системи; але складання подібної вибірки є серйозною і складним завданням. Класичні нейронні мережі мають високу обчислювальну складність навчання, що ускладнює їх застосування на великих потоках даних.

Імунні мережі: Виявлення аномалій є одним з можливих додатків імунних методів. Так як кількість прикладів нормальної поведінки зазвичай на порядки перевищує число прикладів атак, використання імунних мереж для виявлення анормалій має велику обчислювальну складність [6]. Експертні системи: Інформація про нормальному поведінці представляється в подібних системах у вигляді правил, а спостерігається поведінка у вигляді фактів. На підставі фактів і правил приймається рішення про відповідність спостережуваного поведінки «нормальному», або про наявність аномалії. Головний недолік подібних систем

- висока обчислювальна складність (в загальному випадку). В тому числі при виявленні аномалій [7].

Поведінкова біометрія: Включає в себе методи, які не потребують спеціального обладнання (сканерів сітківки, відбитків пальців), тобто методи виявлення атак, засновані на спостереження клавіатурного почерку і використання миші. В основі методів лежить гіпотеза про відмінність «почерку» роботи з інтерфейсами введення-виведення для різних користувачів. На базі побудованого профілю нормального поведінки для даного користувача виявляються відхилення від цього профілю, викликані спробами інших осіб працювати з клавіатурою або іншими фізичними пристроями введення. Поведінкова біометрія має строго локальну стійкість (В межах однієї мережі) і слабо верифіковані [8].

Support vector machines (SVM): SVM застосовний як для виявлення зловживань, так і для виявлення аномалій, при цьому метод має переваги і недоліки, аналогічні нейронних мереж [9].

1.5 Поняття про системи виявлення вторгнень

Система виявлення вторгнень є програмною або апаратною системою, яка автоматизує процес перегляду подій, що виникають в комп'ютерній системі або мережі, і аналізують їх з точки зору безпеки. Відповідний англійський термін - Intrusion Detection System (IDS). Надалі для стислості викладу систему виявлення вторгнень будемо називати СВВ. Виявлення вторгнень є процесом моніторингу подій, що відбуваються в комп'ютерній системі або мережі, і аналізу їх. Вторгнення визначаються як спроби компрометації конфіденційності, цілісності, доступності або обходу механізмів безпеки комп'ютера або мережі. Проникнення можуть здійснюватися як атакуючими, які отримують доступ до систем з Інтернету, так і авторизованими користувачами систем, які намагаються отримати додаткові привілеї, яких у них немає. СВВ є програмними або апаратними пристроями, які автоматизують процес моніторингу та аналізу подій, що відбуваються в мережі або системі, з метою виявлення вторгнень. СВВ

складаються з трьох функціональних компонентів: інформаційних джерел, аналізу та відповіді. Система отримує інформацію про подію з одного або більше джерел інформації, виконує визначається конфігурацією аналіз даних події і потім створює спеціальні відповіді – від найпростіших звітів до активного втручання при визначенні проникнень

Виявлення вторгнень може бути визначено як: ідентифікація комп'ютера або мережевих ресурсів для зловмисних намірів та поведінки і відповідь на процес. Система виявлення може виявляти спроби несанкціонованого проникнення у системний об'єкт або поведінки при моніторингу ліцензіатів незаконної роботи системних ресурсів.

Система виявлення вторгнень складається з трьох модулів:

- Модуля збору інформації;
- Модуля аналізу інформації;
- Модулів сигналізації і відповіді.

1.5.1 Збір та обробка даних

Збір інформації про виявлення вторгнення є важливим аспектом. Хороші чи погані аспекти результатів тесту безпосередньо визначають точність інформації, що збирається, яка повинна бути в межах великої або низької надійності одного джерела інформації. Тільки за допомогою цілого ряду різних джерел інформації, які дозволяють ідентифікувати невідповідності в поведінці, мабуть, єдиний спосіб забезпечити точність виявлення.

1.5.2 Аналіз даних

Основне завдання аналізу інформації – збирати інформацію про тестування, інформація включає в себе комп'ютерні системи, статус мережі і їхній недавній звіт про діяльність. На цьому етапі використовуються різні методи виявлення, база правил, бібліотека функцій, бібліотека атак.

1.5.3 Реагування та відповідь

Цей процес використовується для відповіді на результати аналізу інформації, який дозволяє виявляти тих, хто бачить проблеми в загальному, зазвичай подається звіт , він також відомий як звіт або сигнал тривоги. Серед практичних застосувань це процес який розділений на активний і пасивний, активний відноситься до системи, який повідомляє про результат триваючого вторгнення, Що до пасивної проблеми, повідомляється тільки виявлення цих вторгнень, і якими засобами конкретна атака виконується відповідно до бібліотеки вторгнень.

Система виявлення вторгнень, має декілька видів, а саме:

- Система виявлення вторгнень на основі хоста або вузлова;
- Мережева система виявлення вторгнень;
- Прикладна система виявлення вторгнень.

1.5.4 Система виявлення вторгнень на основі хоста або вузлова.

Вузлові СВВ (ВСВВ), являють собою систему датчиків, що завантажуються на різні сервера організації і керованих центральним диспетчером. Датчики відстежують різні типи подій і роблять певні дії на сервері або передають повідомлення. Датчики ВСВВ відстежують події, пов'язані з сервером, на якому вони завантажені. Сенсор ВСВВ дозволяє визначити, чи була атака успішної, якщо атака мала місце на тій же платформі, на якій встановлений датчик. Процес датчика на сервері може займати від 5 до 15% загального процесорного часу. Тому доведеться купувати більш продуктивну систему, щоб присутність датчика негативно не позначилася на продуктивності використовуваної системі. Данна система має п'ять основних типів датчиків:

- Аналізатори журналів;
- Датчики ознак;
- Аналізатори системних викликів;
- Аналізатори поведінки додатків;
- Контролери цілісності файлів.

1.5.4.1 Аналізатори журналів

Аналізатор журналу – це те, що відображає саму назву датчика. Процес виконується на сервері і відстежує відповідні файли журналів в системі. За відповідності записи в журналі і критерію в процесі датчика ВСВВ, робить встановлену дію. Адміністратор системи, при бажанні, може визначити інші записи журналу, що представляють певний інтерес. Аналізатори журналів не запобігають атаки на систему, а реагують на подію вже після того, як воно сталося. Його можна використовувати для відстеження активності і переміщення запису про активність персоналу в область, недосяжну для адміністратора або користувача.

1.5.4.2 Датчики ознак

Це набори певних ознак подій безпеки, зіставляються з вхідним трафіком або записами журналу. Можливість аналізу вхідного трафіку, є відмінністю даних датчиків від аналізаторів журналів. Датчик ознак ВСВВ є корисним при відстеженні авторизованих користувачів всередині інформаційних систем.

1.5.4.3 Аналізатори системних викликів

Дані аналізатори здійснюють аналіз викликів між додатками і операційною системою для ідентифікації подій, пов'язаних з безпекою. Датчики даного типу розміщують програмну спайку між операційною системою і додатками. При виконанні додатком дій, його виклик операційної системи аналізується і зіставляється з базою даних ознак, які є прикладами різних типів поведінки, що представляють собою, атакуючі дії, або об'єктом інтересу для адміністратора системи виявлення вторгнень. Аналізатори системних викликів відрізняються від вище перерахованих датчиків, що вони можуть запобігати діям. Забезпечення неправильної конфігурації датчиків цього типу, або їх некоректна настройка тягне за собою помилки в додатках або відмови в їх роботі.

1.5.4.4 Аналізатори поведінки додатків

Застосовуються у вигляді програмної спайки між додатками і операційною системою, і перевіряє виклик на предмет того, чи дозволено з додатком виконувати дану дію, замість визначення відповідності виклику ознаками атак. При конфігуруванні таких датчиків необхідно створювати список дій, дозволених для виконання кожним додатком. Постачальники датчиків даного типу надають шаблони для найбільш широко використовуваних додатків.

1.5.4.5 Контролери цілісності файлів

Відстежують зміни в файлах за допомогою використання криптографічного контрольної суми або цифрового підпису файлу (Шифрування). При зміні хоча б малу частину вихідного файлу (це можуть бути атрибути файлу, такі як час і дата створення), кінцева цифровий підпис файлу буде змінена. Мета даного алгоритму - максимальне зниження можливості для внесення змін в файл зі збереженням колишньої підписи.

Обробці даного алгоритму, для створення початкової підписи, піддається при початкової конфігурації датчика кожен файл. Отримане число є доповненням до підпису і при необхідності зіставляється з оригіналом. Невідповідність показує, що в файл були внесені зміни. Контролер цілісності файлів не здійснює ідентифікацію атаки, а деталізує результати проведеної атаки.

1.5.5 Мережева система виявлення вторгнень

Мережева система виявлення вторгнень - це програмний процес, який працює на спеціально виділеній системі, і відповідає за перемикання мережевої карти в системі в нерозбірливий режим роботи, при якому мережевий адаптер пропускає весь мережевий трафік в програмне забезпечення. Аналізує трафік, використовуючи набір правил і ознак атак для визначення того, чи представляє цей трафік якийсь інтерес. Після чого генерується відповідне подія.

На даний момент в більшість систем вбудований набір ознак атак, з якими порівнюється трафік в каналі зв'язку. При відсутності якихось ознак атаки в системі виявлення вторгнень, система не помічає цю атаку. Дані системи дозволяють вказувати певний трафік за адресою джерела, кінцевій адресі, порту джерела або кінцевого порту. Це дає можливість відстеження трафіку, який відповідає ознакам атак.

Переваги використання:

– Можна повністю приховати в мережі таким чином, що зловмисник не знатиме про те, що за ним ведеться спостереження;

– Одна система МСВВ може використовуватися для моніторингу трафіку з великим числом потенційних систем-цілей;

– Може здійснювати перехоплення вмісту всіх пакетів, що прямують на систему-хосту.

Недоліки:

– Система може тільки видавати сигнал тривоги, якщо трафік відповідає встановленим правилам або ознаками;

– Може упустити потрібний трафік через використання широкої смуги пропускання або альтернативних маршрутів;

– Система не може визначити, чи була атака успішної;

– Система не може переглядати зашифрований трафік;

– В комутованих мережах (на відміну від мереж з загальними носіями) потрібні спеціальні конфігурації, без яких МСВВ буде перевіряти не весь трафік.

1.5.6 Прикладні системи виявлення вторгнень

Прикладна СВВ є спеціальним підмножиною вузлових СВВ, які аналізують події, що надійшли в програмне забезпечення програми. Найбільш загальними джерелами інформації, використовуваними прикладними СВВ, є лог-файли транзакцій додатки. Здатність взаємодіяти безпосередньо з додатком, з конкретним доменом або використовувати знання, специфічні для докладання, дозволяє прикладної СВВ визначати підозрілу поведінку авторизованих

користувачів, яке перевищує їх права доступу. Такі проблеми можуть проявитися лише при взаємодії користувача з додатком.

1.6 Історія розробки СВВ

Перша концепція СВВ з'явилася завдяки Джеймсу Андерсону і статті [10]. У 1984 Фред Коен (див. Виявлення вторгнень) зробив заяву про те, що кожне вторгнення виявити неможливо і ресурси, необхідні для виявлення вторгнень, будуть рости разом з ступенем використання комп'ютерних технологій. Дороті Деннинг, за сприяння Пітера Неймана, опублікували модель СВВ в 1986, що сформувала основу для більшості сучасних систем [11]. Її модель використовувала статистичні методи для виявлення вторгнень і називалася IDES (Intrusion detection expert system - експертна система виявлення вторгнень). Система працювала на робочих станціях Sun і перевіряла як мережевий трафік, так і дані користувача додатків [12]. IDES використовувала два підходи до виявлення вторгнень: в ній використовувалася експертна система для визначення відомих видів вторгнень і компонент виявлення, заснований на статистичних методах і профілях користувачів і систем охороняється мережі. Тереза Лунт запропонувала використовувати штучну нейронну мережу як третій компонент для підвищення ефективності виявлення [13]. Слідом за IDES в 1993 вийшла NIDES (Next-generation Intrusion Detection Expert System - експертна система виявлення вторгнень нового покоління). MIDAS (Multics intrusion detection and alerting system), експертна система, яка використовує P-BEST і LISP, була розроблена в 1988 році на основі роботи Деннінга і Неймана [14]. У цьому ж році була розроблена система Haystack, заснована на статистичних методах [15]. W & S (Wisdom & Sense - мудрість і почуття), заснований на статистичних методах детектор аномалій, був розроблений в 1989 році в Лос-Аламоської Національної лабораторії [16]. W & S створював правила на основі статистичного аналізу і потім використовував ці правила для виявлення аномалій. У 1990, в TIM (Time-based inductive machine) було реалізовано виявлення аномалій з використанням індуктивного навчання на основі послідовних патернів користувача на мові

Common LISP [17]. Програма була розроблена для VAX 3500. Приблизно в той же час був розроблений NSM (Network Security Monitor - монітор мережевої безпеки), що порівнює матриці доступу для виявлення аномалій на робочих станціях Sun-3/50 [18]. У тому ж 1990 році був розроблений ISOA (Information Security Officer's Assistant), що містить в собі безліч стратегій виявлення, включаючи статистику, перевірку профілю та експертну систему [19]. ComputerWatch, розроблений в AT & T Bell Labs, використовував статистичні методи і правила для перевірки даних і виявлення вторгнень [20].

1.7 Система виявлення вторгнень у інформаційній безпеці

На відміну від класичних методів побудови оборони, коли засоби захисту діють за принципом відокремлених бар'єрів, що встановлюються на кордоні мережі (наприклад, фільтруючий маршрутизатор або міжмережевий екран), комплексний захист, що включає, крім міжмережевих екранів, цілий набір компонентів (сканери захищеності, системи аутентифікації і авторизації, засоби побудови віртуальних приватних мереж і т.п.) виявляється більш ефективною. Один з необхідних елементів такої системи захисту інформації – засоби виявлення вторгнень. Виявлення вторгнень є процесом оцінки підозрілих дій, які відбуваються в контрольованій інформаційній системі.

Хоча і брандмауери і СВВ є системами мережевої безпеки, між ними існують серйозні відмінності. Основним завданням мережевих екранів є фільтрація трафіку між мережами з метою запобігання атак. Крім того брандмауери не можуть оповістити адміністратора про атаку або підозрілої активності всередині мережі. Системи виявлення вторгнень постійно спостерігають, пропускаючи весь трафік через себе, за потенційними порушеннями політики безпеки як ззовні, так і всередині мережі, і сповіщають про це операторів. Як правило, це досягається за допомогою комбінації методик, наприклад: аналіз мережевого трафіку, евристичний аналіз і ідентифікація сигнатур відомих атак і негайне оповіщення.

Актуальність використання систем виявлення вторгнень підтверджується зростаючим інтересом великих і дрібних організацій до даного сегменту ринку. Багато в чому він знаходиться зараз на тій же стадії, що і ринок міжмережевих екранів кілька років тому. Далеко не всі компанії розуміли важливість наявності прикордонного пристрою фільтрації, і ще менше число подбало про їх встановлення. Тому, системам виявлення вторгнень слід йти тим же шляхом. Сьогодні практично кожна організація має, принаймні, один міжмережевий екран для захисту своєї мережі. Однак при цьому керівництво і співробітники цієї організації можуть практично нічого не знати про методи і засоби виявлення вторгнень. Проте, ця обставина не завадила зародженню ринку [21].

1.8 Недоліки та вимоги до системи виявлення вторгнень

В наш час системи виявлення вторгнення - недостатньо досконалі. Безліч недоліків, властивих СВВ в даний час, згруповані наступним чином:

- відсутня універсальна методологія проектування,
- недолік ефективності;
- недостатня мобільність в контрольованому просторі;
- обмежена гнучкість (включає універсальність і динамічне налаштування);
- обмежена можливість оновлення методів виявлення;
- труднощі з підтримкою наборів правил функціонування;
- відсутність тестів продуктивності і покриття мережі;
- немає прийнятного способу перевіряти ефективність СВВ.

Багато хто продовжує вирішувати деяких з цих недоліків через удосконалення існуючих методів, але деякі недоліки властиві основам, на яких створені СВВ. У той час як мобільні агенти можуть допомагати покращувати СВВ в багатьох областях, вони не приносять ніяку допомогу в інших. Наприклад, здатність СВВ виявити нападу з конкретної точки, шляхом відстеження інформації від конкретного головного комп'ютера, конкретного додатка або конкретного мережевого інтерфейсу, є первинною проблемою, що стоїть перед

виробниками СВВ. Мобільний технологія не може розширити здатність СВВ в області виявлення поодиноких атак або зменшити відсоток помилкових спрацьовувань. Крім того, в більшості випадків, мобільна технологія уповільнює роботу СВВ при обробці подій, таким чином зменшуючи здатність виявлення. Це – несприятливий обмеження для СВВ, яка намагається оцінити події в реальному часі за інформацією з однієї точки мережі. Разом з тим, це не означає, що багатоагентні системи марні для СВВ. Багатоагентна система може вирішити кілька головних проблем, що стоять перед СВВ, але що більш важливо – вони можуть забезпечувати СВВ вигодами продуктивності і перш недоступними можливостями.

Незалежно від механізмів, на яких основана система виявлення вторгнення, вона повинна робити наступне:

- працювати безперервно без втручання людини;
- бути стійким до збоїв;
- враховувати можливі відхилення від нормальної поведінки;
- бути легко адаптованою до певної мережі;
- адаптуватися до зміни власної структури при удосконалення системи;
- бути стійким до дезинформації.

1.9 Нормативно-правова база у сфері інформаційної безпеки

Інформація, що розміщена на веб-вузлі, може бути відкритою та з обмеженим доступом. Насамперед, це може бути деяка комерційна інформація. У разі доступу до неї зловмисника компанія зазнає збитків. Крім цього, можуть бути використані персональні дані співробітників чи клієнтів, що призведе як до фінансових витрат так і до зниження ступені довіри цій компанії. Потрібно забезпечувати безпеку такої інформації у відповідності до нормативно правової бази України. Нижче наведено перелік документів, що регламентують порядок обробки інформації в сфері інформаційної безпеки:

– Закон України «Про інформацію». Цей закон регулює відносини щодо створення, збирання, одержання, зберігання, використання, поширення, охорони, захисту інформації [22];

– Закон України «Про захист інформації в інформаційно-телекомунікаційних системах». В цьому законі насамперед йдеться про те, що для інформації, яка є власністю держави, або інформації з обмеженим доступом, вимогу щодо захисту якої встановлено законом, перелік користувачів та їхні повноваження стосовно цієї інформації визначає законодавство. Захист інформації в системі забезпечує власник системи. Інформація, яка є власністю держави, або інформація з обмеженим доступом, вимогу щодо захисту якої встановлено законом, має оброблятись у системі із застосуванням комплексної системи захисту інформації;

– Закон України «Про державну таємницю». Цей Закон регулює суспільні відносини, пов'язані з віднесенням інформації до державної таємниці, засекречуванням, розсекречуванням її матеріальних носіїв та охороною державної таємниці з метою захисту національної безпеки України [23];

– Закон України «Про захист персональних даних». Цей Закон регулює правові відносини, пов’язані із захистом і обробкою персональних даних, і спрямований на захист основоположних прав і свобод людини і громадянина, зокрема права на невтручання в особисте життя, у зв’язку з обробкою персональних даних. Його дія поширюється на діяльність з обробки персональних даних, яка здійснюється повністю або частково із застосуванням автоматизованих засобів, а також на обробку персональних даних, що містяться у картотеці чи призначені до внесення до картотеки, із застосуванням неавтоматизованих засобів [24];

– НД ТЗІ 2.5-004-99. Критерії оцінки захищеності інформації в комп’ютерних системах від несанкціонованого доступу;

– НД ТЗІ 1.1-002-99. Загальні положення щодо захисту інформації в комп'ютерних системах від несанкціонованого доступу;

– НД ТЗІ 2.5-005-99. Класифікація автоматизованих систем і стандартні функціональні профілі захищеності оброблюваної інформації від несанкціонованого доступу;

– НД ТЗІ 3.7-001-99. Методичні вказівки щодо розробки технічного завдання на створення комплексної системи захисту інформації в автоматизованій системі;

– НД ТЗІ 1.4-001-2000. Типове положення про службу захисту інформації в автоматизованій системі;

– НД ТЗІ 3.6-001-2000. Технічний захист інформації. Комп'ютерні системи. Порядок створення, впровадження, супроводження та модернізації засобів технічного захисту інформації від несанкціонованого доступу;

– НД ТЗІ 3.7-003-05. Порядок проведення робіт із створення комплексної системи захисту інформації в інформаційно-телекомунікаційній системі.

Ці нормативно-правові документи дозволяють вистроїти гармонічні взаємовідносини між власником інформації та користувачем, об`єктивно здійснювати оцінку ступені захищеності інформації. В деяких з них описуються принципи та порядок створення служби захисту інформації та КСЗІ, наводиться класифікація автоматизованих систем та профілі захищеності оброблюваної інформації.

В Україні створена і діє досить розгалужена система забезпечення безпеки інформації, її захисту. Існує певна законодавча база, яка складається з Законів України «Про інформацію», «Про захист інформації в автоматизованих інформаційних системах», «Про державну таємницю» тощо. Діє ряд Указів Президента та Постанов Кабінету Міністрів України, які регулюють конкретні напрями діяльності в галузі захисту інформації.

Функціонує система ліцензування і сертифікації діяльності, зокрема виробництва товарів та надання послуг у галузі технічного і криптографічного захисту інформації. У 1998 р. на базі відповідних підрозділів Служби безпеки й Державного комітету з питань захисту державних таємниць і технічного захисту інформації створено Департамент спеціальних телекомунікаційних систем і

захисту інформації Служби безпеки України, на який покладено завдання забезпечення здійснення державної політики у галузі криптографічного і технічного захисту інформації. Відбуваються позитивні зрушення і у галузі розбудови власного виробництва засобів захисту інформації, зокрема у недержавному секторі економіки. У банківській системі завдяки діяльності Національного банку України досягнуто високого рівня інформатизації.

1.10 Висновок

У першому розділі магістерської дипломної роботи було проаналізовано різновиди та структуру системі виявлення вторгнень, обґрунтовано корисність їх створення, також був здійснений аналіз нормативно-правової бази, міжнародних стандартів, мережевих атак та була приведена їх статистика.

Згідно з метою дипломної роботи у другому розділі необхідне вирішення наступних задач:

- Обґрунтувати необхідність застосування СВВ;
- Провести аналіз систем виявлення вторгнень;
- Синтезувати систему виявлення вторгнень.

РОЗДІЛ 2

АНАЛІЗ ТА РОЗРОБКА СИСТЕМИ ВИЯВЛЕННЯ ВТОРНЕНЬ

2.1 Обґрунтування необхідності застосування СВВ

Один з основних факторів високого рівня безпеки – виявлення і припинення спроб несанкціонованого доступу (СНД) в реальному масштабі часу. Як правило, в повному обсязі це необхідно тільки дуже великим мережам, але створити добре захищену мережу без засобів, що дозволяють виявляти і припиняти СНД, просто неможливо. Прикладом захисту є між мережевий екран. Існують різні його реалізації, але мета їх застосування одна – зниження ризику проникнення в окремий персональний комп'ютер або мережу. Однак якщо в мережі встановлено між мережевий екран, то це ще не означає, що безпека гарантована. Наприклад, він не здатний захистити від користувачів, які пройшли аутентифікацію. Крім того, між мережевий екран, контролюючи кордону мережі, не тільки не запобігає вторгнення в неї через модемні пули або інші точки віддаленого доступу, але і принципово не може виявити такого зловмисника [25].

Таким чином, виявлення вторгнень – один з ключових компонентів комплексної системи захисту. Вони дозволяють збільшити безпеку мережі, контролюючи всі вхідні і вихідні потоки трафіку, як всередині периметра, що захищається організації (відстежуючи за різними оцінками від 70 до 80% порушень, пов'язаних з внутрішніми зловмисниками [26]), так і зовні (виявляючи спроби віддалених вторгнень і збираючи статистику невдалих проникнень). Крім того, мабуть, це один з небагатьох елементів системи захисту, в основі якого лежить динамічний принцип роботи, тобто можливість автоматичної зміни логіки свого функціонування по деякому зовнішній події – зміни політики виявлення вторгнень (тоді як інші засоби, наприклад, між мережеві екрани, системи аутентифікації, більш консервативні і вимагають явного втручання адміністратора). Однак аналіз статистики порушень призводить до висновку, що і цього недостатньо [27]. Незалежно від того, який клас СВВ використовується для захисту (традиційно вони поділяються на два класи: мережеві та вузлові) і

які принципи роботи СВВ відповідного класу застосовуються для виявлення підозрілих дій в мережі (виявлення аномалій або зловживань) або на вузлі (аналіз журналів прикладних програм, змін в файлової системі або контроль системних викликів), особливості вторгнень зловмисників не дозволяють їх своєчасно виявляти і блокувати.

Причина в тому, що розробники не встигають випускати доповнення і зміни до своїх коштів захисту. Відносно СВВ це виражається в несвоєчасному випуску поповнень БД ознак вторгнень. Можна заперечити, що часто винуватцем виявляється навіть не надто повільний розробник, а самі адміністратори, які не встигають підтримувати системи в актуальному стані і своєчасно встановлювати випускаються оновлення. Але недавня поява ряду загроз під назвою «атаки з нульовим часом попередження» («zero-day attacks» [28]) знову ставить на перше місце питання якнайшвидшого випуску доповнень до БД ознак вторгнень з описами останніх виявлених вразливостей, які зловмисники і використовують при проведенні своїх атак [29].

При цьому в більшості випадків негативних наслідків можна було б і уникнути, якщо б адміністратори своєчасно зреагували і виконали рекомендації щодо захисту від знову виявлених вразливостей. У цій справі накопичена величезна світова статистика, яка дозволяє зробити висновок, що найчастіше інформація про нову уразливість відома задовго (за місяці) до того, як відбудеться реальне вторгнення з її використанням. Так, наприклад, існує негласне правило, згідно з яким, хакерська група, виявляючи нове некоректну поведінку ПЗ, насамперед повідомляє про це виробника продукту, даючи йому можливість випустити виправлення і тільки через якийсь час поширює повну інформацію по уразливості [30]. Хоча надання повної інформації провокує атаки зловмисників, засуджувати подібні дії також важко. Адже, з одного боку, розробники об'єктивно зацікавлені виключно в підвищенні прибутку і зниженні витрат, зокрема пов'язаних із затримкою виходу нових версій створюваного ними ПЗ, їх ретельно тестуванням і т.п. З іншого боку, якби у розробників не було мотивації в підвищенні якості своїх продуктів і незабаром їх виправлення

(наприклад, через подібних публікацій про нововиявлених вразливості), то навряд чи б їх користувачі були б ще більше захищені.

При цьому на сьогоднішній день розробки, пов'язані із забезпеченням працездатності СВВ, ведуться в основному в напрямку створення систем централізованого управління і збору подій, оскільки групи методів, використовуваних для виявлення несанкціонованих дій, вважаються досить розвиненими [32]. Багато великі західні дослідні інститути і комерційні організації також безуспішно намагаються знайти підходи до оцінки ефективності СВВ [33], причому роботи з даної тематики можна знайти і в Україні.

Таким чином, можна зробити висновок про недостатню ефективність використовуваних в даний час СВВ, складності та актуальності теми. З більшістю сучасних мережевих погроз можна було б легко впоратися, якби існувала автоматизована система виявлення вторгнень, динамічно підстроює правила виявлення вторгнень під знову виявляються вразливості.

2.2 Аналіз системи виявлення вторгнень

Система виявлення вторгнень - це пристрій або програмне забезпечення, що забезпечує спостереження за мережевий і системної активністю і виявлення шкідливих дій і порушень політики безпеки. Прикладами порушення політики безпеки може бути: атаки на мережеві сервіси, атаки спрямовані на підвищення привілеїв, неавторизований доступ до файлів і т.п. СВВ діляться на кілька типів і підходять до вирішення завдання виявлення шкідливого трафіку по різному. Існує два основних типи СВВ – мережеві і вузлові, а також деякі інші, які будуть розглянуті нижче. Деякі СВВ можуть спробувати зупинити спробу несанкціонованого доступу, але це не є не необхідної ні основним завданням системи виявлення. Основними завданнями систем виявлення і запобігання вторгнень (СВЗВ) є виявлення можливих інцидентів, зберігання інформації про них і складання звітів про спроби злому.

Крім того, підприємства та організації використовують СВЗВ і в інших цілях, наприклад аудит систем безпеки, документування можливих вразливостей, а також в якості «лякала», що запобігає порушення політики безпеки користувачами всередині системи. СВЗВ стали невід'ємною частиною сучасної інфраструктури безпеки практично в будь-яких серйозних організаціях [33].

Як правило, СВЗВ зазвичай записують інформацію, безпосередньо відноситься до спостережуваних подій, повідомляють адміністратора мережі в разі потенційного вторгнення і складають звіти про події. Багато СВЗВ також можуть протистояти виявленим загрозам, намагаючись запобігти успіх атаки. Наприклад, СВЗВ може сама зупинити атаку, змінити налаштування брандмауера або змінити зміст атаки [34].

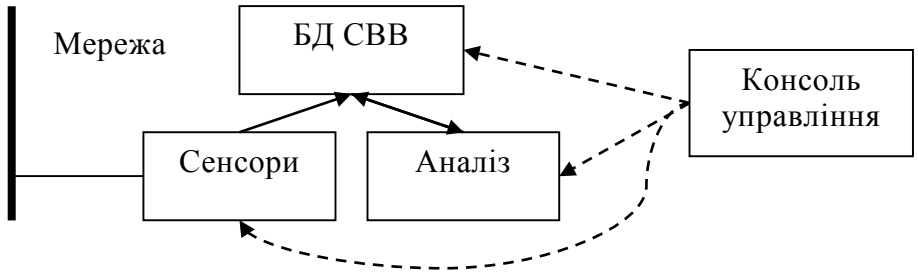

Рисунок 2.1 – Структура СВВ

Як правило, СВВ мають наступну структуру:

– Сенсорна підсистема, що збирає інформацію, пов'язану з безпекою мережі.

– Сховище, в якому зберігається інформація, що отримується від сенсорів і інформація, оброблена аналізатором.

– Аналізатор, який виявляє підозрілий трафік і атаки, грунтуючись на даних від сенсорів.

– Консоль управління, що дозволяє конфігурувати СВВ.

Системи виявлення вторгнень можна розділити на кілька видів:

– Мережеві СВВ, зазвичай представляють собою пристрій встановлюється в мережі.

– Вузлові СВВ, зазвичай представляють собою програму - агент, що встановлюється на пристрої в мережі.

– Протокол-орієнтовані СВВ: системи, які аналізує дані, що передаються певними протоколами.

– OSI7-орієнтовані СВВ: системи, що аналізують дані передаються специфічними методами протоколів сьомого рівня моделі OSI. Наприклад, встановлена на SQL сервері така СВВ буде аналізувати вміст отриманих SQL-команд.

– Гібридні СВВ, що поєднують два і більше підходу.

Надалі розглянемо мережеві і вузлові СВВ як найбільш фундаментальні. [35]

Крім того, системи виявлення вторгнень можна розділити характером відповідної реакції:

− пасивні або системи виявлення, в яких після виявлення і впізнання підозрілого трафіку СВВ тільки повідомляє користувача або адміністратора

− активні або системи запобігання, що протистояти вторгненням, шляхом скидання з'єднання або перепрограмування правил брандмауера з метою блокування підозрілого трафіку.

− гібридні, які здійснюють і виявлення та протистояння вторгненням в автоматичному режимі.

Системи виявлення вторгнень також можна класифікувати по методикам аналізу:

– статистичні СВВ

– сигнатурні СВВ

– гібридні СВВ

Надалі розглянемо їх докладніше.

МСВВ зазвичай встановлюються в стратегічно важливих точках всередині мережі та як правило представляють із себе пристрої, що підключаються до мережі організації. Вони аналізують весь проходить трафік у всій підмережі,

працюючи в нерозбірливому режимі, а потім порівнюють проходить трафік з базою вже відомих атак. Коли атака виявлена і можна сказати, повідомлення про це надсилається адміністратору. Прикладом конфігурації МСВВ є, наприклад установка її в одній підмережі з брандмауерами з метою виявлення спроб їх обходу. В ідеальному випадку МСВВ сканує весь вхідний і вихідний трафік, але на практиці це може призвести до створення «вузького місця», тим самим знижується продуктивність мережі в цілому.

Вузлові системи виявлення вторгнень (ВСВВ) працюють на окремих пристроях і робочих станціях мережі. ВСВВ аналізує трафік тільки одного пристрою, і попереджає адміністратора або користувача в разі тривоги. Крім того, ВСВВ при установці, як правило, створює резервну копію системних файлів і періодично порівнює її з поточним станом цих файлів. У разі їх зміни або відсутності, вона негайно повідомляє адміністратора для подальшого розслідування ситуації. Часто така система встановлюється на критично важливих вузлах, на яких не передбачена зміна системних установок.

Крім того, ВСВВ можуть використовувати системно-залежні засоби і ханіпоти (спеціально сконфігуровані системи, з мінімальним захистом, привал приманювати зловмисників).

2.3 Основні методи аналізу, що використовуються СВВ

Двома основними підходами до аналізу мережевої активності, на сьогоднішній день є статистичний і сигнатурний. Сучасні системи виявлення вторгнень використовують як правило комбінацію цих методів

2.3.1 Статистичні СВВ

Системи виявлення вторгнень, використовує статистичний підхід після установки "навчаються" адміністратором, який задає політику СВВ, відповідну нормальної активності в мережі – типи трафіку, з'єднання між вузлами, використовувані протоколи і порти. При виявленні аномалій в роботі мережі або статистично значущих відмінностей трафіку від типового в даній мережі, СВВ

сповіщає про це адміністратора. Основною проблемою такого підходу є складність в налаштуванні і велика кількість хибно позитивних тривог в разі некоректно заданих правил [36].

2.3.2 Сигнатурні СВВ

Сигнатурні системи виявлення вторгнень аналізують трафік в мережі і порівнюють пакети з базою даних сигнатур (відомих атрибутів атак). Такий підхід схожий з тим, як працює більшість антивірусного ПЗ. При такому підході основною проблемою є старіння баз сигнатур – між проявами нових типів атак і оновленням баз сигнатур може пройти достатню кількість часу, протягом якого СВВ буде нездатна виявити таку загрозу.

2.4 Недоліки та проблеми СВВ

Одними із головних проблем та недоліків системи виявлення вторгнень слід вважати:

− Шум може серйозно вплинути на ефективність роботи СВВ. Пакети, помилково згенеровані недоліками в розробці ПЗ, пошкоджені дані служби доменних імен можуть створити досить високий коефіцієнт помилкових тривог [37].

− Досить часто трапляється так, що кількість справжніх атак набагато менша за кількість помилкових тривог. Іноді різниця настільки велика, що справжня атака може бути проігнорована або взагалі не помічена [37].

− Старіння бібліотек сигнатур, що може серйозно позначитися на ефективності виявлення і запобігання атак [37].

− Система виявлення вторгнень не може компенсувати недоліки в проектуванні інфраструктури безпеки, уразливості протоколів як таких або слабкі методи аутентифікації. Якщо атакуючий отримує доступ, використовуючи вразливості слабкого методу аутентифікації, то СВВ не зможе запобігти збитку [35].

– Зашифровані пакети не обробляються системами виявлення вторгнень. Таким чином, атака з використанням зашифрованих пакетів може привести до успішного вторгнення, що не виявленому СВВ, поки зловмисник не почне робити дії всередині мережі, які виявляються системою [37].

– Системи виявлення вторгнень предоставяет інформацію про атаки використовуючи мережеву адресу, що міститься в IP-пакетах, що проходять в мережі. Це ефективно, якщо мережеву адресу в пакеті справжній, так як як адреса в пакеті може бути спотворений або сфальсифікований.

– Так як мережеві СВВ є мережевими пристроями, вони схильні до тих же протокол-орієнтованим атакам, що і звичайні вузли. Спотворена інформація і атаки на стек TCP/IP можуть привести до відмови в роботі МСВВ.

2.5 Способи обходу СВВ

Існує багато способів обходу СВВ, наведені нижче є найбільш простими і розповсюджений:

− Фрагментація пакетів: відсилаючи фрагментовані пакети, атакуючийздатний легко обійти сигнатурні СВВ, так як в цьому випадку СВВ не зможе виявити сигнатуру атаки, а отже і прийнять якісь заходи по її запобіганню.

− Відмова від установок за замовчуванням: якщо СВВ очікує троянської атаки на порту 12345, а атакуючий змінив порт, який використовується трояном, то СВВ, можливо, не зможе виявити загрозу.

− Скоординована атака з малою кількістю пакетів від одного атакуючого: атакуючий може повністю про сканувати мережу, використовуючи ботнет. Атакуючий назначется кожному боту різну мету і порт. В цьому випадку СВВ буде складно скоррелировать захоплені приходять пакети від цих хостів між собою і прийти до висновку що мережа організації сканується.

− Проксінг і підміна адреси: атакуючий може серйозно підвищити складність виявлення джерела атаки за допомогою погано захищених або сконфигурированних проксі-серверів, прокинувши через них трафік атаки. В такому випадку СВВ станоівтся дуже важко ідентіфіціровать джерело атаки

− Поліморфізм і зміна поведінки: більшість СВВ є сигнатурними. Трохи змінюючи вміст пакетів атаки, можливо уникнути виявлення.

2.6 Аналіз реалізацій систем виявлення вторгнень

Як уже було відзначено вище, в сучасних інфраструктурах СВВ є невід'ємною їх частиною. Найбільш популярними з систем з відкритим кодом є Snort, Suricata і OSSEC HIDS, з систем з пропрієтарним кодом CATNET і McAfee IPS.

Популярними МСВВ є Cisco Secure IDS, що встановлюється на міжмережеві екрани виробництва цієї ж компанії і Dragon IDS, гібридну СВВ, що встановлюється як на пристрої так і на робочі станції.

Найбільш перспективним напрямком розвитку СВВ є впровадження когінтівних здібностей в функціонал цих систем з використанням штучних нейронних мереж і нечіткої логіки, і зниження кількості помилкових тривог. Крім того, спостерігається тенденція до мініатюріації СВВ, що в майбутньому дозволить встановлювати їх на кожен пристрій в мережі, в тому числі на роутери та свитчи, підвищуючи рівень безопаности в цілому.

Крім того, останнім часом мета атак перемістилася на прикладний рівень моделі OSI: на веб-сервіси, XML, SOAP, ERP, CRM, СУБД, IP-телефонію та інше. Мережеві системи виявлення та запобігання перестали справлятися з атаками, так як вони не працюють на рівні їх реалізації. Тому одним з напрямків розвитку стане підтримка нових технологій і протоколів [38].

На сучасному ринку існує безліч різні систем виявлення вторгнення. Наведемо деякі з них:

− OSSEC є масштабованої, мультиплатформенной вузловий системою виявлення вторгнень. Вона має потужний компонента аналізу, в неї інтегрованим аналіз логів, перевірка цілісності файлів, централізована політика, виявлення руткітів, оповіщення в режимі рельной часу і активні заходи у відповідь. СВВ працює в більшості операційних систем, широко використовувана. OSSEC дуже

активно розвивається, тобто випускається кожні s місяці. Для корпоративний клієнтів існує комерційна підтримка. Даний продукт добре задокументований.

− Bro є мережевою системою виявлення вторгнень з відкритим вихідним кодом. Вона є пасивною СВВ тільки для користувачів unix-подібний операційних систем. На сайті виробника стверджується, що даний програмний продукт настійно рекомендується використовувати тільки як доповнення до вже встановленої СВВ. Документація дуже скупа.

− CATNET – це інтелектуальна система для виявлення, аналізу та реєстрації інцидент в мережі. Вона може виявляти аномалії і спроби мережевих вторгнень, контролювати інфраструктуру організації. Продукт пропонує швидкий і ефективний моніторинг мережі, моніторинг безпеки, журнал подій для подальшого аналізу, підтримка продукту. На жаль документація до даного програмного продукту була знайдена тільки на французькій мові, продукт випускає французька компанія.

− Snort – це продукт з відкритим вихідним кодом для виявлення і запобігання вторгнень. Початковою система вміла тільки виявляти вторгнення, але потім переросла в зрілу і більш багатофункціональну систему запобігання вторгнень. Система здатна виконувати в режимі реального часу аналіз трафіку і реєстрацію по ір-мережі. Вона заслужила всесвітню популярність, в зв'язку з цим існує досить велика кількість спільнот з підтримки продукту.

Програмні продукти добре документовані. На офіційному сайті розробника можна завантажити керівництво користувача, в якому доступно описано всі можливості даних СВВ і як їх можна конфігурувати. Мова написання власних правил гнучка.

У таблиці 2.1 наведено порівняння чотирьох систем виявлення систем за кількома параметрами.

Таблиця 2.1 Порівняльна характеристика систем виявлення вторгнень

СВВ/ Параметр	Bro	CATNET	OSSEC	Snort
Безкоштовність	+	-	+	+
Відкритість початкових кодів	+	-	+	+
Мультиплатформеність	-	+	+	+
Графічний інтерфейс	-	+	+	-
Тип системи	Мережева	Мережева	Вузлова	Мережева, вузлова

2.7 Розробка системи виявлення вторгнень.

Не можна не визнати, що технології хмарних обчислень мають величезний потенціал, тому що всі сучасні комп'ютерні продукти постійно збільшують свої вимоги до технічного оснащення комп'ютера користувача, що неминуче веде до значних витрат на вдосконалення ПК.

Обчислювальні хмари складаються з тисяч серверів, розміщених в дата-центрах, що забезпечують роботу десятків тисяч додатків, які одночасно використовують мільйони користувачів. Неодмінною умовою ефективного управління такою великомасштабної інфраструктурою є максимально повна автоматизація. Крім того, для забезпечення різних видів користувачів - хмарним операторам, сервіс-провайдерам, посередникам, IT-адміністраторам, користувачам додатків - захищеного доступу до обчислювальних ресурсів хмарна інфраструктура повинна передбачати можливість самоврядування і делегування повноважень.

Постачальники хмарних сервісів пропонують послуги декількох фундаментальних моделей:

- Інфраструктура як служба (IaaS),
- Платформа як служба (PaaS)

− Програмне забезпечення як сервіс (SaaS)

Інфраструктура як послуга (IaaS) – надання обчислювальних ресурсів за запитом, на яких замовник має можливість розгорнути і запустити довільне програмне забезпечення, що включає в себе операційні системи і додатки. В рамках даної моделі замовник не керує і не контролює лежить в основі фізичну інфраструктуру, але має контроль над операційними системами і розгорнутими додатками. Приклад моделі зображений на рисунку 2.2

Рисунок 2.2 – Модель IaaS

Платформа як послуга (PaaS) – надання хмарної платформи для розгортання програмного забезпечення, створеного на базі мов програмування і інструментів, які підтримуються хмарним провайдером. Замовник не має можливості управляти хмарної інфраструктурою (мережеве та серверне обладнання, СГД, операційними системами), але має контроль над розгорнутими додатками і, можливо, настройками навколишнього середовища.

Приклад моделі PaaS зображений на рисунку 2.3

Рисунок 2.3 – Модель PaaS

Програмне забезпечення як послуга (SaaS) – надання в користування замовнику додатків, розгорнутих на хмарної інфраструктурі провайдера. Додатки можуть бути доступні з різних клієнтських пристроїв за допомогою тонкого клієнта, термінального клієнта або браузера. Замовник не контролює параметри роботи і настройки додатків. Весь сервіс надається під ключ.

Приклад моделі SaaS зображений на рисунку 2.4

Рисунок 2.4 – Модель SaaS

2.8 Пов'язані роботи

У 2012, Kholidyand Baiardi [39] розробив рамки для системи визначення виявлення вторгнення (CIDS), щоб вирішити недоліки поточних систем виявлення вторгнень (IDS). У своїй системі, щоб збільшити охоплення атак, CIDS інтегрує підходи, основані на знаннях і на основі поведінки, та стежить за кожним вузлом для визначення локальних подій. У 2011 році Аль-Джанабі та

Саїд [40] розробили аномальну систему виявлення вторгнень, яка може швидко виявити та класифікувати різні атаки. Вони використовували Атлантичну нейронні мережі для розповсюдження поведінки системи. Набір даних KDD'99 використовується в їх експерименті, і отриманий результат задовольняє їх робочій меті. У 2010 році Маццаріелло та ін. [41] розробили модель, в якій завдання DetectingDenialofService (DoS) атаку здійснює за допомогою ресурсів, придбаних за вимогою, на платформі хмарних сервісів. Модель використовувалася для дослідження наслідків розподіленої стратегії виявлення та блокування атак або інших зловмисних дій, що виникли внаслідок неправильного використання клієнтів хмарного сервісу. У 2010 році Бакши та Йогеш [42] розробили алгоритм захисту «хмар» від атак DDOS з використанням системи виявлення вторгнень у віртуальній машині (VM). Ця модель показує, що стратегія віртуалізації IT може бути використана для реагування на атаку "Відмова в обслуговуванні". У 2009 році Галі [43] представив новий гібридний алгоритм Rough Set Neural Network Algorithm (RSNNA), який суттєво зменшує кількість ресурсів комп'ютера, як пам'яті, так і часу центрального процесора, і необхідний для виявлення атак. Алгоритми Rough Set Theory inorderto reducefea turesand навчені за допомогою артеріальної нейронної мережі для виявлення будь-яких видів нової атаки.

2.9 Запропонована модель системи виявлення вторгнень

Технологія «хмар» зараз широко розповсюджується і часто використовується, але за такою популярністю для підтримки безпеки все ще викликає занепокоєння. Користувач робить запит на потрібні дані або ресурси які здійснюються через мережу. Подальші підходи використовуються для усунення цих запитів та реагування на ці запити. Оскільки хмарний сервіс дійсно стурбований запитом клієнта, спеціальні заходи спрямовані на забезпечення цих запитів від користувачів. Нападники можуть спробувати маніпулювати користувачем, цей процес називається вторгненням і керується за допомогою системи виявлення вторгнень (СВВ). У зв'язку з цим дана запропонована модель

працює для легкого та безпечного виконання завдання, виконуваної користувачем «хмар», показаною на рисунку 2.5.

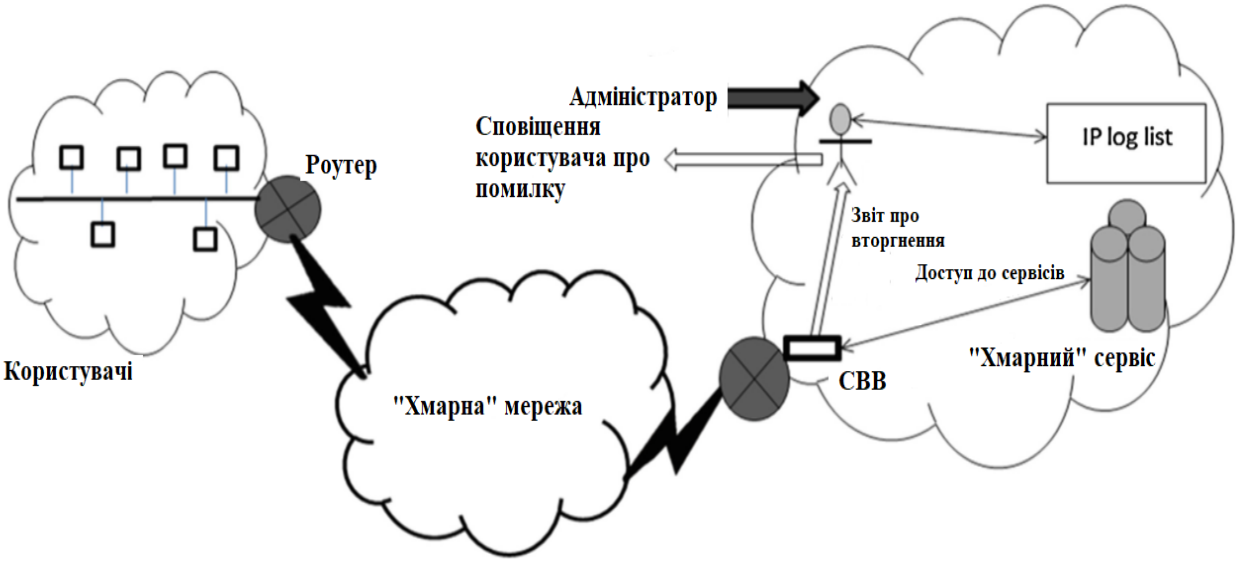

Рисунок 2.5 – Система виявлення вторгнення у «хмарному» сервісі

У запропонованої моделі СВВ мережеве обслуговування або моніторинг, використовується в умовах вузького місця мережі. У цій моделі, для виявлення вторгнення, ми використовували ВСВВ для відстеження запитів, надісланих користувачем. Для подолання трафіку великої мережі та для простого процесу виконується багато поточна обробка даних**.** Запити, зроблені з кінцевого клієнта**,** обробляються за допомогою МСВВ, зареєстрованих у СВВ. Багато потокова модель МСВВ для хмарного-середовища в основному базується на трьох модулях: модулі захоплення та запиту, модуля аналізу та модуля звітування. Модуль захоплення виконує завдання збору та отримання пакетів даних вхідного та вихідного (ICMP, TCP, IP, UDP). Оскільки велика кількість пакетів даних вводяться в МСВВ, модуль спочатку виділяє і організовує їх упорядкованим чином і розміщує їх у спільній черзі. Далі підходять і приймаються замовлені пакети як тестовий приклад для частини аналізу, як показано на рисунку 2.6

Рисунок 2.6 – Блок-схема СВВ, що використовує класифікацію KNN-NN

Пакети, захоплені з загальної черги, передаються на етап аналізу, точно аналізуються за допомогою одночасно обробки декількох потоків там. Модуль звітування відповідає на аналізовані результати та повідомляє Адміністратора про втручання, яке сталося. Після захоплення всіх пакетів для цілей аналізу, декілька потоків будуть постійно оброблятися і намагатимуться перевірити за допомогою класу KNN-NN. Класифікатор уже пройшов навчання,

використовуючи набір даних NSL-KDD. Відхилені пакети від нормальної дії додатково аналізуються для виявлення зловмисників. Процес аналізу продовжується спільним способом для покращення продуктивності системи та виконання пакетів.

Для будь-якого вхідного пакета було виконано детектування аномалій, використовуючи алгоритм K-Nearest Neighbor (KNN).

Алгоритм здатний виділити серед всіх спостережень k відомих об'єктів (k-найближчих сусідів), схожих на новий невідомий раніше об'єкт. На основі класів найближчих сусідів виноситься рішення щодо нового об'єкта. Важливим завданням даного алгоритму є підбір коефіцієнта k – кількість записів, які будуть вважатися близькими.

На першому кроці алгоритму слід задати число k – кількість найближчих сусідів. Якщо прийняти k = 1, то алгоритм втратить узагальнюючу здатність (тобто здатність видавати правильний результат для даних, що не зустрічалися раніше в алгоритмі) так як нового запису буде присвоєно клас близькому до неї. Якщо встановити занадто велике значення, то багато локальні особливості будуть виявлено.

На другому кроці знаходяться k записів з мінімальним відстанню до вектора ознак нового об'єкта (пошук сусідів).

Функція для розрахунку відстані повинна відповідати наступним правилам:

– $d(x,y) \geq 0$, $d(x,y) = 0$ Тоді і тільки тоді, коли x = y;

– $d(x,y) = d(y,x)$;

– $d(x,z) \leq d(x,y) + d(y,z)$, за умови, що точки x, y, z чи не лежать на одній прямій.

Де x, y, z – вектори ознак порівнюваних об'єктів.

Для впорядкованих значень атрибутів знаходиться Евклідова відстань:

$$D_E = \sqrt{\sum_i^n (x_i - y_i)^2} \quad (3.1)$$

де n – кількість атрибутів.

Для строкових змінних, які не можуть бути впорядковані, може бути застосована функція відмінності, яка задається наступним чином:

$$dd(x,y) = \begin{cases} 0, x = y \\ 1, x \neq y \end{cases} \quad (3.2)$$

Також виконується розрахунок нормалізації відстані.

Мінімаксна нормалізація:

$$X^x = \frac{x - \min(X)}{\max(X) - \min(X)} \quad (3.3)$$

Нормалізація за допомогою стандартного відхилення:

$$X^x = \frac{X - X_{cp}}{\sigma_x} \quad (3.4)$$

де σ_x – стандартне відхилення, $X_{ср}$ – середнє значення.

При знаходженні відстані яка дозволяє знизити помилку класифікації використовують формулу:

$$D_E = \sqrt{(x_1 - y_1)^2 + (x_2 - y_2)^2} \quad (3.5)$$

Формула для багатовимірного простору

$$D_E = \sqrt{(x_1 - y_1)^2 + (x_2 - y_2)^2 + \cdots + (x_n - y_n)^2} \quad (3.6)$$

Тобто даний алгоритм класифікує дію як «нормальний» або «аномальний». Для всіх пакетів, класифікованих як «аномальні» використовується для виявлення неправильного використання і класифікує їх до певних типів атак.

Для навчання класифікатора було використано повний пакет бібліотек NSL-KDD [44].

Якщо система помічає класифіковані пакети які позначені як «аномальні» та не може класифікувати до певних типів атак, вона повідомляє про атаку, та формує звіт у якому позначено що дана атака не знайдена у базі даних і додає примітку у звіті «невідома».

Адміністратор отримує звіт про вторгнення після класифікації і в залежності від значення лічильника подій для кожного втручання, він вживає необхідних заходів

Адміністратор використовується для підтримки списку журналів IP для записаних запитів клієнтів та для навчання класифікатора.

Навчання системи виявлення вторгнень адміністратор проводить вручну проводячи аналіз звіту кожної атаки з приміткою «невідома». Після аналізу адміністратор базуючись на висновках отриманих при аналізі, додає до класу

«нормальний» або «аномальний». ВСВВ та МСВВ, розгорнуті в Хмарній-СВВ, використовуються для моніторингу запитів користувачів. Якщо виявлено будь-який запит про втручання до Хмарної-СВВ, протокол вторгнення надсилається адміністратору для наступних дій.

Отримавши звіт про вторгнення, Адміністратор сповіщає користувача про вторгнення, а також додає його до списку журналів IP. Подальший вхід буде оброблятися адміністратором.

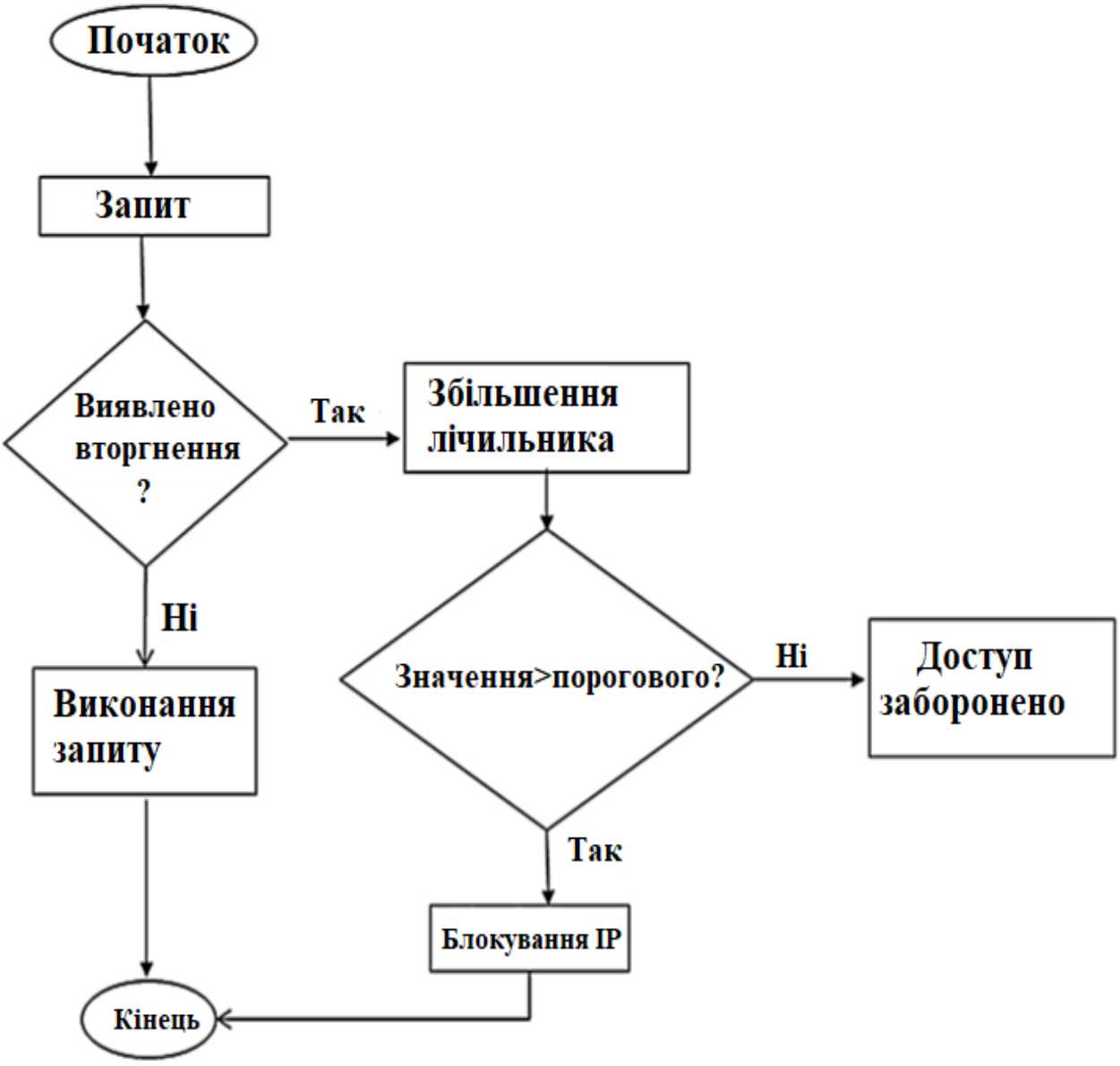

Рисунок 2.7 – Блок-схема роботи адміністратора

Для кожного втручання значення лічильника подій збільшується на 1. Значення лічильника подій перевіряється відносно порогового значення. Якщо значення лічильника буде перевищувати порогове значення, для конкретного користувача буде заборонено доступ, показаний на рисунку 2.7.

2.10 Експериментальні результати

Для виконання експерименту та оцінки ефективності запропонованої моделі як зразки атак обрана база сигнатур NSL KDD.

Після навчання і включення СВВ в режимі експлуатації, з компрометуючого ресурсу запускалася утиліта, в завдання якого входило проведення атак. Для генерації атак був використана утиліта hping3. Hping3 це безкоштовний генератор пакетів і аналізатор для TCP/IP протоколу. Hping, де факто, один з обов'язкових інструментів для аудиту безпеки і тестування файерволов і мереж, він використовувався для виконання експлойта техніки сканування Idle Scan. Нова версія hping - hping3 - написана на скриптах з використанням мови Tcl. У ній реалізується движок для зручного опису рядками TCP/IP пакетів.

На рисунку 2.8 показаний приклад DoS атаки за допомогою утиліти hping3.

```
1       root@WebWare-Kali:~# hping3 -c 10000 -d 120 -S -w 64 -p 21 --flood -
2   -rand-source 192.168.1.37
3       HPING 192.168.1.37 (eth0 192.168.1.37): S set, 40 headers + 120 data b
4   ytes
5       hping in flood mode, no replies will be shown
6       ^C
7       --- 192.168.1.37 hping statistic ---
8       3258138 packets transmitted, 0 packets received, 100% packet loss
        round-trip min/avg/max = 0.0/0.0/0.0 ms
        root@WebWare-Kali:~#
```

Рисунок 2.8 – Приклад DoS атаки за допомогою утиліта hping3

Диспетчер атак запускав у випадковій послідовності сканування і атаки, спрямовані на тестову мережу. Атаки відтворювалися через кожні 5-10 хвилин у

випадковому порядку протягом 24 годин. Інформація про час запуску і про тип атаки зберігалося в файлі історії.

Для порівняння ефективності роботи розробленої СВВ як аналог була обрана система Snort [45].

Snort – вільна і відкрита СВВ, що виробляє аналіз трафіку і використовує правила для виявленя вторгнень. Snort і запропонована СВВ в процесі своєї роботи зберігали історію роботи, виводячи час виявлення вторгнення і його тип. Після закінчення тестування файли історій атак і історій виявлення вторгнень були проаналізовані

Для визначення ефективності роботи СВВ використовувалися наступні оцінки [46]:

- False Positive (FP) – ймовірність виявлення вторгнення в разі, якщо його не було, обумовлена як відношення кількості помилкових виявлених вторгнень до загальної кількості сесій, що містять вторгнення. Таку ситуацію будемо розглядати як помилку першого роду.
- False Negative (FN) – ймовірність не виявлення вторгнення в разі, якщо воно мало місце, що визначається як відношення невиявлених вторгнень до загальної кількості сесій, що містять вторгнення. Таку ситуацію будемо розглядати як помилку другого роду.

Всього було проведено 235 атак протягом 8365 нормальних сесій. У таблиці 2.2 представлені результати порівняння роботи систем. Система Snort не змогла виявити нові типи вторгнення, так як правила для неї задаються ззовні і не формуються в процесі роботи. Розроблена СВВ показала високу ймовірність виявлення вторгнення і меншу, ніж Snort, ймовірність помилкових спрацьовувань. Крім того, виявленно 8 нових вторгнень під час експерименту.

Таблиця 2.2 Результати порівняння роботи систем

	Виявлені вторгнення	Пропущено вторгнень (Помилка II роду)	Сесії, визнані нормальними	Помилкові спрацьовування (Помилка I роду)	Нові виявлені вторгнення
Snort	186 (79,15%)	49 (20,85%)	7780(93%)	586 (7%)	0
Розроблена СВВ	216 (91,84%)	19 (8,16%)	8047 (96,2%)	235 (2,8%)	8

2.11 Висновок

Проведена робота показала актуальність проведення нових робіт в області захисту «хмарних» сервісів. Можливості розробленої інтелектуальної системи автоматизованого виявлення мережевих атак, та порівняння її з іншою системою на рику. В цей час розрахунки дозволять підвищити рівень інформаційної безпеки як наявних, так і перспективних корпоративних інфраструктур, інтегруючих обласних середовищ. У випадку запропонованої системи виявлення вторгнень для зменшення пам'яті та часу з захоплених пакетів даних витягується ряд відповідних функцій. Після вибору функції всі пакети класифікуються гібридним багаторівневим класифікатором KNN-NN для отримання більш швидкої та ефективної СВВ. Адміністратор вживає відповідних заходів для підвищення продуктивності системи після класифікації та проводить дії що до навчання класифікатора відзначаючи атаку або помилкове спрацювання до «нормального або «аномального» стану. Проведені експерименти показали більшу ефективність запропонованої системи в порівнянні з системою Snort для досліджених типів атак з точки зору здатності виявляти нові вторгнення і зменшення помилок першого і другого роду. Отже, запропонована модель служить ефективним, швидшим і безпечним підходом до виявлення вторгнення.

3 РОЗДІЛ

ЕКОНОМІЧНЕ ОБГРУНТУВАННЯ ВПРОВАДЖЕННЯ СИСТЕМИ ВИЯВЛЕННЯ ВТОРНЕНЬ

Однією з головний цілей захисту інформаційних ресурсів від внутрішніх загроз є мінімізація збитків від порушення інформаційної безпеки підприємства.

Інтернет магазини дуже швидко розповсюджуються у мережі та користуються великою популярністю у користувачів. Інтернет магазин «Parfum.ua» не виняток, згідно його даних була розроблена економічна модель.

Економічно доцільним слід вважати, якщо витрати на забезпечення інформаційної безпеки не перевищують збитків від реалізації загрози її порушення.

Щоб обґрунтувати економічну доцільність впровадження системи виявлення вторгнень порівняємо величину витрат на впровадження СВВ з величиною можливої шкоди, яку може понести підприємство внаслідок втрати інформаційних ресурсів.

3.1 Розрахунок (фіксованих) капітальних витрат

Капітальні інвестиції:

− вартість розробки проекту інформаційної безпеки (розробка схем пристроїв, політики функціонування системи тощо);

− вартість створення основного й додаткового програмного забезпечення (ПЗ);

− витрати на первісні закупівлі апаратного забезпечення;

− витрати на навчання технічних фахівців і обслуговуючого персоналу.

Спершу розрахуємо час, який буде витрачено на створення ПЗ:

$$t = t_{\text{тз}} + t_{â} + t_{б} + t_{\text{пр}} + t_{\text{опр}} + t_{д}, \text{ годин}, \qquad (3.1)$$

де $t_{\text{тз}}$ – тривалість складання технічного завдання на розробку ПЗ;

$t_{â}$ – тривалість вивчення ТЗ, літературних джерел за темою тощо;

$t_б$ – тривалість розробки блок-схеми алгоритму;

$t_{пр}$ – тривалість програмування за готовою блок-схемою;

$t_{опр}$ – тривалість опрацювання програми на ПК;

$t_д$ – тривалість підготовки технічної документації на ПЗ.

Умовна кількість оперантів у програмі:

$$Q = q \cdot c\ (1 + p), \text{ штук,} \qquad (3.2)$$

де q – очікувана кількість оперантів - 15;

c – коефіцієнт складності програми -1.25;

p – коефіцієнт корекції програми в процесі її опрацювання – 0.05.

$$Q = 15 \cdot 1{,}25(1+0.05)=19, \text{ штук.}$$

Оцінка тривалості складання технічного завдання на розробку ПЗ $\mathbf{t_{тз}}$ – 2 год.

Тривалість вивчення технічного завдання:

$$t_в = \frac{Q \cdot B}{(75...85) \cdot k} = \frac{19 \cdot 1.3}{80 \cdot 0.8} = 0.3, \text{ годин,} \qquad (3.3)$$

де B – коефіцієнт збільшення тривалості етапу внаслідок недостатнього опису завдання, B = 1,3;

k – коефіцієнт, що враховує кваліфікацію програміста і визначається стажем роботи за фахом

- до 2 років – 0,8;

Тривалість розробки блок-схеми алгоритму:

$$t_б = \frac{Q}{(20...25) \cdot k} = \frac{19}{22 \cdot 0.8} = 1, \text{ година.} \qquad (3.4)$$

Тривалість складання програми за готовою блок-схемою:

$$t_{пр} = \frac{Q}{(20...25) \cdot k} = \frac{19}{23 \cdot 0.8} = 1, \text{ година.} \qquad (3.5)$$

Тривалість опрацювання програми на ПК:

$$t_{\text{опр}} = \frac{1{,}5Q}{(4...5)\cdot k} = \frac{1.5\cdot 19}{4\cdot 0.8} = 9 \text{, годин.} \qquad (3.6)$$

Тривалість підготовки технічної документації на ПЗ:

$$t_д = \frac{Q}{(15...20)\cdot k} + \frac{Q}{(15...20)}\cdot 0{,}75 = \frac{19}{17\cdot 0.8} + \frac{19}{17}\cdot 0.75 = 2 \text{ години.} \qquad (3.7)$$

$$t = 9 + 0{,}3 + 1 + 1 + 9 + 2 = 22 \text{ години.}$$

Розрахунок витрат на створення програмного продукту

$$К_{пз} = З_{зп} + З_{мч}. \text{ грн} \qquad (3.8)$$

Заробітна плата виконавця враховує основну і додаткову заробітну плату, а також відрахування на соціальне потреби (пенсійне страхування, страхування на випадок безробіття, соціальне страхування тощо) и визначається за формулою:

$$З_{зп} = t \cdot З_{пр} = 22\cdot 62 = 1375 \text{, грн,} \qquad (3.9)$$

де t – загальна тривалість створення ПЗ, годин;

$З_{пр}$ – средньогодинна заробітна плата програміста з нарахуваннями, грн/годину.

$$З_{пр} = \frac{З_м}{168} = \frac{10500}{168} = 62 \text{, грн/годину.} \qquad (3.10)$$

де $З_м$ – середня заробітна плата на місяць – 3200 грн.

Вартість машинного часу для налагодження програми на ПК визначається за формулою:

$$З_{\text{мч}} = t_{опр}\cdot C_{\text{мч}} + t_д \cdot C_{\text{мч}} = 9\cdot 0.8 + 2\cdot 0{,}8 = 9 \text{, грн.} \qquad (3.11)$$

де $t_{опр}$ – трудомісткість налагодження програми на ПК, годин;

$t_д$ – трудомісткість підготовки документації на ПК, годин;

$С_{мч}$ – вартість 1 години машинного часу ПК, грн./година.

Вартість 1 години машинного часу ПК визначається за формулою:

$$C_{\text{мч}} = P \cdot C_e + \frac{Ф_{зал} \cdot H_a}{F_p} + \frac{K_{лпз} \cdot H_{апз}}{F_p} = 0.4 \cdot 1.68 + \frac{4500 \cdot 0.1}{1920} = 0.8, \text{ грн/год}, \qquad (3.12)$$

де Р – встановлена потужність ПК, 0.4 кВт;

$С_е$ – тариф на електричну енергію, 1.68 грн/кВт·година;

$Ф_{перв}$– первісна вартість ПК на початок року, 4500 грн.;

$Н_а$ – річна норма амортизації на ПК, 0.1 частки одиниці;

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

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

$F_р$ – річний фонд робочого часу (за 40-годинного робочого тижня $F_р$ = 1920 год).

Отже:

$$К_{пз} = 1375 + 9 = 1384 \text{ грн}$$

Таким чином, капітальні (фіксовані) витрати на проектування та впровадження проектного варіанта системи інформаційної безпеки складають:

$$К = К_{пз} + К_{аз} + К_{навч} + К_{н}, \text{ тис. грн} \qquad (3.13)$$

де $К_{пз}$ – вартість створення програмного продукту, тис. грн;

$К_{аз}$ – вартість закупівлі апаратного забезпечення та допоміжних матеріалів, тис. грн;

$К_{навч}$ – витрати на навчання технічних фахівців і обслуговуючого персоналу, тис. грн;

$К_{н}$ – витрати на встановлення обладнання та налагодження системи інформаційної безпеки, тис. грн.

Таблиця 3.1 Вартість закупівлі апаратного забезпечення

Назва комплектуючих	Вартість грн.
Процесор: Intel Celeron G3900 зі вбудовану графікою Intel HD 510	1100
Системна плата: MSI H110M PRO-VD	1500
ОЗУ для Intel: Samsung DDR4 4GB 2133Mhz (M378A5143EB1-CPB)	800
Жесткий диск: Western Digital WD3200AAJS	500
Корпус з блоком живлення: Frime FC-004B 400W	600
Разом	4500

$К_{аз}$ = 4500 грн.

Витрати на навчання технічних фахівців і обслуговуючого персоналу, це є підготовчі курси з адміністрування та обслуговування системи виявлення вторгнень що складають 6 тис. грн; $К_{навч}$ = 6000 грн.

Витрати на встановлення обладнання та налагодження системи інформаційної безпеки складають, 0.5 тис. грн. $К_{н}$ = 3000 грн.

К = 1384 + 4500 + 3 + 3 = 11884 грн.

3.2 Експлуатаційні витрати:

$$С_к = С_н + С_а + С_з + С_{ел} + С_{тос} \quad (3.14)$$

де витрати на навчання адміністративного персоналу й кінцевих користувачів($С_н$). визначаються за даними організації з проведення тренінгів персоналу, курсів підвищення кваліфікації – 3 тис. грн.

Річний фонд амортизаційних відрахувань ($С_а$) визначається у відсотках від суми капітальних інвестицій за видами основних фондів і нематеріальних активів (ПЗ) – 20% або 922 грн.

Річний фонд заробітної плати інженерно-технічного персоналу, що обслуговує систему інформаційної безпеки ($С_з$), складає:

$$С_з = З_{осн} + З_{дод} = 12000 \cdot 12 + 12000 \cdot 0.22 \cdot 12 = 175680 \text{ грн.} \quad (3.15)$$

де $З_{осн}$, $З_{дод}$ – основна середня заробітна плата на 01.12.2017, грн на рік.

Единий соціальний внесок – 0.22, частки одиниці;

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

$$С_{ел} = Р \cdot F_р \cdot Ц_е = 0.4 \cdot 365 \cdot 24 \cdot 1.68 = 3\,433 \text{ грн,} \quad (3.16)$$

де Р – встановлена потужність апаратури інформаційної безпеки, кВт;

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

$Ц_е$ – тариф на електроенергію, грн/кВт·годин.

Витрати на технічне й організаційне адміністрування та сервіс системи виявлення вторгнень визначаються у відсотках від вартості капітальних витрат 2%. А саме:

$$С_{тос} = К \cdot 0.2 = 2376 \text{ грн}$$

$$Ск = 3 + 0.922 + 175.680 + 3.433 + 2.376 = 185411. \text{ грн.}$$

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

Кінцевим результатом впровадження й проведення заходів щодо забезпечення інформаційної безпеки є величина відвернених втрат, що розраховується, виходячи з імовірності виникнення інциденту інформаційної безпеки й можливих економічних втрат від нього. По суті, ця величина відображає ту частину прибутку, що могла бути втрачена.

Загалом можливо виділити такі види збитку, що можуть вплинути на ефективність комп'ютерної системи інформаційної безпеки (КСІБ):

− порушення конфіденційності ресурсів КСІБ (тобто неможливість доступу до них неавторизованих суб'єктів або несанкціонованого використання каналів зв'язку);

− порушення доступності ресурсів КСІБ (тобто можливість доступу до них авторизованих суб'єктів (завжди, коли їм це потрібно);

− порушення цілісності ресурсів КСІБ (тобто їхня неушкодженість);

− порушення автентичності ресурсів КСІБ (тобто їхньої дійсності, непідробленості).

Вихідні дані:

$t_п$ =30 годин – час простою вузла або сегмента корпоративної мережі внаслідок атаки, годин;

$t_в$=12 годин – час відновлення після атаки персоналом, що обслуговує корпоративну мережу, годин;

$t_{ви}$=8 годин – час повторного введення загубленої інформації співробітниками атакованого вузла або сегмента корпоративної мережі, годин;

$З_о$=6000 грн – місячна заробітна плата обслуговуючого персоналу (адміністраторів та ін.) з нарахуванням єдиного соціального внеску, грн на місяць;

$З_с$ =5000 грн – місячна заробітна плата співробітника атакованого вузла або сегмента корпоративної мережі з нарахуванням єдиного соціального внеску, грн на місяць;

$Ч_о$=2 – чисельність обслуговуючого персоналу (адміністраторів та ін.), осіб.;

$Ч_с$=3 – чисельність співробітників атакованого вузла або сегмента корпоративної мережі, осіб.;

О = 150 000 грн – обсяг чистого прибутку/дохід від реалізації/ атакованого вузла або сегмента корпоративної мережі, грн у рік, або оподаткований прибуток атакованого вузла або сегмента корпоративної мережі;

$П_{зч}$ = 2000 грн – вартість заміни встаткування або запасних частин, грн;

I=1 – число атакованих вузлів або сегментів корпоративної мережі;

N = 30 – середнє число можливих атак на рік.

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

$$U = П_п + П_в + V, \text{ грн.} \qquad (3.17)$$

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

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

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

Втрати від зниження продуктивності 3 співробітників з ЗП атакованого вузла або сегмента корпоративної мережі являють собою втрати їхньої заробітної плати (оплата непродуктивної праці) за 30 годин простою внаслідок атаки:

$$П_п = \frac{\sum З_с * Ч_с}{F} \cdot t_п \ , \qquad (3.16)$$

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

$$П_п = \frac{\sum 5000 \cdot 3}{160} \cdot 30 = 2810 \text{ грн.}$$

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

$$П_в = П_{ви} + П_{пв} + П_{зч}, \text{ грн.}$$

(3.17)

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

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

$П_{зч}$ – вартість заміни устаткування або запасних частин, грн.

Витрати на повторне введення інформації $П_{ви}$ розраховуються виходячи з розміру заробітної плати 5000 грн 3 співробітників атакованого вузла або сегмента корпоративної мережі $З_с$, які зайняті повторним введенням втраченої інформації, з урахуванням необхідного для цього часу $t_{ви}$=8:

$$П_{ви} = \frac{\sum 5000 \cdot 3}{160} \cdot 30 = 2810 \text{ грн.} \quad (3.18)$$

Витрати на відновлення вузла або сегмента корпоративної мережі $П_{пв}$ визначаються часом відновлення після атаки $t_в$ = 12 і розміром середньогодинної заробітної плати обслуговуючого персоналу (адміністраторів):

$$П_{пв} = \frac{\sum 6000 \cdot 2}{160} \cdot 12 = 900 \text{ грн.} \quad (3.19)$$

$$П_в = 2810 + 900 + 2000 = 5710 \text{ грн.}$$

Втрати від зниження очікуваного обсягу продаж в 150 000 грн за 30 годин простою атакованого вузла або сегмента корпоративної мережі виходячи із середньогодинного обсягу продажів і сумарного часу простою атакованого вузла або сегмента корпоративної мережі:

$$V = \frac{O}{F_г} \cdot (t_п + t_в + t_{ви}) = \frac{150000}{8760} \cdot (30 + 12 + 8) = 850 \text{ грн}, \quad (3.20)$$

де $F_г$ – річний фонд часу роботи організації (прийом заказів інтернет-магазином) становить близько 8760 ч.

$$U = П_п + П_в + V = 2810 + 5710 + 850 = 9370 \text{ грн.}$$

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

$$B = \sum\sum U * N * I = 9370 \cdot 30 \cdot 1 = 281100 \text{ грн.} \quad (3.21)$$

3.4 Загальний ефект від впровадження системи інформаційної безпеки

Загальний ефект від впровадження системи інформаційної безпеки визначається з урахуванням ризиків порушення інформаційної безпеки і становить:

$$E = B \cdot R - C = 281100 \cdot 0 - 185411 = 39469 \text{ грн}, \quad (3.22)$$

де B – загальний збиток від атаки на вузол або сегмент корпоративної мережі, грн;

R – очікувана імовірність атаки на вузол або сегмент корпоративної мережі, частки одиниці;

C – щорічні витрати на експлуатацію системи інформаційної безпеки, тис. грн.

Визначення та аналіз показників економічної ефективності системи інформаційної безпеки

Коефіцієнт повернення інвестицій ROSI:

$$ROSI = \frac{E}{K} = \frac{39469}{11884} = 3{,}3, \text{ частки одиниці}, \quad (3.23)$$

де E – загальний ефект від впровадження системи інформаційної безпеки, грн;

K – капітальні інвестиції за варіантами, що забезпечили цей ефект, грн.

Термін окупності:

$$T_o = \frac{K}{E} = \frac{1}{ROSI} = \frac{1}{3{,}3} = 0.3 \text{ років.} \quad (3.24)$$

3.5 Висновок

Розробка і впровадження системи виявлення вторгнень для інтернет магазину «Parfum.ua» є економічно доцільним, так як витрати на її створення значно менші за суму збитків, завдяки не дорогій системи та мінімальній вартості комплектуючих необхідних для відновлення системи та її інформаційних ресурсів у разі успішних атак порушників. При цьому ми маємо:

- Капітальні витрати склали : К = 11884 (грн.);
- Поточні витрати склали : С = 185411 (грн.);
- Величина можливого збитку: $B = 281100$ (грн.);
- Загальний ефект від впровадження системи: Е = 33469 (грн.);
- Рентабельність інвестицій у безпеку складає: ROSI = 3,3 (частки одиниці);
- Термін окупності капітальних інвестицій T_o = 0,3 (роки).

ВИСНОВКИ

Під час виконання дипломної роботи проаналізовано різновиди та структуру системи виявлення вторгнень , обґрунтовано корисність створення на підприємствах.

Також проведений аналіз системи виявлення вторгнень, існуючих систем виявлення вторгнень, приведена статистика та класифікація мережевих атак, проведено опис існуючих систем виявлення вторгнень.

Підсумком проведеної роботи є створення системи виявлення вторгнень на основі алгоритму k-найближчих сусідів, та проведено порівняння створеної системи із системою Snort.

В економічному розділі проведено розрахунок витрат на створення, впровадження, обслуговування, та терміну окупності системи виявлення вторгнень, визначання збитків від реалізації загроз.

СПИСОК ВИКОРИСТАНОЇ ЛІТЕРАТУРИ

1. Классификация сетевых атак [Електронний ресурс]. – Режим доступу : http://www.internet-technologies.ru/articles/article_237.html
2. Как хакеры атакуют веб-приложения: боты и простые уязвимости [Електронний ресурс]. – Режим доступу : https://www.securitylab.ru/analytics/485977.php
3. Debra Anderson, Teresa F. Lunt, Harold Javitz, Ann Tamaru, and Alfonso Valdes, “Detecting unusual program behavior using the statistical component of the next generation intrusion detection system (NIDES)”. // Technical Report SRI-CSL-95-06, Computer Science Laboratory, SRI International, Menlo Park, CA, USA, May 2016
4. Y. Frank Jou, Fengmin Gong, Chandru Sargor, Shyhtsun FelixWu, and CleavelandW Rance, “Architecture design of a scalable intrusion detection system for the emerging network infrastructure.” // Technical Report CDRL A005, Dept. of Computer Science, North Carolina State University, Releigh, N.C, USA, April 2015
5. Р.Л. Смелянский, А.И. Качалин. “Применения нейросетей для обнаружения аномального поведения объектов в компьютерных сетях”. // Факультет Вычислительной Математики и Кибернетики, МГУ им. М. В. Ломоносова, Москва, 2014
6. S.A. Hofmeyr, An immunological model of distributed detection and its application to computer security. // Ph.D. thesis, University of New Mexico, May 1999
7. Sebring, M., Shellhouse, E., Hanna, M. & Whitehurst, R. Expert Systems in Intrusion Detection: A Case Study. // Proceedings of the 11th National Computer Security Conference, 2009
8. Ahmed Awad E. Ahmed, Issa Traore, “Anomaly Intrusion Detection based on Biometrics.” // Proceedings of the 2005 IEEE, Workshop on Information Assurance, United States Military Academy, West Point, NY June 2010
9. Srinivas Mukkamala, Andrew H. Sung, Ajith Abraham, “Intrusion detection using an ensemble of intelligent paradigms.” // Journal of Network and Computer Applications, 2015

10. Anderson, James P., "Computer Security Threat Monitoring and Surveillance, " Washing, PA, James P. Anderson Co., 1980.

11. Denning, Dorothy E., "An Intrusion Detection Model, " Proceedings of the Seventh IEEE Symposium on Security and Privacy, May 1986, pages 119—131

12. Lunt, Teresa F., "IDES: An Intelligent System for Detecting Intruders, " Proceedings of the Symposium on Computer Security; Threats, and Countermeasures; Rome, Italy, November 22-23, 1990, pages 110—121.

13. Lunt, Teresa F., "Detecting Intruders in Computer Systems, " 1993 Conference on Auditing and Computer Technology, SRI International

14. Sebring, Michael M., and Whitehurst, R. Alan., "Expert Systems in Intrusion Detection: A Case Study, " The 11th National Computer Security Conference, October, 1988

15. Smaha, Stephen E., "Haystack: An Intrusion Detection System, " The Fourth Aerospace Computer Security Applications Conference, Orlando, FL, December, 1988

16. Vaccaro, H.S., and Liepins, G.E., "Detection of Anomalous Computer Session Activity, " The 1989 IEEE Symposium on Security and Privacy, May, 1989

17. Teng, Henry S., Chen, Kaihu, and Lu, Stephen C-Y, "Adaptive Real-time Anomaly Detection Using Inductively Generated Sequential Patterns, " 1990 IEEE Symposium on Security and Privacy

18. Heberlein, L. Todd, Dias, Gihan V., Levitt, Karl N., Mukherjee, Biswanath, Wood, Jeff, and Wolber, David, "A Network Security Monitor, " 1990 Symposium on Research in Security and Privacy, Oakland, CA, pages 296—304

19. Winkeler, J.R., "A UNIX Prototype for Intrusion and Anomaly Detection in Secure Networks, " The Thirteenth National Computer Security Conference, Washington, DC., pages 115—124, 1990

20. Dowell, Cheri, and Ramstedt, Paul, "The ComputerWatch Data Reduction Tool, " Proceedings of the 13th National Computer Security Conference, Washington, D.C., 1990

21. Howell D. Hackers often choose their corporate targets. // Investors Business Daily. — January 30,2012.

22. Про інформацію [Електронний ресурс]. – Режим доступу : http://zakon3.rada.gov.ua/laws/show/2657-12

23. Закон про державну таємницю [Електронний ресурс]. – Режим доступу : http://zakon3.rada.gov.ua/laws/show/3855-12

24. Про захист персональних даних [Електронний ресурс]. – Режим доступу : http://zakon3.rada.gov.ua/laws/show/2297-17

25. Лукацкий А. В. Новые подходы к обеспечению информационной безопасности сети. 2002.

26. Зотова Т. Сплоченная команда профессионалов главный гарант ИТ-безопасности. // Сетевой. — 2014. — №5

27. FAQ: Network Intrusion Detection Systems. Windows Security. Access : http://www.secinf.net/intrusion detection/FAQ Network Intrusion Detection Systemshtml

28. Schwartz M. New Technology Combats Zero-Day Attacks. August 2014.

29. Игнатьев В. Очередная веская причина задуматься о переходе с ОС Windows на альтернативу. // Системный администратор. 2013. - №9(10).

30. Польская исследовательская группа «Last Stage of Delirium», [Електронний ресурс]. – Режим доступу : http://www.lsd-pl.net.

31. Hollander Y., Agostini R. Stop Hacker Attacks at the OS Level. // Internet Security Advisor Magazine. September/October 2010.

32. Mell P., Ни V., Lippmann R., Haines J., Zissman M. An Overview of Issues in Testing Intrusion Detection Systems. / В сб. материалов National Institute of Standards and Technology. July 2013.

33. Scarfone, Karen; "Guide to Intrusion Detection and Prevention Systems (IDPS)" / Scarfone, Karen, Mell, Peter. Computer Security Resource, Austin, 2007.

34. Mattord, Verma; "Principles of Information Security." / Verma Mattord, 300p, 2008

35. Sen, Sevil; "Power-Aware Intrusion Detection in Mobile Ad Hoc Networks" / Sevil Sen, John E. Clark, Juan Tapaidor, York , 2006 Access: http://www-users.cs.york.ac.uk/~jac/PublishedPapers/AdhocNetsFinal.pdf

36. Аудит и мониторинг сети. Адаптивное управление безопасностью. [Електронний ресурс]. – Режим доступу : http://www.isecuritv.ru/technologies/audit.php.

37. Anderson, Ross; Security Engineering: A Guide to Building Dependable Distributed Systems./ Ross Anderson, New York: pp. 387–388., 2007

38. Лукацкий, Алексей, "Предотвращение сетевых атак, технологии и и решения" / Алексей Лукацкий, Москва , 2006

39. Kholidy, H.A., Baiardi, F.: CIDS: a framework for intrusion detection in cloud system. In: Ninth International Conference on Information Technology—New Generations, pp. 379–385. IEEE Computer Society (2012)

40. Al-Janabi, S.T.F., Saeed, H.A.: A neural network based anomaly intrusion detection system. In: IEEE Computer Society, pp. 221–226 (2011)

41. Mazzariello, C., Bifulco, R., Canonico, R.: Integrating a network IDS into an open source computing environment. In: Sixth International Conference on Information Assurance and Security (IAS), pp. 265–270. IEEE Publisher, Atlanta, GA (2010)

42. Bakshi, A., Yogesh, B.: Securing cloud from DDOS Attacks using Intrusion detection system in virtual machine. In: Second International Conference on Communication Software and Networks, IEEE Computer Society, pp. 260–264 (2010)

43. Ghali, N.I.: Feature selection for effective anomaly-based intrusion detection. Int. J. Comput. Sci. Netw. Secur. (IJCSNS) 9, 285–289 (2009)

44. Tavallaee, M., Bagheri, E., Lu, W., Ghorbani, A.A.: A detailed analysis of the KDD Cup 99 data set. In: Proceedings of the IEEE Symposium on Computational Intelligence in Security and Defense Application (CISDA). pp. 53–58. IEEE Publisher (2009)

45. Sourcefire. Inc. Snort Users Manual 2.9.2 [Електронний ресурс]. – Режим доступу : http://www.snort.org/assets/166/snort_manual.pdf

46. Mattord H., Whitman M. Principles of Information Security // Course Technology. – 2008. – P. 290–301.

ДОДАТОК А. Перелік документів на оптичному носії

01 Титульна сторінка.doc

02 Зміст.doc

03 Список умовних скорочень.doc

04 Реферат.doc

05 Вступ.doc

06 Стан питання, постановка задачи.doc

07 Спеціальний розділ.doc

08 Економ розділ.doc

09 Висновки.doc

10 Список використаної літератури.doc

11 Додаток А.doc

12 Додаток Б.doc

13 Презентація.pptx

ДОДАТОК Б. Відгуки керівників розділів

Б.1 Відгук керівника економічного розділу

Керівник розділу _____ к.е.н.,доц.Волотковська Ю.О.
(підпис) (ініціали, прізвище)