**МІНІСТЕРСТВО ОСВІТИ ТА НАУКИ УКРАЇНИ**

ДЕРЖАВНИЙ УНІВЕРСИТЕТ ТЕЛЕКОМУНІКАЦІЙ

Навчально-науковий інститут захисту інформації

На рецензiю

Зав. Кафедрою УІКБ доктор економічних наук, доцент

\_\_\_\_\_\_\_\_\_\_\_\_\_\_ С.В. Легомiнова

\_\_\_\_ \_\_\_\_\_\_\_\_\_\_\_\_\_ 2020р.

До захисту

Зав. Кафедрою УІКБ доктор економічних наук, доцент

\_\_\_\_\_\_\_\_\_\_\_\_\_\_ С.В. Легомiнова \_\_\_\_ \_\_\_\_\_\_\_\_\_\_\_\_\_ 2020р.

**ДИПЛОМНА РОБОТА**

на тему:

**Методичнi пiдходи до аналiзу систем виявлення мережевих вторгнень і виявлення ознак комп'ютерних атак**

|  |  |
| --- | --- |
| СТУДЕНТ:Поляков Дмитро Андрійович | \_\_\_\_\_\_\_\_\_ |
|  | (підпис) |
| КЕРІВНИК:      к. в. н., доцент Якименко Юрій Михайлович | \_\_\_\_\_\_\_\_\_\_ |
|  | (підпис) |
| НОРМОКОНТРОЛЕР: к.т.н., с.н.с Щебланін Юрій Миколайович | \_\_\_\_\_\_\_\_\_\_ |
|  | (підпис) |

Київ – 2020

ДЕРЖАВНИЙ УНІВЕРСИТЕТ ТЕЛЕКОМУНІКАЦІЙ

Навчально-науковий інститут захисту інформації

Кафедра управління інформаційною та кібернетичною безпекою

Освітньо-кваліфікаційних рівень – бакалавр

Спеціальність «Кібербезпека»

Спеціалізація «Управління інформаційною безпекою»

"ЗАТВЕРДЖУЮ"

Завідувач кафедри УІКБ

\_\_\_\_\_\_\_\_\_\_ С.В.Легомінова

(підпис)

“\_\_\_”\_\_\_\_\_\_\_\_\_\_\_\_\_\_ 2020 р.

**ЗАВДАННЯ**

**НА ДИПЛОМНУ РОБОТУ СТУДЕНТУ**

**Полякову Дмитрові Андрійовичу**

1.**Тема роботи** “ Методичнi пiдходи до аналiзу систем виявлення мережевих вторгнень і виявлення ознак комп'ютерних атак ”, керівник Якименко Юрій Михайлович, к. в. н., доцент, затверджена наказом по університету від “16” березня 2020 р. № 81.

2. **Термін здачі** студентом оформленої роботи “2”червня 2020 р.

**3.Об’єкт дослідження:** процес захисту інформації та впровадження системи виявлення мережевих вторгнень і виявлення ознак комп'ютерних атак на підприємстві.

**4. Предмет дослідження:** методичні підходи впровадження системи виявлення мережевих вторгнень і виявлення ознак комп'ютерних атак на прикладі побудови надійної системи захисту інформації підприємства.

**5.Мета дослідження:** аналіз використання можливостей систем виявлення мережевих вторгнень та ознак комп’ютерних атак в забезпеченні захисту інформації підприємства.

**6.Перелік питань, які мають бути розроблені:**

- проаналізувати види мережевих вторгнень і ознаки сучасних комп'ютерних атак та досвід використання систем їх виявлення на підприємстві;

- проаналізувати можливості сучасних систем виявлення мережевих вторгнень та підходи до їх вдосконалення;

- розгянути методичнi пiдходи щодо використання систем виявлення мережевих вторгнень і виявлення ознак комп'ютерних атак на підприємстві;

- на основі запропонованої методики провести дослідження та розробити

рекомендації щодо побудови систем виявлення мережевих вторгнень і виявлення ознак комп'ютерних атак для підприємства на прикладі.

7. **Перелік графічного матеріалу**:

* типові схеми щодо систем виявлення мережевих вторгнень і виявлення ознак комп’ютерних атак;
* презентація доповіді, виконана в Microsoft PowerPoint.

**8. Дата видачі завдання** «22» лютого 2020 р.

**Календарний план**

|  |  |  |  |
| --- | --- | --- | --- |
| № з/п | Назва етапів бакалаврської роботи | Строк виконання  етапів | Примітка |
| 1 | 2 | 3 | 4 |
|  | Уточнення постановки завдання. | 23.03.2020 |  |
|  | Підбір і аналіз науково-технічної літератури. | 6.04.2020 |  |
|  | Аналіз та систематизація матеріалу. Обґрунтування вибору рішення. | 20.04.2020 |  |
|  | Аналiз сучасних систем виявлення та запобiгання мережевих вторгнень | 27.04.2020 |  |
|  | Основні методичні підходи щодо використання систем виявлення мережевих вторгнень і виявлення ознак комп'ютерних атак на підприємстві | 06.05.2020 |  |
|  | Проведення дослідження та розробка рекомендацій щодо вдосконалення систем виявлення мережевих вторгнень і виявлення ознак комп'ютерних атак для підприємства (на прикладі). | 18.05.2020 |  |
|  | Апробація роботи на науково-методичному семінарі. | 04-05.2020 |  |
|  | Оформлення та друк дипломної роботи. | 28.05.2020 |  |
|  | Підготовка демонстраційного матеріалу, оформлення презентації. | 2.06.2020 |  |
|  | Отримання відгука та рецензії на роботу. | 29.05.2020 |  |
|  | Попередній захист на кафедрі. | 2.06.2020 |  |
|  | Захист в ДЕК. | 10.06.2020 |  |

Студент \_\_\_\_\_\_\_\_\_\_\_\_\_ Поляков Дмитро Андрійович

(підпис) (прізвище, ім’я, по-батькові)

Керівник \_\_\_\_\_\_\_\_\_\_\_\_\_\_ Якименко Юрій Михайлович

(підпис) (прізвище, ім’я, по-батькові)

**РЕФЕРАТ**

Дипломна робота присвячена дослідженню методичних пiдходів до аналiзу систем виявлення мережевих вторгнень і виявлення ознак комп'ютерних атак. Робота складається зі переліку умовних позначень та скорочень, вступу, трьох розділів, висновків та списку використаних джерел. Загальний обсяг роботи становить 65 аркушів.

**Об’єктом дослідження** в роботі є процес захисту інформації та впровадження системи виявлення мережевих вторгнень і виявлення ознак комп'ютерних атак на підприємстві на прикладі **компанії «Sitronics Telecom Solutions Ukraine»**.

**Метою роботи –** є підвищення рівня захищеності СВВ за рахунок оптимального використання ресурсів системи. Для цього у роботі використовуються методи теорії інформаційної безпеки, теорії управління інформаційною безпекою, теорії захисту від мережевих вторгнень та виявлення ознак комп’ютерних атак.

Як результат у роботі проведено аналіз засобів виявлення вторгнень в інформаційну систему, аналіз можливих дій зі сторони зловмисників за допомогою методичних підходів, а також методи впливу вірусних програм та протидії такому впливу, досліджено методи та принципи встановлення оптимальної СВВ, розглянуто моделі та їх можливості для можливого подальшого встановлення їх в систему захисту інформації.

Запропоновані методи та системи можуть бути використані при плануванні та побудови системи виявлення вторгнень для організації.

**Галузь застосування.** Матеріали та результати роботи можуть бути використані при проектуванні та подальшому розгортанні надійної СВВ та оптимального вибору засобів для її комплектування в інформаційно-комунікаційній системі підприємства.

**Ключові слова:** ІНФОРМАЦІЙНА БЕЗПЕКА, СИСТЕМИ ВИЯВЛЕННЯ ВТОРГНЕНЬ, МЕРЕЖА, ЗАГРОЗИ, ЗЛОВМИСНИК, ІНФОРМАЦІЯ, ЗАХИСТ, ІНФОРМАЦІЙНА СИСТЕМА, АТАКА.

|  |  |  |
| --- | --- | --- |
| **ЗМІСТ** | | Стор. |
| ПЕРЕЛІК УМОВНИХ ПОЗНАЧЕНЬ І СКОРОЧЕНЬ………………..... | | 8 |
| ВСТУП……………………………………………………………..…….... | | 9 |
| Розділ 1 | АНАЛIЗ СУЧАСНИХ СИСТЕМ ВИЯВЛЕННЯ ТА ЗАПОБIГАННЯ МЕРЕЖЕВИХ ВТОРГНЕНЬ ………..…. | 12 |
| 1.1 | Види мережевих вторгнень і ознаки сучасних комп'ютерних атак та досвід використання систем їх виявлення на підприємстві …..………………………………. | 12 |
| 1.2 | Можливості сучасних систем виявлення мережевих вторгнень та підходи до їх вдосконалення...... …………….. | 19 |
| Висновки до першого розділу……………...……………………………. | | 22 |
| Розділ 2 | ОСНОВНІ МЕТОДИЧНІ ПІДХОДИ ЩОДО ВИКОРИСТАННЯ СИСТЕМ ВИЯВЛЕННЯ МЕРЕЖЕВИХ ВТОРГНЕНЬ І ВИЯВЛЕННЯ ОЗНАК КОМП'ЮТЕРНИХ АТАК НА ПІДПРИЄМСТВІ…………..................................... | 23 |
| 2.1 | Аналіз захисту інформації від комп'ютерних атак …........... | 23 |
| 2.1.1 | Класифікація атак, види, ознаки та механізми їх реалізації…………..……………………………………..……. | 28 |
| 2.1.2 | Сучасні методи виявлення атак ……………………..……… | 35 |
| 2.2 | Організаційні та технічні підходи до розробки систем виявлення мережевих вторгнень і виявлення ознак комп'ютерних атак …………………………………………… | 38 |
| 2.3 | Розробка методики використання систем виявлення мережевих вторгнень і виявлення ознак комп'ютерних атак | 43 |
| Висновки до другого розділу………………………...……....................... | | 51 |
| Розділ 3 | ПРОВЕДЕННЯ ДОСЛІДЖЕННЯ ТА РОЗРОБКА РЕКОМЕНДАЦІЙ ЩОДО ВДОСКОНАЛЕННЯ СИСТЕМ ВИЯВЛЕННЯ МЕРЕЖЕВИХ ВТОРГНЕНЬ І ВИЯВЛЕННЯ ОЗНАК КОМП'ЮТЕРНИХ АТАК ДЛЯ ПІДПРИЄМСТВА ……………..……….…………………….. | 53 |
| 3.1 | Проведення дослідження компанії «Sitronics Telecom Solutions Ukraine (STSU)»…………………………………… | 54 |
| 3.2 | Рекомендації щодо вдосконалення систем виявлення мережевих вторгнень і виявлення ознак комп’ютерних атак…………………………………………………………….. | 57 |
| Висновки до третього розділу……………………...……......................... | | 61 |
| ВИСНОВКИ……………………………………………………….......….. | | 62 |
| СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ………………………...………. | | 64 |

**ПЕРЕЛІК УМОВНИХ ПОЗНАЧЕНЬ І СКОРОЧЕНЬ**

|  |  |
| --- | --- |
| IPS | – Intrusion Prevention System |
| IDS | – Intrusion Detection System |
| DMZ | –Demilitarized Zone |
| MIB | – Management Information Base |
| АС | – Автоматизована система |
| ДТЗС | – Допоміжні технічні засоби і системи |
| ІБ | – Інформаційна безпека |
| ІС | – Інформаційна система |
| КА | – Комп’ютерна атака |
| ЛОМ | – Локальна обчислювальна мережа |
| МЕ | – Мережевий екран |
| МСВВ | – Мережева система виявлення вторгнень |
| ОС | – Операційна система |
| ПБ | – Платформа безпеки |
| ПЗ | – Програмне забезпечення |
| ПК | – Персональний комп’ютер |
| СВА | – Система виявлення атак |
| СВВ | – Система виявлення вторгнень |
| СЗІ | – Системи захисту інформації |
| ТЗПІ | – Технічні засоби передачі інформації |

**ВСТУП**

**А к т у а л ь н і с т ь т е м и.** В наш час Інтернет розвивається дуже швидко, що зумовлює перехід на електронні форми зберігання і передачі інформації, активне впровадження в повсякденне життя електронних форм платежів і багато іншого.

Разом з цим розвивається і змінюється кіберзлочинність, тому за останні 30 років багато речей встигли розвинутися і практично зникнути. Десять -двадцять років тому кіберзлочинність у більшості випадків була “кібервандалізмом” (сайти знищували просто заради того, щоб комусь щось довести). А зараз більшість злочинів в Інтернеті — економічно мотивована. Так само злочинність еволюціонувала від дій одиноких аматорів та груп “одного дня” до багатошарових структур, дії кожного з прошарків яких несуть реальну небезпеку.

Члени організованих угруповань можуть користуватися програмним забезпеченням «державних» хакерів, а «державні» хакери попутно можуть викрадати гроші з банків держави, проти якої йде спецоперація. А якщо інструментарій один раз виклали в мережу, то ним починає користуватися вся спільнота, від професіоналів високого рівня до “скріпткідді”. Все це піднімає ціну кібербезпеки для бізнесу — як і в випадку інших злочинів, подолання наслідків зламів обходиться значно дорожче, ніж їхнє попередження чи навіть те, що злодії можуть вкрасти (а якщо порівняти ціну виконання таких дій із ціною подолання наслідків, то тут різниця, як мінімум, у два порядки).

Найбільше шкідливих кампаній з використанням теми коронавіруса прийшло з Китаю. Перша з двох атак сталася на початку березня. В'єтнамська фірма з кібербезпеки VinCSS виявила, що злочинна група Mustang Panda поширює електронні листи з шкідливим файлом RAR, нібито призначеним для передачі повідомлення про спалах коронавіруса від прем'єр-міністра В'єтнаму[ 1].

Компанія CheckPoint зафіксувала злочинну діяльність іншою китайською групи під назвою Vicious Panda. Зловмисники націлилися на урядові організації Монголії, відправляючи документи з інформацією про поширеність нових коронавірусних інфекцій[ 1].

Всі останні події та стрімкий розвиток Інтернету вплинули на те, що безпека мереж і мережевих сервісів стала дійсно нагальною проблемою практично кожного користувача, установи або підприємства. Тож пріоритетним завданням є проведення ефективного аналізу систем виявлення мережевих вторгнень і виявлення ознак комп'ютерних атак.

**М е т а і з а в д а н н я д о с л і д ж е н н я.Мета роботи** полягає в покращенні та підвищенні рівня захищеності інформаційних систем підприємства від мережевих вторгнень та комп’ютерних атак за рахунок оптимального використання ресурсів системи. Для досягнення цієї мети потрібно виконати такі **завдання:**

1. дослідити методологічні підходи до розробки та використання систем, а також головні функції та можливості системи;
2. зробити аналіз характеристик та досвіду з використанням систем виявлення мережевих вторгнень і виявлення ознак комп'ютерних атак на підприємстві;
3. провести дослідження та розробити рекомендації щодо впровадження системи виявлення мережевих вторгнень і виявлення ознак комп'ютерних атак на підприємстві.

Виходячи з цього, **об’єктом дослідження** у роботі є процес захисту інформації та впровадження системи виявлення мережевих вторгнень і виявлення ознак комп'ютерних атак на підприємстві на прикладі **компанії «Sitronics Telecom Solutions Ukraine»**. **Предмет дослідження** – засоби та методи захисту інформації в інформаційних системах (ІС) та рекомендації щодо впровадження системи виявлення мережевих вторгнень і виявлення ознак комп'ютерних атак на прикладі побудови надійної системи яку пропонує **компанія «Sitronics Telecom Solutions Ukraine»**.

**М е т о д и д о с л і д ж е н н я.** Для того щоб вирішити поставлені наукові завдання в роботі використані методи впровадження інформаційної безпеки, теорії управління інформаційною безпекою, теорії захисту від мережевих вторгнень та комп’ютерних атак.

**Н а у к о в а н о в и з н а о д е р ж а н и х р е з у л ь т а т і в.** Науково-обґрунтованими результатами, що отримані в роботі, є:

1. покращена технологія, яка застосовується для розробки рекомендацій щодо впровадження систем виявлення мережевих вторгнень і виявлення ознак комп'ютерних атак, що має на меті дослідити життєвий цикл захисту інформації в ІС;
2. покращена технологія прийняття рішення щодо раціональних та злагоджених дій при виборі засобів МСВВ, що дозволяє здійснювати обґрунтований вибір серед множини можливих засобів виявлення мережевих вторгнень та ознак комп’ютерних атак з метою її реалізації.

**П р а к т и ч н е з н а ч е н н я о д е р ж а н и х р е з у л ь т а т і в.** Наукові результати, отримані в роботі, у сукупності складають підґрунтя для розроблення системи виявлення мережевих вторгнень і виявлення ознак комп'ютерних атак для забезпечення потреб державних і комерційних організацій, а також підрозділів спеціального призначення.

**Апробація результатів дипломної роботи**. Основні наукові результати роботи доповідалися та обговорювалися на двох науково-технічних конференціях (НТК), а саме на:

1) Науково-технічна конференція «Актуальні проблеми інформаційної та кібернетичної безпеки», 26 жовтня 2018 року, ( м Київ, 2018. Державний університет телекомунікацій, ННІЗІ);

2) Науково-технічна конференція «Цифрова трансформація кібербезпеки» , 26 квітня 2020 року, ( м Київ, 2020. Державний університет телекомунікацій, ННІЗІ ).

**Публікації.** Основні наукові результати роботи відображені у двох тезах доповідей на НТК.

**Розділ 1**

**АНАЛIЗ СУЧАСНИХ СИСТЕМ ВИЯВЛЕННЯ ТА ЗАПОБIГАННЯ МЕРЕЖЕВИХ ВТОРГНЕНЬ**

Вторгнення в мережу стосується будь-якої несанкціонованої діяльності в цифровій мережі. Вторгнення в мережу часто передбачає крадіжку цінних мережевих ресурсів і майже завжди загрожує безпеці мереж та / або їх даних. Для того, щоб проактивно виявляти та реагувати на вторгнення в мережу, організації та підрозділи з кібербезпеки повинні мати глибоке розуміння того, як працюють вторгнення в мережу та впроваджувати системи вторгнення, виявлення та реагування на мережі, розроблені з використанням методів атаки та прихованих методів.

**1.1.Види мережевих вторгнень і ознаки сучасних комп'ютерних атак та досвід використання систем їх виявлення на підприємстві**

Зважаючи на кількість нормальної активності, яка постійно відбувається в цифрових мережах, визначити аномалії, які можуть вказувати на порушення мережі, може бути дуже важко. Нижче наведено декілька найбільш поширених мережевих вторгненнь, за якими організація повинна пильно стежити.

Атаки відмови в обслуговуванні (DoS) та розповсюджені атаки відмови в обслуговуванні (DDoS)

Атака відмови в обслуговуванні переповнює ресурси системи, тому вона не може відповідати на запити служби. Атака DDoS - це також атака на ресурси системи, але вона запускається з великої кількості інших хост-машин, заражених шкідливим програмним забезпеченням, керованим зловмисником.

На відміну від атак, розроблених для того, щоб зловмисник мав змогу отримати або збільшити доступ, відмова в наданні послуг не дає прямих переваг для нападників. Для деяких із них достатньо задовольнити відмову в обслуговуванні.

Однак якщо атакований ресурс належить бізнес-конкуренту, то користь для зловмисника може бути достатньо реальною. Іншою метою DoS-атаки може бути поставити системи в режим офлайн, щоб можна було запустити різного виду інші атаки. Одним із поширених прикладів є злом та викрадення важливих даних.

Існують різні типи **DoS і DDoS атак** (див.рис. 1.1); найпоширенішими є **атака повені TCP SYN атака, smurf атака, teardrop атака, атака пінг-смерті та ботнети.**

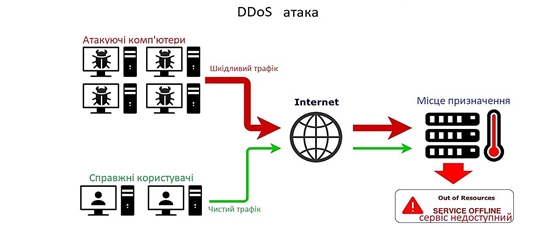


Рис.1.1. Приклад DDoS атаки

**TCP SYN атака**. У цьому нападі нападник експлуатує використання буферного простору під час сесії протоколу TCP. Пристрій нападника затоплює нечисленну незавершену чергу цільової системи запитами зв’язку, але на них не відповідає, коли цільова система відповідає на ті запити. Це викликає перерву зв`язку системи, очікуючи відповіді від пристрою нападника, яке змушує систему зупинитися чи стати непридатною, коли черга зв 'язку заповнюється.

Є кілька контрзаходів до нападу повені TCP SYN:

- сервери розміщати позаду налаштованого брандмауера, щоб зупинитипакети SYN;

- збільшити розмір черги зв 'язку та зменшити перерву на відкритих

зв' язках.

**Teardrop атака**. Цей напад змушує довжину і області фрагментації в послідовних пакетах InternetProtocol (IP) накладатися один на одного на хості нападу; система, що зазнала нападу намагається відновити пакети під час процесу, але зазнає невдачі. Цільова система тоді стає заплутаною і зупиняється.

Якщо користувачі не мають оновлень, щоб захиститися від цієї DoS-атаки, відключають SMBv2 і блокують порти 139 і 445.

**Smurf атака**. Цей напад включає використання IP спуфингу та ICMP, щоб насичувати мережу трафіком. Цей метод нападу використовує запити ICMP, призначені для міжмережевих повідомлень IP-адрес. Ці запити ICMP походять із адреси "жертви". Наприклад, якщо адреса жертви 10.0.0.10, нападник спрямував би запит ICMP від 10.0.0.10 до широкомовної адреси 10.255.255.255. Цей запит пішов би до всіх IP в діапазоні, з усіма відповідями, що поверталися би до 10.0.0.10, пригнічуючи та переповнюючи мережу. Цей процес повторюємо, і може бути автоматизований, щоб створити величезні «затори» в мережі.

Щоб захистити ваші пристрої від цього нападу, ви повинні відключити спрямовані на IP передачі в маршрутизаторах. Це запобігатиме запит ICMP мовлення в мережевих пристроях. Інший варіант полягає в тому, щоб налаштувати кінцеві системи, щоб перешкодити їм відповідати на пакети ICMP від широкомовного запиту.

**Атака пінг-смерті.** Цей тип нападу використовує IP пакети, щоб відправити пінг запити до системи з IP розміром пакетів більше 65,535 байтів. IP пакети цього розміру не дозволені, таким чином, нападник фрагментує IP пакет. Як тільки система повторно збирає пакет, вона може перенести буферне переповнення та інші аварії.Пінг смерті може бути заблокований за допомогою брандмауера, який перевірить фрагментовані IP пакети на максимальний розмір.

**Ботнети**. Ботнети - мільйони систем, заражені шкідливими програмами під контролем хакера, щоб виконувати DDoS-атаки. Ці боти або системи зомбі використовуються, щоб здійснити напади на системи, які переповнюють пропускна здатність системи і можливості обробки запитів. Ці DDoS-атаки важко простежити, тому що ботнети зазвичай розташовані різних географічних точках.

Ботнети можуть бути зупинені:

* Фільтрацією RFC3704, яка буде блокувати трафік від спуфінгових адрес і допоможе гарантувати, що трафік простежується до своєї правильної вихідної мережі. Наприклад, фільтрація RFC3704 виключить пакети з вільних ip адрес.
* Фільтрація чорної діри, яка блокує небажаний трафік, перш ніж він увійде в захищену мережу. Коли DDoS-атака виявлена, прикордонний міжмережевий протокол BGP (Border Gateway Protocol), хост повинен послати оновлення на напрямки маршрутизаторів постачальника послуг Інтернету так, щоб вони направили весь трафік, що прямує в сервери жертви до нульового інтерфейсу[12].

**Man-in-the-middle (MitM) атака.** Ця атака відбувається, коли хакер опиняється між комунікаціями сервера та клієнта. Ось деякі загальні типи таких атак:**викрадення сесії, спуфінг, фішинг атаки, підслуховування** (див. приклади атак на рис.1.2а і б. та рис.1.3)[11].

**Викрадення сесії**.У цьому типі атаки MitM нападник викрадає сесію між довіренним клієнтом і мережевим вузлом. Комп'ютер, що атакує замінює своїм IP - адресою клієнта, в той час як сервер продовжує сесію, вважаючи, що це спілкується з клієнтом. Атака може розвиватися так:

* Клієнт з'єднується з сервером.
* Комп'ютер нападника отримує контроль над клієнтом.
* Комп'ютер нападника роз'єднує клієнта від сервера.
* Комп 'ютер нападника замінює IP-адресу клієнта своїм власним IP – адресом і підроблює порядкові номери клієнта.
* Комп 'ютер нападника продовжує діалог із сервером, і сервер вважає, що це все ще спілкується з клієнтом[11].

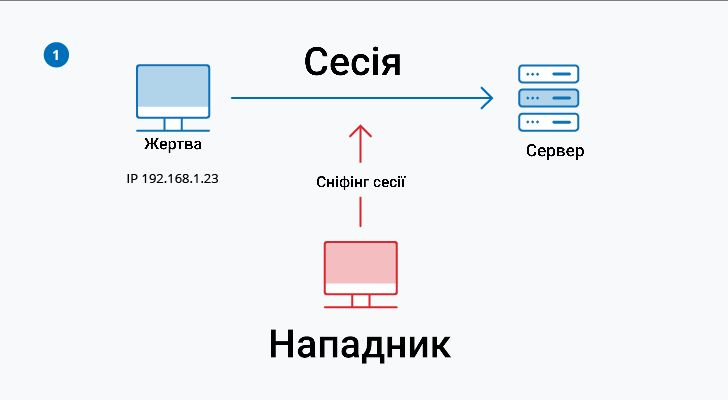


Рис. 1.2а.

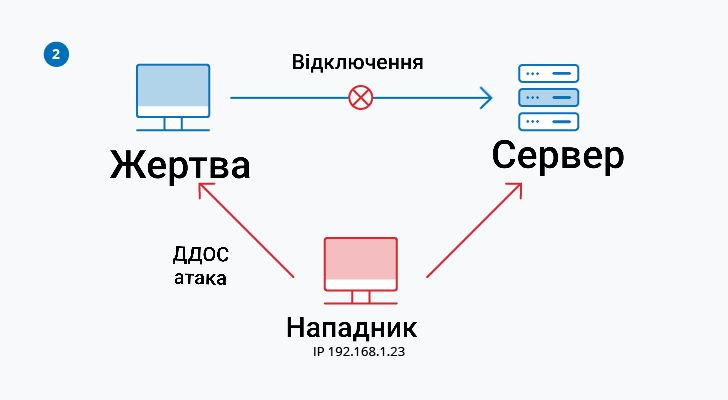


Рис. 1.2б.

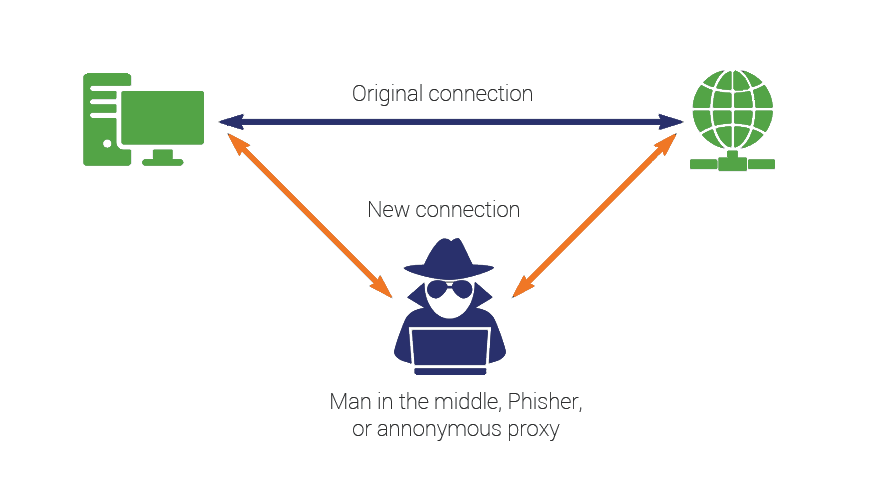


Рис. 1.3.

Рис.1.2(а і б). та рис.1.3. Приклади Man-in-the-middle (MitM) атаки

**Спуфінг**. При проведенні атак зловмисникові важливо не тільки досягти своєї мети, яка полягає в заподіянні шкоди атакованому об'єкту, але і знищити всі сліди своєї діяльності. Одним з основних прийомів, використовуваних зловмисниками для "замітання слідів", є підміна вмісту пакетів, або спуфінг (spoofing). Зокрема, для приховування місця знаходження джерела шкідливих пакетів зловмисник змінює значення поля адреси відправника в заголовках пакетів. Оскільки адреса відправника генерується автоматично системним програмним забезпеченням, зловмисник вносить зміни в відповідні програмні модулі так, щоб вони давали йому можливість відправляти  зі свого комп'ютера пакети з будь-якими IP-адресами (рис.1.4).

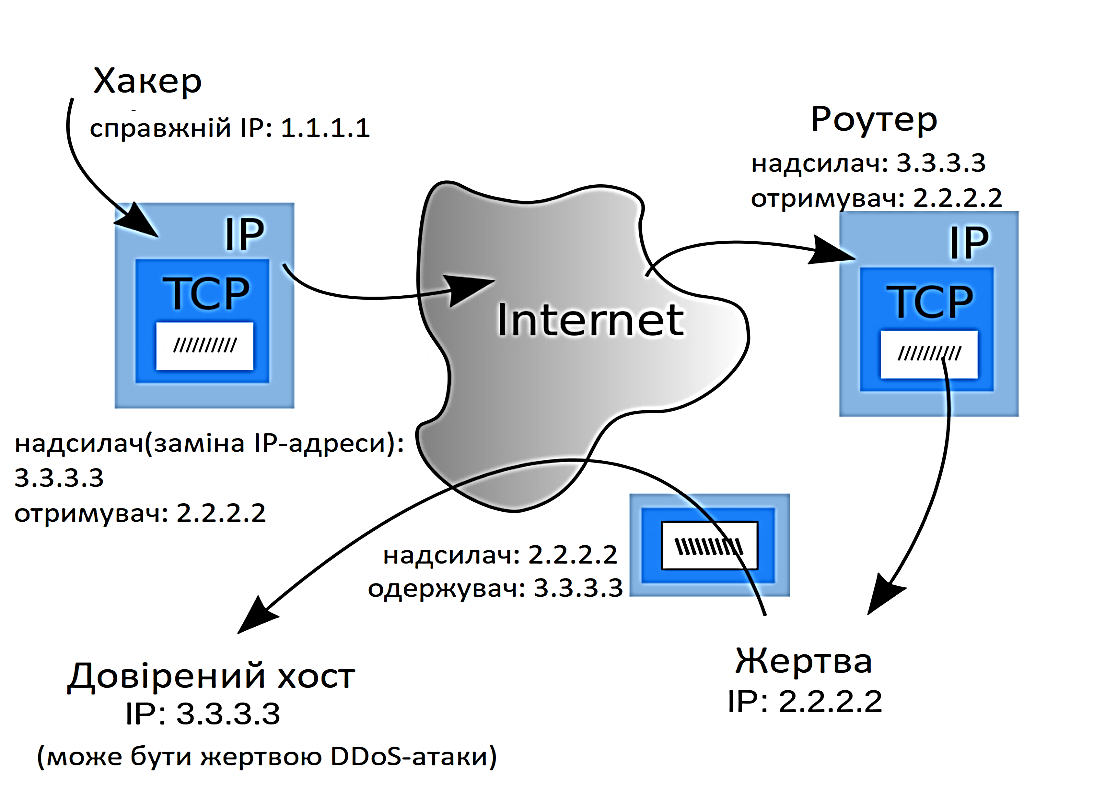


Рис. 1.4. Приклад використання спуфінгу

Ще важче визначити адресу джерела розподіленої атаки, так як безпосередніми виконавцями виступають "зомбовані" комп'ютери і саме їх адреси містяться в полі адреси відправника пакетів. І хоча нічого не підозрюючі власники комп'ютерів-виконавців стають учасниками розподіленої атаки проти своєї волі, велика частина відповідальності лягає і на них. Адже саме їх прогалини в забезпеченні безпеки власних систем зробили ​​цю атаку можливою.

**Фішинг атаки**. Фішинг-атака - це практика надсилання електронних листів, які здаються що є надіслані з надійних джерел, з метою отримання особистої інформації або впливу на користувачів, щоб вчинити якісь дії. Це поєднує в собі соціальну інженерію та технічну хитрість. Такі листи можуть містити додатки до електронного листа, що при відкритті завантажує шкідливе програмне забезпечення на ваш комп’ютер. Це також може бути посиланням на нелегітимний веб-сайт, який може привести вас до завантаження зловмисного програмного забезпечення або передачі вашої особистої інформації[15].

Щоб зменшити ризик піддатися фішингу, можна скористатися цими методами:**критичне мислення до сприймання електронної пошти, аналіз заголовків електронної пошти, пісочниця, критичне мислення для розшифровки URL-адреси, наведення курсору на посилання.**

**Критичне мислення** - не сприймайте електронну пошту, як реальну річ, лише тому, що ви зайняті чи піддані стресу, або у вас є 150 інших непрочитаних повідомлень. Зупиніться на хвилину і проаналізуйте електронний лист.

**Аналіз заголовків електронної пошти** - заголовки електронної пошти визначають, як електронний лист потрапив до вашої адреси. Параметри "Відповідь" та "Шлях повернення" повинні вести до того самого домену, що вказано в електронній пошті.

**Пісочниця** - Ви можете протестувати вміст електронної пошти в середовищі пісочниці, здійснюючи реєстрацію активності, відкриваючи вкладення або натискаючи посилання в середині електронної пошти.

Застосування критичного мислення для розшифровки URL-адреси.

**Наведення курсору на посилання** - наведіть курсор миші на посилання, але не натискайте на нього! Просто потримайте курсор миші над посиланням і подивіться, куди б вас насправді направило.

**Підслуховування**. Атаки підслуховування відбуваються через перехоплення мережевого трафіку. Підслуховуючи, зловмисник може отримати паролі, номери кредитних карток та іншу конфіденційну інформацію, яку користувач може надсилати по мережі. Підслуховування може бути пасивним або активним:

Пасивне підслуховування - хакер виявляє інформацію, прослуховуючи передачу повідомлення в мережі.

Активне підслуховування - хакер активно захоплює інформацію, маскуючи себе як дружню одиницю та надсилаючи запити передавачам. Це називається зондуванням, скануванням або підробкою.

Виявлення пасивних атак підслуховування часто важливіше, ніж виявлення активних, оскільки активні атаки вимагають від зловмисника здобути знання про дружні підрозділи, проводячи пасивні підслуховування раніше (шифрування даних - найкращий контрзахід для підслуховування).

Взагалі, важливість систем виявлення вторгнень досить велика на підприємствах. ІТ- підрозділи розгортають систему для отримання розуміння потенційно шкідливої ​​діяльності, яка відбувається в їх технологічному середовищі. Крім того, це дозволяє передавати інформацію між департаментами та організаціями все більш безпечним і надійним способом. Багато в чому це оновлення інших технологій кібербезпеки, таких як Брандмауери, Антивірус, Шифрування даних тощо.  
 Цікавим фактом, є те, що відповідно до нещодавно опублікованого звіту Global Market Insights Inc.[3], очікується, що ринок систем виявлення / запобігання вторгненням зросте з 3 млрд. Дол. США у 2019 р. До 8 млрд. Дол. США до 2025 р.. Ключові фактори, що сприяють зростанню ринку систем виявлення / запобігання вторгнень, - це кількість шкідливих дій, що відбуваються як внутрішньо, так і зовні, та масове зростання кібератак. На додаток до вищезазначеного, звіт GMI також виявляє, що на основі мережевих СВВ належить понад 20% частки на світовому ринку систем виявлення / запобігання вторгнень. Крім того, дослідження ринку системи виявлення вторгнень від Future Market Insights (FMI) говорить про те, що глобальний ринок СВВ сегментований на основі: типу, послуг та моделі розгортання.

**1.2. Можливості сучасних систем виявлення мережевих вторгнень та підходи до їх вдосконалення**

**Мережева система виявлення вторгнень** - система виявлення вторгнень (СВВ), яка відстежує такі види шкідливої ​​діяльності, як DoS атаки, сканування портів або навіть спроби проникнення в мережу. (Рис.1.5)

Мережева СВВ переглядає всі вхідні пакети на наявність в них підозрілих ознак. Якщо, наприклад, виявлена ​​велика кількість запитів на TCP з'єднання з широким діапазоном різних портів, то, скоріш за все, проводиться сканування портів. Також подібна система найчастіше відстежує вхідні запити. Прикладом мережевої СВВ є Snort.

Мережева СВВ не обмежується відстеженням тільки тим, що входить до мережевого трафіку. Часто важливу інформацію про те, що відбувається вторгнення можна отримати також з вихідного або локального трафіку. Дія деяких атак може розгортатися всередині спостережуваної мережі або сегмента мережі, і ніяк не відбиватися на вхідному трафіку.

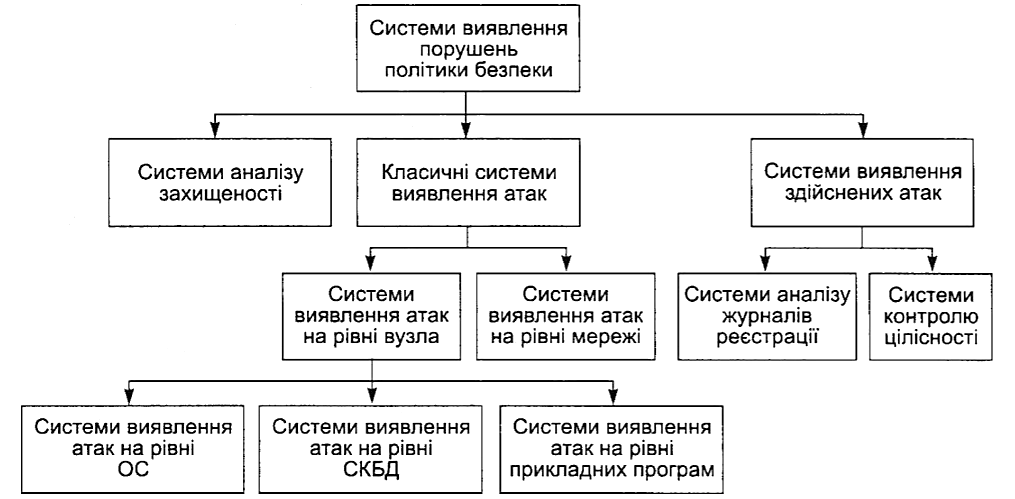


Рис.1.5. Узагальнена класифікація систем виявлення вторгнень

Найчастіше, мережева СВВ добре взаємодіє з іншими захисними системами. СВВ можуть на основі результатів своєї роботи оновлювати чорні списки міжмережевих екранів, заносячи туди IP адреси машин, запідозрених у здійсненні атаки зловмисників.

**Заснована на протоколі СВВ** (Protocol-based IDS, PIDS) являє собою систему (або агента), яка відстежує і аналізує комунікаційні протоколи зі зв'язаними системами або користувачами. Для веб-сервера подібна СВВ зазвичай веде спостереження за HTTP і HTTPS протоколами. При використанні HTTPS СВВ повинна розташовуватися на такому інтерфейсі, щоб переглядати HTTPS пакети ще до їх шифрування та надсилання у мережу.

**Заснована на прикладних протоколах СВВ** (Application Protocol-based IDS, APIDS) - це система (або агент), яка веде спостереження і аналіз даних, що передаються з використанням специфічних для певних програм протоколів. Наприклад, на веб-сервері з SQL базою даних СВВ буде відстежувати вміст SQL команд, що передаються на сервер.

**Хостова СВВ** (Host-based IDS, HIDS) - система (або агент), розташована на хості, що відслідковує вторгнення, використовуючи аналіз системних викликів, логів додатків, модифікацій файлів (виконуваних, файлів паролів, системних баз даних), стану хоста і інших джерел . Прикладом є OSSEC.

**Гібридна СВВ** поєднує два і більше підходів до розробки СВВ. Дані від агентів на хостах комбінуються з мережевою інформацією для створення найбільш повного уявлення про безпеку мережі. Як приклад гібридної СВВ можна привести Prelude [2].

Виходячи з того, що в неоднорідній мережі з високою ймовірністю можуть бути присутні клієнти з різними ОС, помітним мінусом мережевої IDS стає потенційна вразливість до атак, що враховує особливості реалізації різних TCP / IP-стеків, наприклад, при обробці фрагментированого мережевого трафіку. Аналізуючи механізм способу моніторингу системи виявлення вторгнень, розглянуто методи реагування (див. рис. 1.6): **блокування з'єднання, блокування хоста комп'ютерної мережі, виявлення атак за допомогою мережевих датчиків.**

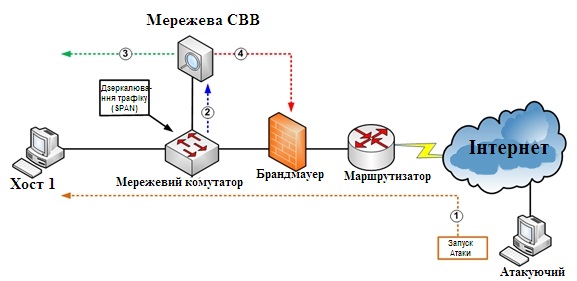


Рис. 1.6. Механізм виявлення та блокування вторгнень

**Блокування з'єднання**. Якщо для атаки використовується [TCP](https://uk.wikipedia.org/wiki/TCP)-з'єднання, то реалізується його закриття за допомогою посилки кожному або одному з учасників TCP-пакета з встановленим прапором RST. У результаті зловмисник позбавляється можливості продовжувати атаку, використовуючи мережеве з'єднання. Даний метод найчастіше реалізується з допомогою наявних мережевих датчиків.

**Блокування хоста комп'ютерної мережі**. Якщо з одного з [хостів](https://uk.wikipedia.org/wiki/%D0%A5%D0%BE%D1%81%D1%82) була зафіксована атака, то може бути проведене його блокування хостовими датчиками або блокування мережевих інтерфейсів або на нього, або на маршрутизаторі або комутаторі, за допомогою яких хост підключений до мережі. Розблокування може відбуватися через заданий проміжок часу або за допомогою активації адміністратором безпеки.

**Блокування атаки за допомогою мережевого екрану** (МЕ). IPS формує і надсилає нові конфігурації в [МЕ](https://uk.wikipedia.org/wiki/%D0%9C%D0%B5%D1%80%D0%B5%D0%B6%D0%B5%D0%B2%D0%B8%D0%B9_%D0%B5%D0%BA%D1%80%D0%B0%D0%BD), за якими екран буде фільтрувати трафік від порушника.

**Виявлення атак за допомогою мережевих датчиків**. Мережеві датчики встановлюються в розрив каналу зв'язку так, щоб аналізувати всі пакети які проходять. Для цього вони оснащуються двома мережевими адаптерами, які функціонують у «змішаному режимі», на прийом і на передачу, записуючи всі пакети в буферну пам'ять, звідки вони зчитуються модулем виявлення атак IPS. У разі виявлення атаки ці пакети видаляються.

**Висновки до першого розділу**

У розділі розглянуто: основні види мережевих вторгнень і ознаки сучасних комп'ютерних атак на ІС підприємства, можливості сучасних систем виявлення мережевих вторгнень та підходи до їх вдосконалення.

За кінцевими результатами проведеного аналізу та дивлячись з перспектив впровадження новітніх технологій захисту інформації, засоби захисту (міжмережеві екрани, кріптомаршрутізатори, сервери аутентифікації та ін.) гарантують додатковий рівень захисту інформаційної системи, доповнюючи "традиційний" захист. Дієвою СВВ можна вважати ту, яка функціонує в реальному часі та здійснює моніторинг трафіку мережі, а також відстежує аномалії, як в трафіку так і в діях користувачів і системи. Для цього в системі відповідно повинні діяти системи моніторингу та прогнозу network-based (NIDS) і host-based (HIDS).

Відповідно до мети дипломної роботи в другому розділі необхідне вирішення наступних завдань:оглянути види та ознаки мережевих вторгнень;проаналізувати недоліки сьогоднішніх СВВ; оглянути основні групи атак, їх види, ознаки та механізми; методи побудови системи виявлення мережевих вторгнень та виявлення ознак комп’ютерних атак.

**Розділ 2**

**ОСНОВНІ МЕТОДИЧНІ ПІДХОДИ ЩОДО ВИКОРИСТАННЯ СИСТЕМ ВИЯВЛЕННЯ МЕРЕЖЕВИХ ВТОРГНЕНЬ І ВИЯВЛЕННЯ ОЗНАК КОМП'ЮТЕРНИХ АТАК НА ПІДПРИЄМСТВІ**

Забезпечення безпеки інформаційних ресурсів є однією з найбільших проблем приблизно для всіх мереж в будь-якій галузі. Є численне велика кількість шкідливих методів заволодіти доступом до приватної інформації, мереж й веб-служб компаній, тому різні компанії використовують різні методи, в залежності від потреб, для забезпечення інформаційної безпеки інструментів, апаратних і програмних компонентів, в тому числі пристрої: брандмауери, механізми кодування і віртуальні власні мережі для високого захисту власної інформації. Численний розподіл і фактичне створення багатоелементних і багаторівневих колективних мереж призводить до потреби гарантувати безпеку всередині мережі.

Зазвичай використовують прості механізми захисту: ідентифікацію та аутентифікацію, механізми обмеження проходу до інформації відповідно правам суб'єкта і криптографічні механізми.

Звідси потреба в механізмах, які доповнюючи традиційні, дозволяють виявити спроби несанкціонованого доступу і інформують про це відповідальних людей. Важливо, щоб такі налагоджені системи зуміли протидіяти атакам, навіть якщо би правопорушник був авторизований і з його точки зору додержання прав, мав усі повноваження на свої дії. Для розуміння, як СВВ буде реагувати та протидіяти на дії зловмисників, необхідно детально розглянути: види мережевих проникнень, проаналізувати методи захисту та підходи до розробки систем виявлення атак.

**2.1 Аналіз захисту інформації від комп'ютерних атак**

Роблячи аналіз захисту від комп’ютерних атак на підприємстві можна зрозуміти, що немає жодної сфери суспільної діяльності, яка не була б цікава хакерам. На одні компанії нападають в пошуках конфіденційної інформації, на інші - з метою наживи, а хтось і зовсім стає випадковою жертвою масової атаки. Досвід роботи з моніторингу та реагування на інциденти дозволяє простежити певні тренди і зробити висновки про те, які галузі атакують найбільш часто і як це відбувається (див. рис. 2.1).

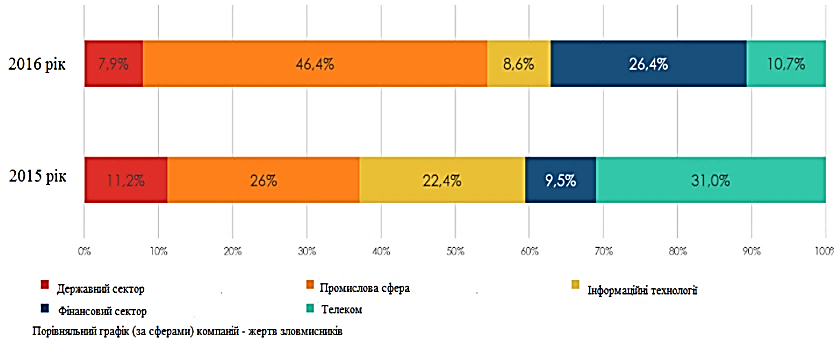


Рис. 2.1. Статистика інформаційної безпеки за сферами компаній

В 2016 році зафіксовано майже в тричі більше промислових компаній, що зіткнулися з інцидентами інформаційної безпеки, ніж було за рік до цього. Причому комп'ютерні атаки на промислові об'єкти склали близько 37% від загального числа розслідуваних інцидентів за останні два роки [4].

Зазвичай зловмисник мають на меті атакувати об'єкти критичної інфраструктури, але в даному випадку атаки відрізнялися ретельністю підготовки. Вони використовували передові технології та складні шкідливі програми, а інструменти розроблялися з урахуванням специфіки конкретної цільової системи. Такі атаки вимагають значних фінансових і тимчасових витрат. Цільові атаки на об'єкти критичної інфраструктури можуть призводити до серйозних наслідків і навіть потенційно до людських жертв, але найбільш частим наслідком є витік конфіденційної інформації.

У 2016 року експерти з питань кібербезпеки розслідували інцидент, який, незважаючи на швидке реагування, встиг завдати значної шкоди одному з найбільших українських банків. Атака була реалізована з використанням шкідливого ПЗ Green Dispenser, встановленого на банкомати. Ця троянська програма дозволяла по команді здійснювати видачу готівки з диспенсера. Важливим є те, що для захисту від випадкового запуску у шкідливій програмі використовувалася двухфакторна аутентифікація з двома пін-кодами - статичним і динамічним (унікальним для кожного запуску) [5].

Зловмисник підходив до банкомату з попередньо завантаженим шкідливим програмним забезпеченням, вводив статичний пін-код, після чого на екрані банкомату з'являвся QR-код. За допомогою мобільного додатка злочинець сканував QR-код, отримував другий (динамічний) пін-код, що відкриває доступ до диспенсеру готівки, забирав гроші і йшов.

Також, восени 2016 року було зафіксовано діяльність угруповання Cobalt, про існування якого стало відомо зовсім недавно. В результаті інциденту за одну ніч з декількох банкоматів одного з банків Східної Європи була вкрадена сума, еквівалентна 2 мільйонам гривень в місцевій валюті [5 ]. На підготовчі роботи зловмисники витратили два місяці: спочатку вони за допомогою поштових розсилок, що містять шкідливе програмне забезпечення скомпрометували внутрішню мережу банку, отримали доступ до комп'ютерів співробітників, відповідальних за роботу банкоматів, а потім віддалено завантажили шкідливі програми на банкомати і отримали можливість керуванням ними.

Також, зловмисники застосовували утиліти для роботи з обліковими записами і програмне забезпечення для віддаленого управління комп'ютерами, яке будь-хто міг завантажити з сайтів виробника. Щоб не привертати уваги до своїх дій, для завантаження на сервери і робочі станції необхідних утиліт злочинці використовували легітимні ресурси, обрані на основі результатів пошуку в поширених пошукових системах (зокрема, github.com), а для завантаження шкідливих програм – популярні файлообмінники.

Для віддаленого керування банкоматами використовувалася програма Radmin, яку зазвичай застосовували адміністратори цього банку, а тому її запуск не викликав підозр у відділу безпеки.

Для безпосереднього отримання готівки зловмисники використовували підставних осіб, яких знаходили по оголошеннях в Інтернеті. Ця підставна особа в призначений час (переважно вночі) підходила до банкомату і забирала гроші, які видавав банкомат по команді зловмисника.

В половині випадків при реалізації атак зловмисники використовували шкідливі програми. При цьому в 27% всіх атак мало місце впливу на користувачів методами соціальної інженерії [5 ].

Слабким місцем в системі захисту будь-якої організації, як і раніше залишається недостатні знання в області інформаційної безпеки співробітників. Багатьом зловмисникам це відомо, і тому вони активно використовують соціальну інженерію як при реалізації масових атак, так і в якості початкового етапу цільової атаки..

У 2016 році, навесні, було проведено аналіз скомпрометованих мереживих вузлів великої промислової компанії. В ході розслідування з'ясувалося, що компрометація сталася в результаті запуску шкідливого коду, отриманого співробітниками компанії з масових спам-розсилок (див. рис. 2.2).

Рис. 2.2. Розподіл типів атак, які застосовуються зловмисниками [6]

Зловмисники підроблювали листи від партнерів, з якими жертви регулярно взаємодіяли в рамках роботи. Це не викликало підозр, так як відправнику повністю довіряли. Такі атаки можливі лише після ретельної підготовки і вивчення внутрішніх процесів компаній, а також після атак на партнерські організації.

Виходячи з цього, можна говорити про те, що методи соціальної інженерії вже не перший рік популярні у зловмисників, і вони не стануть від них відмовлятися в найближчий час, подбавши про створення нових, ще більш переконливих сценаріїв.

У 2015-2016 роках, майже три чверті комп'ютерних атак, виявилися цільовими [5]. Однак зустрічалися і такі ситуації, коли до порушень роботи інфраструктури хакери не мали ніякого відношення (див. рис. 2.3).

Рис. 2.3. Типи подій ІБ, зафіксованих у 2015-2016 роках [5]

Наприклад, вкінці 2015 року, експерти проводили аналіз інциденту, що стався на одному підприємстві і викликав аварійну зупинку промислового обладнання. Незрозумілість була у тому, що причиною спрацювання аварійного режиму на програмно-апаратному комплексі виявилися проблеми в проводці і сильна вібрація будівлі при роботі обладнання. І хоча подія не була інцидентом інформаційної безпеки, це стало поштовхом до проведення оцінки захищеності автоматизованих систем підприємства, в результаті якої були виявлені і усунені суттєві недоліки в захисті.

Підводячи підсумки, можна сформулювати тренди комп'ютерних атак, які спостерігали в останні роки:

* для отримання фінансової вигоди під прицілом зловмисників регулярно виявляються банки і біржі. Злочинці мислять глобально. Вкрасти кошти цілого банку вигідніше, ніж спустошити рахунок одного клієнта або касети одного банкомату;
* у ході атак на промислові підприємства під загрозою розголошення виявляється конфіденційна інформація, а іноді і державна таємниця. Такі атаки вимагають гарної підготовки і фінансування, оскільки застосовуються передові технології і програмне забезпечення, розроблене з урахуванням специфіки конкретної цільової системи;
* соціальна інженерія є для зловмисників гарним способом «увійти у зачинені двері». Компанії, до яких можно підібрати такий підхід можуть бути у разних галузях, оскільки вихідним вектором атак є вплив на працівників, яких переконують відкрити поштові вкладення, відповісти на пару питань по телефону, ввести облікові дані на підробленому сайті тощо. Даний метод проникнення в локальну мережу виявляється настільки дієвим, що зловмисники і далі дбають про створення ще більш переконливих сценаріїв.
* на промислових підприємствах не полюбляють робити оновлення для того щоб не перебивати робочий процес. Процес управління оновленнями програмного забезпечення в компаніях досить тривалий і може затягнутися на роки. У зв'язку з цим можна сказати, що в атаках переважали використання відомих уразливостей і готових, перевірених не на одній жертві експлойтів [4].

**2.1.1. Класифікація атак, види, ознаки та механізми їх реалізації**

Існує безліч категорій та видів атак[ 7 ], які в свою чергу розрізняються механізмами та способами реалізації (див. рис. 2.4.):

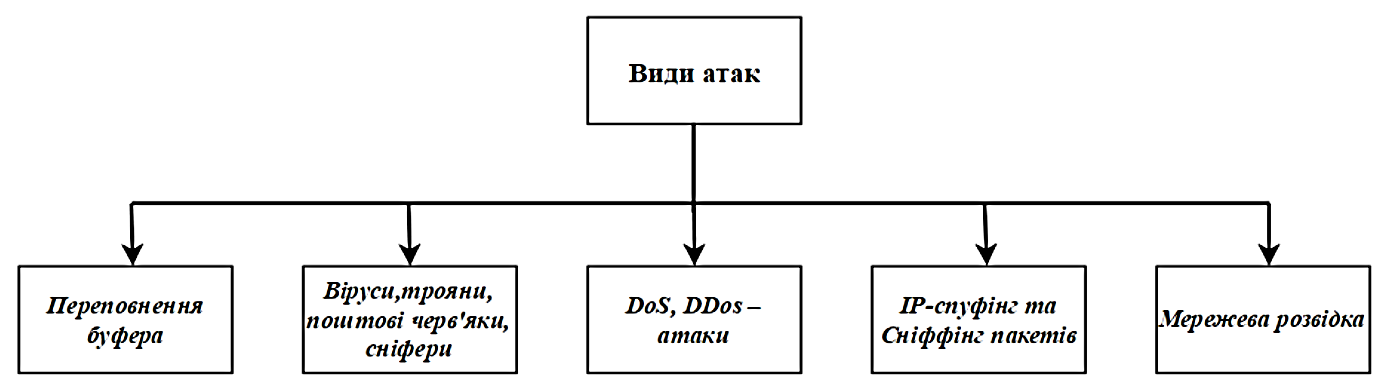


Рис. 2.4. Схема основних видів атак

Інформаційні мережі та автоматизовані системи є предметом для атак з боку зловмисників та шкідливого програмного забезпечення.

Засоби, за допомогою яких проводяться сучасні атаки, можна поділити на три групи, а саме:

* віруси та хробаки - коли шкідливе програмне забезпечення здатне додати свій код в інші програми або файли;
* троянські програми - маскуються під нешкідливі, навіть корисні додатки, але наносять збитки інформаційній системі після інсталяції;
* мережеві атаки - спрямовані на вторгнення до інформаційної мережі з метою аналізу уразливостей та в подальшому нанесення удару по інформаційній системі.

**Віруси та хробаки**(див. рис. 2.5.)**.** Вірус - це програма, яка активізується, копіюючи саму себе в виконувані об'єкти.

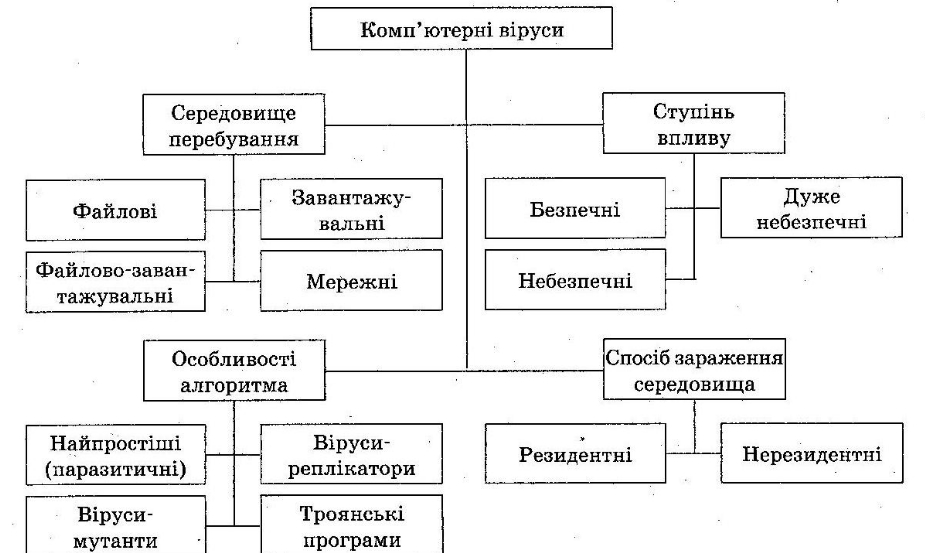


Рис. 2.5. Класифікація вірусів

Віруси можуть проникнути в ваш комп'ютер з інших заражених комп'ютерів, через носії даних (флешки, компакт-диски тощо) або через мережу (локальну або Інтернет). Розрізняють такі основні типи вірусів:

-файлові віруси, віруси, що заражають файли, атакують виконувані програми, зокрема, всі файли з розширеннями EXE і COM;

-віруси скриптів, вони є різновидом файлових вірусів. Вони написані на різних мовах скриптів (VBS, JavaScript, BAT, PHP і т. д.).

Ці віруси або заражають інші скрипти (наприклад, командні і службові файли Windows або Linux), або входять до складу багатокомпонентних вірусів. Віруси скриптів здатні заразити файли інших форматів, що дозволяють виконання скриптів, наприклад, HTML;

-завантажувальні віруси, вони атакують завантажувальні сектори (гнучкого або жорсткого диска) і встановлюють свої підпрограми, що завантажуються під час запуску комп'ютера;

-макровіруси, атакують документи, в які можуть вставлятися макрокоманди (макроси). Ці віруси часто впроваджуються в додатки обробки текстів чи електронних таблиць, так як в ці типи файлів легко вставляються макроси.

Інший варіант класифікації вірусів - за способом їх дії. У той час як віруси прямої дії виконують свою функцію відразу після активізації зараженого об'єкта, резидентні віруси зберігаються і функціонують в пам'яті комп'ютера.

Хробаки(див. рис. 2.6. )- це незалежні програми, які «розмножують» свої копії через мережу.

На відміну від вірусів (для поширення яких потрібен заражений файл, в якому ці віруси - самокопіри), хробаки активно поширюються, посилаючи свої копії через локальну мережу та Інтернет, комунікації електронної пошти або через вразливі місця операційних систем.

При цьому в них може бути включена додаткова начинка - шкідливі програми (наприклад, вони можуть встановлювати бекдор - це додаток клієнт-серверу, який відкриває розробникам таких програм віддалений доступ до вашого комп'ютера.

На відміну від звичайних (законних) програм з подібними функціями, бекдор - програми встановлюють доступ без згоди власника комп'ютера клієнта), хоча такою особливістю володіють не тільки хробаки.

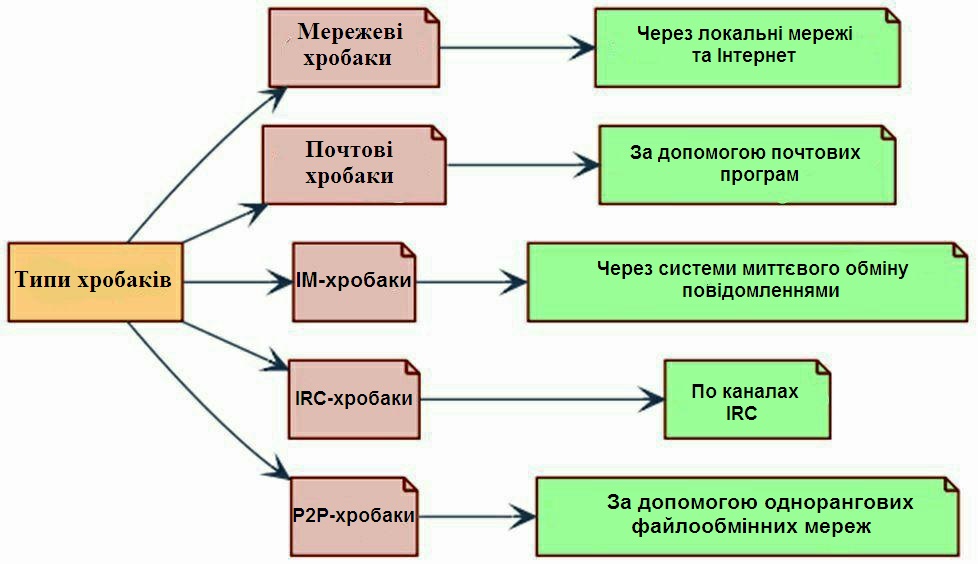


Рис. 2.6. Класифікація хробаків

Через Інтернет хробаки здатні розповсюдитися по всьому світу за лічені хвилини. Цей тип шкідливого програмного забезпечення можна класифікувати за типом поширення [7]:

* E-mail Worms. Поширюються через електронну пошту, а саме через прикріплені файли у електронному листі.
* Internet Worms. Поширюються безпосередньо через мережу Інтернет, користуючись відкритими портами або уразливостями системи.
* Network Worms. Поширюються по відкритим, незахищеним ін- формаційним мережам.
* Multivector Worms. Мають два, або більше методів поширення. До найбільш небезпечних атак можна віднести Boot sector Virus, Polymorphic Virus, Stealth Virus, Multipartite Virus.

Такі атаки можуть нанести значних збитків та витоку конфіденційної інформації, ці атаки маскуються та перешкоджають антивірусному програмному забезпеченню, що ускладнює процес виявлення та обеззараження інформаційної системи.

**Троянські програми**( див. рис. 2.7.[13])– це тип шкідливого програмного забезпечення, що маскується під корисний додаток або корисну програму, але насправді уражає цільову інформаційну систему після інсталяції.



Рис. 2.7. Троянські програми [13]

Суттєвою різницею між вірусом та трояном є те, що троян не інсталюється самостійно, він вводить в оману користувача маскуючись під корисне програмне забезпечення. Троян може розповсюджуватися за допомогою електронної розсилки у вигляді посилання або прикріпленого файлу.

**Поширені типи троянів:**

Remote Access Trojans (RAT) або Backdoor Trojan. Цей тип трояна відкриває бекдор на інфікованій інформаційній системі, щоб дозволити зловмиснику отримати віддалений доступ або навіть повний контроль над системою.

Trojan-DdoS. Цей вид троянів встановлюється одночасно на велику кількість комп’ютерів з метою створення мережі зомбі (ботнет) машин, які будуть використані для реалізації DDoS атаки на конкретну цільову інформаційну мережу.

Trojan-Proxy. Призначений для використання цільового комп’ютера як проксі-сервера, що дозволить виконати безліч операцій анонімно, навіть реалізувати подальшу атаку на мережу за допомогою ураженого комп’ютера.

Trojan-FTP. Призначений для відкриття FTP портів, що дозволить отримати віддалений доступ до інфікованої системи та мережі в цілому, а також вікна для подальшого поширення різноманітних загроз.

Destructive Trojans. Призначені для знищення або видалення даних на інфікованій інформаційній системі.

Keylogger Trojans. Троян, який призначений для зчитування та запам’ятовування інформації під час натискання клавіш на клавіатурі інфікованої системи та з подальшою передачею цієї інформації зловмиснику, що буде використана з метою викрадення таємних даних.

Cryptolock Trojan (Trojan.Cryptolocker). Новий тип троянів, що з’явився у 2013 році та призначений для шифрування та замикання окремих файлів на інфікованій системі[13].

Наслідки ураження інформаційної системи даним типом шкідливого програмного забезпечення можуть значно відрізнятися, від заміни робочого простору до відкриття бекдорів на інфікованому комп`ютері, що дозволить іншим вірусам уразити інформаційну систему або дозволить зловмиснику отримати віддалений доступ до комп’ютера, видалити важливі системні файли та форматувати жорсткий диск.

**Мережеві атаки** (див. рис. 2.8. ) відносяться до пасивних атак, які застосовується для аналізу мережевого середовища, збору інформації щодо відкритих портів або інших вразливих місць інформаційної системи.

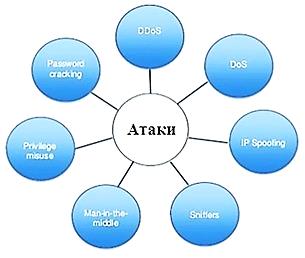


Рис. 2.8. Види мережевих атак

Залежно від процедур під час нападу або типу уразливості, мережеві атаки можуть бути класифіковані наступним чином:

Social Engineering. Відноситься до психологічної маніпуляції людьми в інформаційній мережі. Мета полягає у несанкціонованому отриманні доступу до конфіденційної інформації, крадіжки даних, промислового шпигунства і переривання обслуговування.

Phishing attack. Тип атак, що використовує соціальну інженерію для викрадення конфіденційної інформації – найбільш поширена мета таких атак полягає у викраденні інформації щодо до кредитних карток жертви.

Фішинг атака, як правило спочатку розповсюджують електронні листи, що ведуть користувачів на заражені сайти, які маскуються під банківські системи.

Watering Hole Attack. Найбільш складний тип атак, що базується на комплексному підході до ураження інформаційної системи конкретного користувача. Спочатку зловмисник вивчає звички потенційної жертви, збирає історію про відвідувані веб-сайти та обирає найбільш популярні портали, що мають вразливість у безпеці. Наступним кроком є інсталяція свого шкідливого коду або програми у такий веб-сайт.

Port scanning. Тип атаки де зловмисник сканує порти на цільовій інформаційній системі, щоб з’ясувати де знаходяться активні та відкриті порти з метою ураження системи шкідливими послугами, що пов’язані з конкретними портами.

Spoofing. Тип атаки, що маскує зловмисника, програму або адрес під інший шляхом фальсифікації даних з метою несанкціонованого доступу до інформаційної системи.

Denial of Service Attack (DoS Attack) and Distributed Denial of Service Attack (DDoS Attack). Атака пов’язана з призупиненням надання послуг або повною зупинкою інформаційної системи шляхом створення потужної активності фальсифікованих користувачів в системі та великої кількості запитів до бази даних, що призводить до завантаження відповідної інформаційної системи[12].

Ping of Death (PoD). Атака, що базується на відправці спотвореного або шкідливого пінгу на цільову інформаційну систему з метою переповнення буферу.

Smurf Attack. Атака яка повторює дії Ping of Death з маскуванням IP адреса зловмисника.

Bluesnarfing. Атака, що дозволяє отримати доступ до інформації на пристрої за допомогою зв’язку Bluetooth. Будь-який пристрій з включеним режимом Bluetooth може бути схильним до такого типу атак.

Мережеві атаки не руйнують ресурси або дані. Активна фаза відбувається коли зловмисник застосовує комбінований метод і поєднує мережеву атаку з будь яким типом вище розглянутих атак [7].

**2.1.2. Сучасні методи атак та їх виявлення**

Для виявлення багатьох типів атак потрібно розуміти принцип дії зловмисників та можливі способі протидії для спеціалістів центру інформаційної безпеки. Взагалі, існує безліч методів атак та їх виявлення.

Брандмауери повинні комбінувати при роботі пакетні фільтри та шлюзи додатків, щоб забезпечити належну адресну безпеку. Шлюз додатків переглядає не лише заголовки, але й приймає рішення щодо дотримання політки на основі даного прикладного рівня. Також, він виконує роль сервера, що працює на прикладному рівні, і через цей сервер мають протікати всі дані додатків (вхідні і вихідні). На одному хості може працювати одразу декілька шлюзів додатків, проте кожний шлюз - це самостійний сервер з власним набором процесів[14](див.рис.2.9).

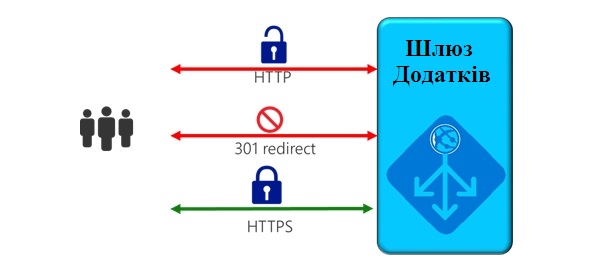


Рис. 2.9. Приклад роботи шлюзу додатків

Для виявлення багатьох типів атак потрібно виконувати поглиблену перевірку пакетів з даними - аналізувати не лише поля заголовків, а й дані додатків, що містяться у пакеті. Шлюзи додатків можуть виконувати дану операцію, проте вони вирішують цю задачу лише для конкретного додатку.

Системи виявлення вторгнень дозволяють виявляти різні атаки, а саме трасування мережі, сканування портів, стеків ТСР, атаки відмови в обслуговуванні, застосування червів та вірусів, атаки на вразливості операційної системи чи окремих додатків.В мережі організації можуть бути декілька таких систем. При одночасній роботі вони працюють узгоджено , пересилаючи повідомлення про підозрілий трафік в центральний процесор системи, який збирає та систематизує ці дані, а також повідомляє адміністратору якщо це необхідно.

Системи виявлення сигнатур (див. рис. 2.10) можна розділити на дві категорії: ті, **що працюють на основі перевірки сигнатур і ті, що працюють на основі виявлення аномалій.**

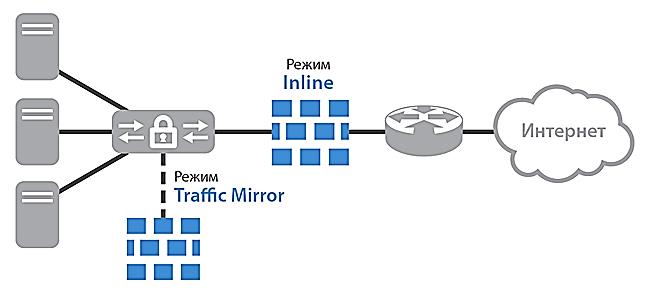


Рис. 2.10. Принцип роботи системи виявлення сигнатур

Система, що працює на основі перевірки сигнатур, веде загальну базу даних сигнатур атак. Кожна сигнатура - це набір правил, що описують способи боротьби з вторгненнями. Дана система аналізує кожний пакет, що проходить повз неї, порівнюючи його вміст з сигнатурами бази даних. Якщо пакет співпадає з сигнатурою, то генерується попередження. Проте мінусом даного підходу є те, що система безсильна проти незареєстрованих атак, збіг сигнатур може бути зовсім не атакою, а також при порівнянні пакету з величезною колекцією сигнатур система може просто не впоратись з такою роботою і проґавити шкідливі пакети.

Система, що працює на основі виявлення аномалій, створює профіль надійного трафіку, який спостерігається у штатному режимі. Потім вона відстежує такі потоки пакетів, які мають, статичні зміни. Наприклад непропорціональне збільшення пакетів, чи різкий скачок інтенсивності сканування портів. Гарною стороною є те, що вони можуть відстежувати нові, ще не описані атаки, проте з іншої сторони, виключно важко розрізняти нормальній і статично незвичайний трафік.

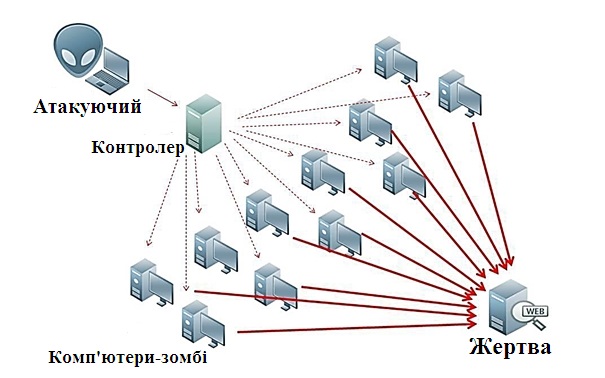


Рис. 2.11. Приклад DDoS атаки

Для того, щоб визначити DDoS атаку (див.рис. 2.11.) , за допомогою програми можна відфільтрувати окремі адреси джерел пакетів та проаналізувати колонки Time та DestPort. Якщо значення DestPort співпадають, то це явна ознака DDoS атаки. Дивлячись на стовпець Time, можна помітити, як мало часу між кожним пакетом - всього тисячі секунд. Це ще одна ознака атаки DoS.

Вище було досліджено яким способом та чи інша атака може здійснювати вплив на ІС. Отже, аналізуючи ці дані,можливо розробити методику побудови системи виявлення мережевих вторгнень та виявлення ознак комп’ютерних атак.

**2.2. Організаційні та технічні підходи до розробки систем виявлення мережевих вторгнень**

**Брандмауер (англ. Firewall)** – є основним компонентом для впевненості в надійності системи виявлення мережевих вторгнень. Брандмауер - програмний продукт або програмно-апаратний комплекс, який контролює мережеві пакети або встановлені програми. Потрібен для захисту системи від комп'ютерних атак. Брандмауером також можуть називати міжмережевий екран, мережевий екран або firewall.

На комп'ютерах з сучасними операційними системами йде як вбудоване програмне забезпечення. Також брандмауер може входити до складу платних антивірусних систем.

Програмні реалізації для Windows - вбудований брандмауер (можна відкрити в панелі управління або з центру управління мережами і загальним доступом), окремі програми, антивірусні системи з включеним до складу мережевим екраном. На Linux представлений, найчастіше, вбудованим в ядро ​​Netfilter, управління якого здійснюється із застосуванням різних утиліт, наприклад, iptables або firewalld. Для BSD - ipfirewall, для управління яким використовується ipfw.

Чи потрібен брандмауер? На сервері, який підключений до мережі Інтернет безпосередньо - обов'язково. На звичайному домашньому комп'ютері, який використовується для розваг і отримання інформації можна сміливо відключити. Всі брандмауери за функціонуванням можна поділити на три категорії: **традиційні пакети фільтрів, фільтри, що враховують стан з'єднання та шлюзи додатків.**

* Традиційні фільтри пакетів. Весь вхідний та вихідний трафік внутрішньо корпоративної мережі проходить через маршрутизатор, на якому відбувається фільтрація пакетів. Фільтр пакетів перевіряє кожну дейтаграмму, визначаючи як і що з нею зробити згідно з правилами, встановленими адміністратором мережі. Адміністратор мережі конфігурує брандмауер, спираючись на політику, що діє в організації (див. рис. 2.12.).

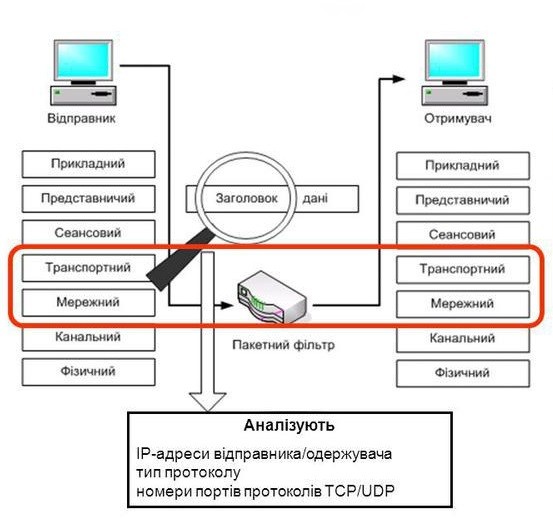


Рис. 2.12. Принцип роботи фільтрації пакетів

Рішення, пов'язані з фільтрацією, зазвичай засновані на наступних факторах: вихідна чи кінцева ІР-адреса, тип протоколу в відповідному полі дейтаграми, флагові біти, тип повідомлення, різні правила, що характеризують вхідні і вихідні дейтаграми даної мережі та правила, що стосуються інтерфейсів. Правила брандмауера реалізуються в маршрутизаторах за допомогою списків контролю доступу. Ці правила застосовуються для кожної дейтаграми, яка проходить через даний інтерфейс.

* Фільтри, які враховують стан з'єднання відстежують ТСР-з'єднання і виконують фільтрацію на основі цієї інформації. Всі поточні ТСР-з'єднання відстежуються в спеціальній таблиці з'єднань. Якщо ж вхідний пакет не буде відноситись до поточних з'єднань, то він буде відкинутий брандмауером (рис. 2.13).

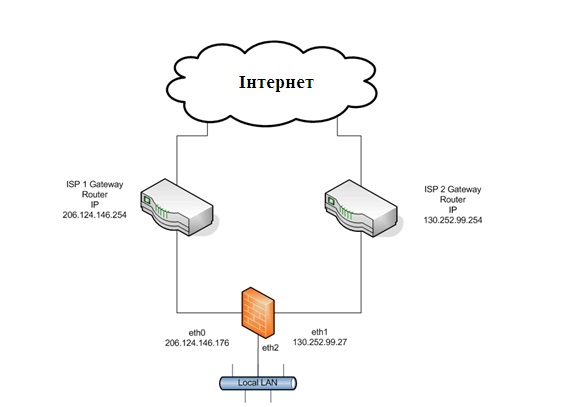


Рис. 2.13. Принцип фільтрацій які враховують стан з’єднання

* Шлюзи додатків - замість аналізу IP-пакетів шлюзи цього типу вивчають дані на рівні додатків. Часто шлюзи додатків використовують додатки які відповідають за створення окремого сеансу. На відміну від фільтр-пакетів цей сеанс не допускає прямого з’єднання між двома мережами, іншими словами цей шлюз не може виступати в якості посередника для трафіку пакетів (див.рис. 2.14).

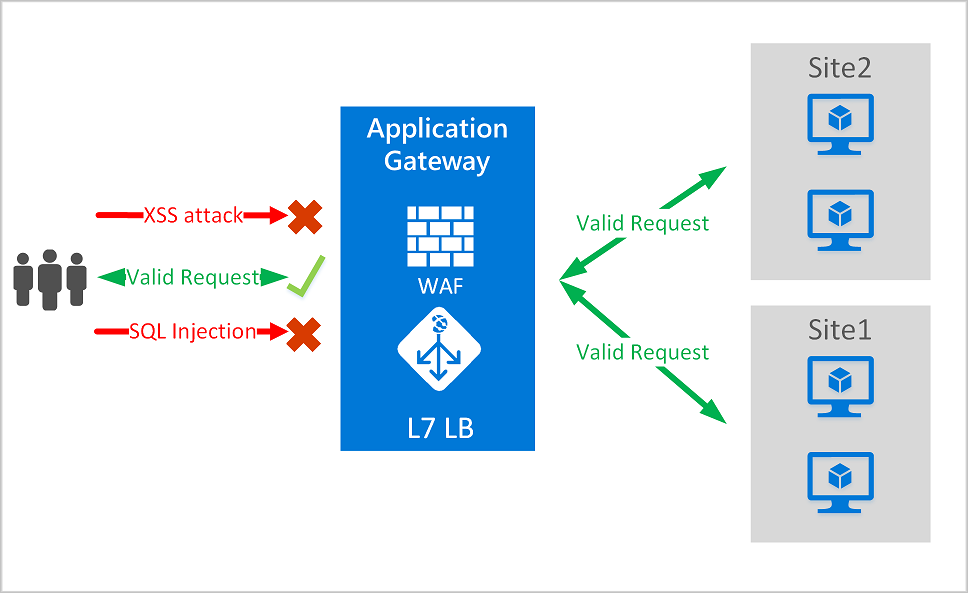


Рис. 2.14. Принцип роботи брандмауера через шлюз додатків

Якщо раціонально підібраний та правильно встановлений брандмауер функціонує в системі то він може слугувати не поганою системою захисту від можливих злочинних нападів.

Аналізуючи те, що будь-яка система, яка встановлена для запобігання можливих вторгнень, має свої певні недоліки, то слід більш детальніше вивчити їх наслідки та врахувати при побудові і поліпшені системи захисту інформації. Взагалі структура сучасних СВВ повинна включати такі підсистеми:

* підсистема збору інформації про систему, яка підлягає захисту;
* підсистема аналізу для пошуку атак та вторгнень в систему;
* підсистема представлення даних для контролю системи в режимі реального часу (див. рис. 2.15).

Підсистема збору інформації отримує дані від автономних модулів, датчиків програмного забезпечення (ПЗ) системи, датчиків хосту, міжмережевих та мережевих датчиків, скомпонованих у залежності від задач структури мережі та типу інформації, яка підлягає аналізу.

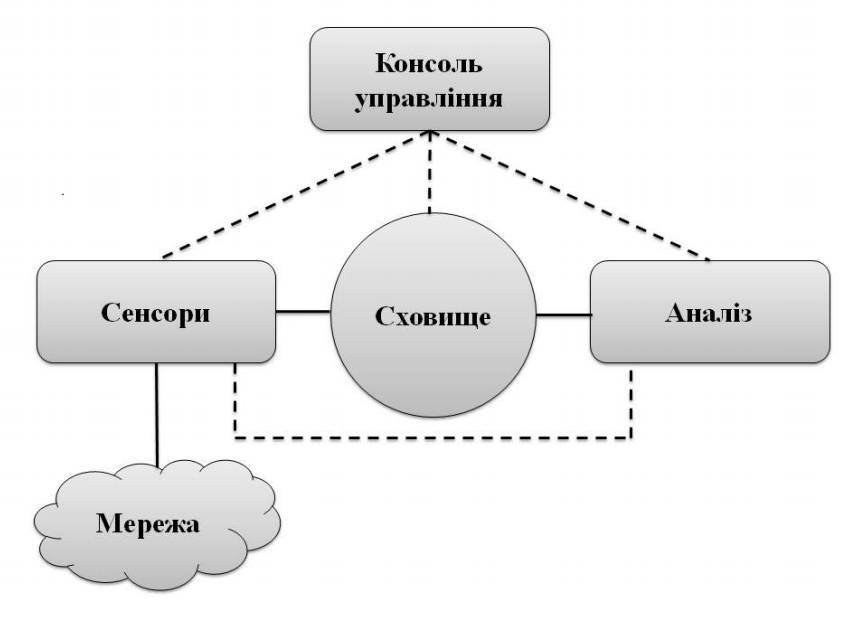


Рис. 2.15. Схема загальної структури СВВ

Ієрархічно підсистема аналізу як вхідні дані використовує інформацію із попередньої підсистеми і містить у собі набір аналізаторів, скомпонованих за задачами виявлення вторгнень заданого типу. Ефективність виявлення вторгнень залежить від параметрів аналізаторів та їх кількості.

Підсистема представлення даних орієнтована на різні групи користувачів, які контролюють певні підсистеми мережі. Тому в таких СВВ використовують розмежування доступу, групові політики, повноваження та ін.

У залежності від наборів параметрів оцінки стану системи сучасні СВВ використовують дві групи методів. У випадку фіксованого набору параметрів оцінки і фіксованого часу навчання використовуються методи контрольованого навчання («навчання з учителем»).

У випадку, коли множина параметрів оцінки може змінюватися протягом заданого часу дослідження, а процес навчання відбувається весь час, використовуються методи не контрольованого навчання («навчання без учителя»).

Основною ідеєю виявлення нестандартної поведінки мережі, яка підлягає захисту, є формування профілю чи образу мережі. Тому основними методами, на яких базується реалізація СВВ, є методи розпізнавання образів. При цьому образ нормальної поведінки формується на основі аналізу параметрів оцінки мережі.

Висновки про аномальну поведінку формуються на основі відхилень значень оцінок параметрів від профілю мережі. Величина та характер відхилень, як правило, в режимі реального часу, дають змогу проводити ідентифікацію аномалії – технічний збій, допустиме відхилення пов’язане із дією зовнішнього середовища, атака на мережу.

Формування профілю чи образу в СВВ проводиться за допомогою таких методів:

* статистичні методи аналізу параметрів оцінки;
* методи множинного опису подій та формальної логіки;
* методи нечіткої логіки та нейронні мережі.

Виходячи із способів формування профілю мережі та методів виявлення аномалій, можна визначити два класи задач:

* вибір оптимальної множини параметрів оцінки;
* визначення загального показника аномальності.

Питання визначення інтегральної оцінки аномальності поведінки мережі на сьогодні є практично не вирішеним завдяки неоднозначності розв’язку задачі формування множини оцінок параметрів мережі, яка підлягає захисту.

Розв’язок задач формування множини оцінок параметрів та їх динаміки можливий при використанні методу групового врахування аргументів, еволюційних та генетичних алгоритмів. Тоді визначення інтегральної оцінки може бути проведене за допомогою аналізу коваріацій (мірою спільної мінливості) параметрів оцінок, методів кореляційного аналізу, автокореляційних моделей.

**2.3. Розробка методики побудови систем виявлення мережевих вторгнень і виявлення ознак комп'ютерних атак**

Для розробки методики побудови систем виявлення мережевих вторгнень і виявлення ознак комп'ютерних атак в роботі визначено, що засобами технології виявлення мережевих атак є програмні та апаратні системи виявлення, які функціонують переважно в TCP / IP мережах і базуються на сигнатурних та статистичних методиках виявлення на основі хостових і мережевих моделей.

Виявлення атак вимагає виконання однієї з двох умов: або розуміння очікуваної поведінки контрольованого об’єкта системи, або знання всіх можливих атак і їх модифікацій. У першому випадку використовується технологія виявлення аномальної поведінки, а в другому – технологія виявлення зловживань.

Серед відомих методів побудови систем виявлення мережевих вторгнень і виявлення ознак комп'ютерних атак виділяються наступні [8]:

1. Статистичний метод;
2. Приховані марківські моделі;
3. Нечітка логіка;
4. Експертні системи;
5. Використання прогнозованих шаблонів;
6. Генетичні алгоритми;
7. Штучні нейронні мережі;
8. Аналіз переходів зі стану в стан.
9. Data mining-методи.

Застосовувані при виявленні та запобіганні мережевих атак методи і моделі зводяться до мережевого і хостового аналізу сигнатурних і статистичних даних мережевого трафіку з подальшим виведенням засобів виявлення атак про здійснення атаки. До таких висновків відносяться повідомлення на консоль або в журнали засобів виявлення атак про час виявлення, проведення, назви та типу атаки. Результатами роботи засобів виявлення атак є дані про номери пакетів, що містяться в сеансі атаки.

Сигнатурний аналіз і контроль профілів при виявленні комп’ютерних атак включає в себе аналіз заданих заздалегідь послідовностей, як самих аналізованих даних, так і послідовностей дій. Сучасні методики виявлення мережевих атак досить різнорідні і не зведені до єдиного критерію, за яким можливо оцінювати ефективність їх застосування. Таким критерієм може служити повнота охоплення всіх аналізованих параметрів, необхідних для точного і найбільш ймовірного виявлення атаки з мінімально хибним спрацьовуванням.

Окремим сегментом систем виявлення атак мережного рівня є системи виявлення безпровідних атак – WIDS (Wireless Intrusion Detection System), основу яких складають сенсори, що виконують функцію збору безпровідного трафіку в режимі моніторингу та його обробку. Як правило, сенсори є достатньо інтелектуальними пристроями, які підтримують протоколи TCP/IP та мають розвинений інтерфейс управління.

Сучасні IDPS системного рівня для виявлення атак використовують журнали реєстрації подій. Цей процес автоматизований, він об’єднує складні методи виявлення, що ґрунтуються на новітніх дослідженнях у галузі математики. Як правило, IDPS системного рівня контролюють систему, події та журнали реєстрації подій безпеки (security log чи syslog). Коли якийсь з цих файлів змінюється, то IDPS порівнює нові записи з сигнатурами атак, щоб перевірити, чи є збіжність. Якщо вона знайдена, то система надсилає адміністратору сигнал тривоги або приводить в дію інші задані механізми реагування [9].

IDPS системного рівня постійно розвиваються, поступово об’єднуючи все нові й нові методи виявлення, одним з них є метод, що полягає у перевірці контрольних сум ключових системних та виконуючих файлів через регулярні інтервали часу на предмет несанкціонованих змін. При цьому своєчасність реагування на атаки безпосередньо пов’язана з частотою опитування.

При виявленні та запобіганні мережевих атак вже використовуються методики, що мають можливість саме запобігання мережевих атак і включають в себе тільки лише такі дії, як блокування прийому / передачі тих мережевих пакетів, які ідентифікуються та ті пакети, що містяться в атаці.

Методики виявлення і запобігання мережевих атак зводяться до застосування технологій виявлення мережевих атак, які включають в себе програмні та апаратні системи виявлення атак. Ці системи функціонують переважно в *TCP / IP* мережах і базуються на сигнатурних та статистичних методиках виявлення атак і на основі хостових і мережевих моделей, результатом яких є виявлення атак з метою автоматизації забезпечення захисту локальної обчислюваної мережі (ЛОМ).

У таких методиках спільною рисою з формальної точки зору є те, що існує кілька підходів подання повідомлень про виявлені атаки.

При виявленні мережевих атак в основному застосовуються методики узагальнення приватних рішень, які будуються з використанням різноманітних методів і технологій.

Для того, щоб система прийняття рішень могла узагальнювати дані, отримані від різних підсистем системи виявлення вторгнень, необхідно стандартизувати формат повідомлень про атаки, що посилаються цими аналізаторами.

Підсистема системи виявлення вторгнень передає в систему підтримки рішень вектор виду 2.1:

, (2.1)

де *А* – системний ідентифікатор виявника атаки, *С* – ідентифікатор виявленої атаки, *G* – вид атаки, *Т* – системний час атаки, *М* – ідентифікатор методу, яким виявлена атака, *Р* – ймовірність проведення атаки, *Рн* – нижня межа ймовірності атаки, *Рв* – верхня межа ймовірності атаки.

Подальша обробка проводиться роздільно для кожного з видів атак. Тимчасова вісь *t* розбивається на інтервали аналізу Δ*t.* Довжина інтервалу Δ*t* визначається виходячи з типу атаки і швидкості її виявлення підсистемами СВВ. У кожному інтервалі проводиться аналіз повідомлень з метою оцінки узагальненої ймовірності атаки.

У ряді робіт, виконаних у суміжних областях, показано, що вироблення оптимального методу об’єднання статистичних гіпотез про виявлення різнорідних об’єктів в практичній ситуації неможлива.

Для систем виявлення атак це пояснюється відсутністю даних про апріорні ймовірності атак різних видів, різною природою проаналізованих ознак, неможливістю оцінки спільних рис розподілу значень цих ознак, рознесенням в часі моментів повідомлень про атаки [8].

Збільшення ймовірності виявлення атаки веде до зростання ймовірності „помилкової тривоги”. Для того щоб ймовірність „помилкової тривоги” залишалася в допустимих межах, пропонується використовувати мажоритарний критерій для прийняття рішень. Якщо в системі присутні кілька виявників атак, які виявлятимуть заданий вид атаки, то рішення про наявність атаки приймається в випадку, якщо вона виявлена більш ніж половиною СВА.

Розвитком мажоритарного підходу є вимоги трудомісткої експертної роботи та застосування при обчисленні ймовірності атаки апріорної інформації про властивості підсистем, які реалізуються на основі обчислення зваженої суми значень *Pi*, де в якості ваги застосовується ступінь довіри до того чи іншого виявника (підсистемі СВВ) при розгляді даної конкретної атаки. Тоді ймовірність виявлення атаки (Класу або групи атак) *k* може бути представлена виразом 2.2:

(2.2)

де *m* – число аналізаторів, що використовуються в СВВ, *Pkj* – ймовірність атаки *k*, передана *j*-м аналізатором на інтервалі Δ*ti*,, *Wkj* – ступінь довіри результатам роботи аналізатора *j* при виявленні атаки *k*, причому . Якщо повідомлень про атаки в інтервалі аналізу Δ*ti* не зафіксовано, .

Відповідно застосування ймовірнісної оцінки виявлення атак, залежить від числа аналізаторів, ймовірності атаки і ступеня довіри аналізаторам при виявленні атаки.

Таким чином, сучасні засоби захисту можна розділити за характеристиками, що представлені на (див. рис. 2.16):



Рис. 2.16. Схема характеристик систем виявлення вторгнень

Основними принципами створення засобів виявлення і протидії комп’ютерним атакам є наступні[8]:

* **Принцип прозорості**. Система виявлення та протидії комп’ютерним атакам (КА) повинна функціонувати у фоновому режимі непомітно для користувачів, не знижуючи оперативності виконання технологічних циклів управління, при цьому забезпечуючи виконання своїх цільових функцій;
* **Принцип оптимальності**. Розробка системи виявлення та протидії КА повинна проводитися з урахуванням того, що кожен з методів виявлення (протидії) КА дозволяє досить ефективно і достовірно виявляти (нейтралізувати) тільки певні види КА. Тому при створенні системи виявлення та протидії КА повинно бути знайдено оптимальне співвідношення між методами виявлення і протидії КА і способами їх застосування в складі системи;
* **Принцип адекватності**. Розробляються для реалізації в системі виявлення та протидії КА проектні рішення повинні бути диференційовані залежно від частоти, ймовірності та очікуваного збитку від успішної реалізації кожного виду КА;
* **Принцип повноти**. Даний принцип полягає у використанні для виявлення КА інформації про стан і значення основних параметрів всіх програмних і технічних елементів пунктів управління АС;
* **Принцип адаптивності**. Система виявлення та протидії КА повинна створюватися з урахуванням того, що з розвитком АС здійснюватиметься поступова зміна складу і характеристик програмних і технічних засобів АС, що, у свою чергу, призведе до розширення переліку загроз безпеки. Тому при створенні системи виявлення та протидії КА в її складі повинні бути передбачені механізми адаптації системи до мінливих умов функціонування.

Під захищеною ІС розуміється система, в якій використовуються персональні комп’ютери (ПК), технічні канали зв’язку, які передбачають середовище передачі даних і каналоутворюючого обладнання ЛОМ.

У таку ІС входять:

* Програмне забезпечення, що використовується при роботі користувачів і виконанні основних функцій по роботі з базами даних, клієнтськими додатками та інше;
* Технічні засоби – вузли ЛОМ, комунікаційне і каналоутворююче обладнання та лінії зв’язку між ними, сукупність яких утворює фізичну топологію мережі;
* Програмні засоби, що забезпечують функціонування, а також фізичну та логічну взаємодію всіх технічних засобів, що входять в ІС, такі як системне ПЗ, спеціалізоване мережеве ПЗ.

Основною проблемою і обов’язковою умовою у створенні захищеної ІС є формалізація методу опису предметної області та оперування моделями, які адекватно описують архітектуру і функціонування об’єкта, що проектується. Для опису платформи безпеки (ПБ) розподілених ІС використовують формалізм семантичних мереж фреймів [8]:

В основі мережевих моделей лежить конструкція виду 2.3:

, (2.3)

де *I* – множина інформаційних одиниць, *Ci, C2, ..., Cn*  – множина типів зв’язків між елементами; *Г* – відображення, що задає зв’язок з прийнятого набору між інформаційними одиницями.

З точки зору захищеності ІС розглядають графову модель системи захисту з повним перекриттям.

У цій моделі розглядається взаємодія „області загроз”, „область, що захищається” (ресурсів АС) і „системи захисту” (механізмів безпеки АС).

Таким чином, маємо три множини:

*Т = {ti}* – множина загроз безпеки, *О = {oj}* – множина об’єктів (Ресурсів) захищеної системи, *М = {mk}* – множина механізмів безпеки.

Елементи цих множин знаходяться між собою у певних відношеннях, власне і описують систему захисту.

Для опису системи захисту зазвичай використовується графова модель. Множина відношень загроза-об’єкт утворює дводольний граф *{<Т, О>}*. Мета захисту полягає в тому, щоб перекрити всі можливі ребра в графі. Це досягається введенням третього набору *М*. У результаті виходить тридольний граф *{<Т, М, О>}*. Розвиток цієї моделі припускає введення ще двох елементів:

*V* – набір вразливих місць, які визначаються підмножиною декартового добутку *Т\*О: vr = <ti, оj>*. Таким чином, під вразливістю системи захисту будемо розуміти можливість здійснення загрози *t* відносно об’єкта *о* (на практиці під вразливістю системи захисту зазвичай розуміється не сама можливість здійснення загрози безпеки, а ті властивості системи, які сприяють успішному здійсненню загрози, або можуть бути використані зловмисником для здійснення загрози);

*В* – набір перешкод, що визначається декартовим добутком *V\*M: bi = <ti,Oj,mk>*, які представляють собою шляхи здійснення загроз безпеці, перекриті засобами захисту.

При побудові систем захисту, які використовують пристрої виявлення мережевих атак, необхідно використовувати існуючі мережеві і хостові моделі та статистичні методи для повного перекриття підсистемами захисту *М* вдалого здійснення мережевих атак.

Загалом ІС надає такі види послуг:

* встановлення зв’язку – реалізується засобами каналоутворюючого обладнання за допомогою каналів зв’язку;
* передача даних – ЛОМ оснащена апаратурою та каналами передачі даних для забезпечення заданих швидкостей і надійності обробки даних.

Параметри захищеної ІС повністю підходять під описані нижче:

* Залежно від виду засобів, методів і алгоритмів керування, можна виділити ІС з централізованим і розподіленим управлінням. При цьому можуть виконуватися як жорсткі, так і гнучкі алгоритми управління ІС, що враховують численні фактори. Об’єднання мереж здійснюється або через загальний вузол, або шляхом створення спеціальних каналів, з’єднують вузли однієї системи з вузлами іншої. Якщо мережа може бути з’єднана з іншими, то вона називається відкритою, якщо ні, то – закритою.
* За функціонально-цільовим і прикладним призначенням ІС можна розділити на дві групи: загального користування та спеціального призначення.
* ІС загального користування призначені для різних сфер застосування незалежно від конкретного змісту даних, що обробляються в ІС. Засоби, структура і функціональні можливості виявляються однаковими для багатьох випадків застосування і забезпечують широкий діапазон послуг.
* ІС спеціального призначення призначені для вирішення завдань в певній предметній або відомчої області.

Характеристики засобів, що забезпечують обробку даних в ІС, включають:

* технічні засоби (сервера, робочі станції, комунікаційне обладнання, міжмережеві екрани) і лінії зв’язку між ними, сукупність яких утворює фізичну топологію АС (ЛОМ) та точки взаємодії (Стики) з іншими АС;
* програмні засоби, що забезпечують функціонування, а також фізична і логічна взаємодія (канали керування і передачі даних) всіх технічних засобів, що входять до АС (системне ПЗ, спеціалізоване мережеве ПЗ);
* прикладне та сервісне програмне забезпечення, що розробляється окремо від загальносистемного ПЗ і виконує покладені на нього функції в рамках реалізації тієї чи іншої інформаційної технології (СУБД, офісні додатки, редактори, компілятори, WEB-сервера та інше).

Мається на увазі, що компоненти ЛОМ розосереджені в просторі і зв’язок між ними фізично здійснюється за допомогою мережевих з’єднань, а програмно – за допомогою механізму повідомлень, заснованого на стеку протоколів *TCP / IP*. При цьому всі керуючі повідомлення і дані, пересилаються між об’єктами ЛОМ, передаються по мережевим з’єднанням у вигляді пакетів обміну [8].

**Висновки до другого розділу**

Проведена робота показала, що системи виявлення вторгнень, які використовуються на сьогодні, значною мірою базуються на емпіричних схемах. Тому, проаналізувавши структури СВВ, методи, які використовуються в них, їх переваги і недоліки та підходи до розробки самої СВВ, а також отримані результати проведеного дослідження, можна буде налаштувати якісну та надійну систему захисту інформації. Тим самим конфіденційна інформація, яка обробляється різними інформаційними процесами, не буде змінена, викрадена або спотворена.

На наступному етапі дослідження постає завдання отримання формалізованими методами оптимальної структури СВВ, яка за допомогою програмних і апаратних засобів, зможе функціонувати не конфліктуючи один з одним для можливості подальшого її використання та модернізації. Це дозволить на основі запропонованої методики також провести дослідження та розробити рекомендації щодо побудови систем виявлення мережевих вторгнень і виявлення ознак комп'ютерних атак для підприємства на вибраному прикладі.

**Розділ 3**

**ПРОВЕДЕННЯ ДОСЛІДЖЕННЯ ТА РОЗРОБКА РЕКОМЕНДАЦІЙ ЩОДО ВПРОВАДЖЕННЯ СИСТЕМ ВИЯВЛЕННЯ МЕРЕЖЕВИХ ВТОРГНЕНЬ І ВИЯВЛЕННЯ ОЗНАК КОМП'ЮТЕРНИХ АТАК ДЛЯ ПІДПРИЄМСТВА**

**В ході проведення дослідження пропонується компанія «Sitronics Telecom Solutions Ukraine (STSU)»,** що **проектує, будує та підтримує корпоративні мережі передачі даних для будь-яких підприємств – від середнього і малого бізнесу до найбільших телекомунікаційних операторів. При цьому вона використовує обладнання найбільш передових та кращих компаній, як Fortinet, Cisco Systems, Aruba Networks та інших), що забезпечують максимальний захист серверів і баз даних [10].**

**У системних рішеннях компанії реалізуються як складові технологічна та експлуатаційна безпека. Реалізація вимог технологічної та експлуатаційної безпеки будується на спеціально розробленому для мережі комплексі організаційних, технічних та організаційно-технічних заходів щодо захисту інформації та мережевих ресурсів.**

**В компанії реалізована найсучасніша система забезпечення безпеки інформації (див. рис. 3.1) з використанням:**

* **сучасних та новітніх міжмережевих екранів;**
* **сканерів уразливості мережі та емуляторів атак, що мають базу відомих вразливостей, яка постійно оновлюється;**
* **систем реагування, що дозволяють оперативно відповідати на позаштатні ситуації;**
* **дистанційного WWW-сервера, який здійснює контроль за вмістом запитуваних ресурсів;**
* **дистанційного поштового сервера, який контролює отриманні повідомлення та має можливості пересилати їх;**
* **загальної та єдиної системи управління та контролю за станом інформаційної безпеки.**

**Засоби, що використовує компанія є новітніми розробками та вже не перший рік успішно представлені на ринку захисту інформації. Всі індивідуальні вимоги щодо поновлення систем або концепцій самого рішення враховуються та реалізуються на етапі розробки.**

**Забезпечення безперервного якісного рівня функціонування мережі та її стійкості до внутрішніх і зовнішніх факторів (віруси, атаки і т.п.) досягається за допомогою застосування комплексного рішення на базі, як спеціальних засобів забезпечення безпеки, так і на базі мережевого обладнання.**

**Системи забезпечення інформаційної безпеки містять в собі засоби управління, що дозволяють навіть в момент надзвичайних не прогнозованих ситуацій, змінювати основні показники роботи мережі, що можуть реалізувати можливості:**

* **надання мережевих ресурсів організаціям і користувачам;**
* **контролю та слідкуванням за трафіком;**
* **контроль завантаженості мережі;**
* **контролю взаємодії компонентів у мережі.**

**Мережеві вузли зазвичай будуються на базі обладнання, яке має в своєму складі схеми та резервуючі елементи.**

**Запропонована система забезпечення інформаційної безпеки передбачає можливість обмеження списку станцій управління для кожного з пристроїв і мережевих ресурсів, з яких може здійснюватися доступ до обладнання та управління їм.**

**Одним з найголовніших результатів реалізації комплексу організаційних, організаційно-технічних і технічних заходів щодо захисту інформації та ресурсів у мережі є стійкість використовуваного в проекті обладнання до атак, спрямованих на зупинку та відмову сервісів (DoS - Denial of Service).**

**3.1 Проведення дослідження компанії «Sitronics Telecom Solutions Ukraine»**

**Для наглядного прикладу було проаналізовано елементи структури компанії «Sitronics Telecom Solutions Ukraine» (рис. 3.1).**



**Рис. 3.1. Структура компанії «Sitronics Telecom Solutions Ukraine»**

**Система інформаційної безпеки мережі компанії забезпечує:**

* авторизацію та аутентифікацію користувачів і мережевих пристроїв;
* контроль доступу до мережевих ресурсів;
* контроль мережевих ресурсів;
* захист від відмов в обслуговуванні.

**Завдання, що описані вище, досягаються наступними методами і засобами від компанії** Cisco**.**

CiscoSecure ACS (Cisco Secure Access Control Server) - це програмне забезпечення для адміністрації корпоративних мереж і постачальників послуг, що дозволяє визначити правила доступу - які користувачі мають право доступу у внутрішню мережу або в Інтернет і якими послугами вони можуть скористатися.

Cisco Secure ACS використовується для ідентифікації спільно з іншими пристроями Cisco - серверами доступу по комутованих лініях, маршрутизаторами і міжмережевими екранами. Це дає можливість поєднати в одному місці контроль і авторизацію на серверах комутованого доступу і міжмережевих екранах і контроль над управлінням комутаторами і маршрутизаторами. При використанні Cisco Secure ACS адміністратори мережі можуть проконтролювати наступні етапи:

-аутентифікацію (хто може увійти в мережу);

-авторизацію (які права має кожен користувач);

-облік (яку інформацію про діяльність користувача потрібно зберегти для майбутнього використання).

Cisco Secure ACS випускається для платформ Windows. Функціонально Cisco Secure ACS служить центральним сховищем обліку та аудиту. Інформацію про всі сесії, встановлених користувачами, можна повністю записати в базу даних, а потім використовувати в цілях визначення політик безпеки, планування зростання мережі або для ведення обліку та оплати використання мережевих ресурсів.

Cisco Secure ACS дозволяє централізувати контроль і облік роботи користувачів з такими компонентами мережі як сервера доступу, віртуальні приватні мережі (VPN), міжмережеві екрани (firewall), IP-телефонія, маршрутизатори і комутатори. Використовуючи це обладнання, мережеві адміністратори можуть легко управляти користувача обліковими записами, а також змінювати рівні безпеки і мережевого захисту для цілих груп користувачів.

Для забезпечення безпечної маршрутизації у мережі використовуються механізми для її цілісності та запобігання атак на руйнування мережі шляхом застосування помилкових маршрутів. Ідентифікація та підтвердження маршрутів пакетів гарантує, що оновлення виходять від перевіреного джерела і що ніякі дані не зіпсовані. Вона використовує шифрування, односторонню хеш-функцію для забезпечення ідентифікації робочого місця і цілісності змісту відновлення маршрутизації.

Стійкість до відмови в обслуговуванні мережевих елементів повинна розглядатися в двох виглядах: можливості самого обладнання до стійкості таможливості обладнання до стійкості під впливом зовнішніх мережевих впливів.

Перше питання розглядається у розділах проектної документації, що описує технічні характеристики обладнання. Друге питання відноситься до питань забезпечення інформаційної безпеки і передбачає проведення комплексу організаційно-технічних заходів щодо захисту обладнання і елементів мережі від атак типу «DoS».

Проведений аналіз свідчить, що система інформаційної безпеки мережі компанії не забезпечує виявлення мережевих вторгнень і виявлення ознак комп’ютерних атак в сучасних умовах. Для вирішення цього питання пропонуються впровадити в систему інформаційної безпеки мережі окремі спеціальні пристрої від відомих IT-компаній (Cisco і інші).

**3.2 Рекомендації щодо впровадження систем виявлення мережевих вторгнень і виявлення ознак комп’ютерних атак**

Пропонується типовий варіант побудови корпоративної мережевої системи із забезпеченням безпеки компанії «**Sitronics Telecom Solutions Ukraine**» на базі корпоративного рішення СВВ, з урахуванням рекомендацій від CiscoSystems (рис. 3.2).



Рис. 3.2. Загальна схема побудови рішення СВВ

Структурні елементи впровадження систем виявлення мережевих вторгнень і виявлення ознак комп’ютерних атак, як рекомендації для **компанії «Sitronics Telecom Solutions Ukraine», представлені в табл. 3.1**

**Таблиця 3.1**

Структурні елементи впровадження СВВ для компанії

«Sitronics Telecom Solutions Ukraine»

|  |  |  |
| --- | --- | --- |
| **№** | Призначення елементів | **Елементи** СВВз використанням CiscoSystems |
| **1** | Моделі «міжмережевих екранів» з функцією резервування данних | Cisco PIX-515Е, Cisco PIX-525 або Cisco PIX-535 з підтримкою портів FastEthernet або GigabitEthernet |
| **2** | Системи виявлення атак або системи запобігання вторгнень | Серії Cisco IDS 4200 або  **Cisco IPS 4200, які мають порти FastEthernet або GigabitEthernet** |
| **3** | Належна система захисту на рівні серверів | «Host based IDS» (системи виявлення вторгнень на рівні хоста) серії Cisco Security Agent на критичні сервера |
| **4** | Комплексне управління елементами забезпечення безпеки | Спеціалізована система управління Cisco VPN Management Solutions (VMS) - в зоні серверів аутентифікації та управління. |
| **5** | Використання сервера аутентифікації | Cisco ACS - в зоні серверів аутентифікації та управління. |
| **6** | Забезпечення безпечного підключення та доступу до публічної мережі (Інтернет і електронної пошти ) | Розміщення зовнішніх серверів (SMTP, WWW, Proxy) та внутрішніх серверів в окремі мережеві зони, що контролюються міжмережевими екранами(до Інтернет і електронної пошти - за допомогою серверів Proxy Proxy або SMTP - relay агенти) |
| **7** | Забезпечення захисту в офісах, віддалених від головного, та для дистанційних співробітників (побудова системи забезпечення інформаційної безпеки) | Варіант 1.Рішення на базі інтегрованої в маршрутизатор функції міжмережевого екрану (маршрутизатори серій Cisco 800, 1800, 2800 і вище) і системи виявлення атак (NM-CIDS-K9 для серій Cisco 2800 і вище)  Варіант 2. Рішення для забезпечення високого рівня безпеки корпоративної мережі- на окремих її компонентах з більшою надійністю і безпекою (маршрутизатори серії Cisco 800, 1800 і вище, а в якості міжмережевих екранів Cisco PIX-501, Cisco PIX-506Е або вище. Мережеві системи виявлення/запобігання атак (IDS / IPS) або host based IDS (Security Agent)  Для підключення дистанційних користувачів - використання зовнішнього VPN пристрою, Cisco PIX Firewall або маршрутизатора зі спеціалізованим ПЗ в центральному офісі та програмним забезпеченням Cisco VPN клієнтів, на робочих місцях користувачів. |

Щоб запровадити таке рішення, в головному офісі рекомендується використовувати моделі «міжмережевих екранів» з функцією резервування та відновлення даних, такі як Cisco PIX-515Е, Cisco PIX-525 або Cisco PIX-535 з підтримкою портів FastEthernet або GigabitEthernet. Міжмережеві екрани цих серій дозволяють здійснювати гнучке налаштування політик безпеки та при цьому мають продуктивність та надійність відносно до конкретного вузла мережі.

Щоб мати можливості комплексного захисту, рекомендується встановлення систем виявлення атак серії Cisco IDS 4200 або систем запобігання вторгнень Cisco IPS 4200, які мають порти FastEthernet або

GigabitEthernet і розраховані на різні швидкості для аналізу трафіку.

Потрібно пам`ятати, що рекомендується розміщувати сенсори як на зовнішньому периметрі доступу в публічні мережі так і найбільш критичних ресурсів мережі компанії з метою запобігання вторгнення та несанкціонованого доступу до ресурсів, що перебувають під захистом. Однією з переваг встановлення IPS системи є те, що вона може працювати в декількох режимах:

- pежим виявлення вторгнень (відбувається аналіз трафіку без участі самого пристрою, а для того щоб заблокувати трафік потрібно мати зовнішні пристрої, такі як брандмауер або маршрутизатор;

- режимі запобігання вторгнень (при аналізі трафіку сам пристрій бере участь в цьому та може здійснювати його блокування без додаткових зовнішніх пристроїв);

- змішаний режим - режим виявлення вторгнень й режим запобігання вторгнень (система запобігання вторгнень працює для однієї ділянки мережі, система виявлення вторгнень для іншої ділянки мережі).

**Також, є можливість підключити систему запобігання вторгнень та атак в гібридному режимі, що** дозволить використовувати її в якості інтерфейсу брандмауера, який насамперед буде під`єднуватися до корпоративної мережі виконуючи роль системи виявлення вторгнень на маршрутизаторі.

Для забезпечення належної системи захисту на рівні серверів рекомендується встановлення «Host based IDS» (систем виявлення вторгнень на рівні хоста) серії Cisco Security Agent на критичні сервера, що може виявити несанкціоновану активність на рівні сервера або робочої групи.

Для забезпечення комплексного управління елементами забезпечення безпеки рекомендується використання спеціалізованої системи управління Cisco VPN Management Solutions (VMS), що розміщується в зоні серверів аутентифікації та управління.

Щоб мати змогу аутентифікувати користувачів та мережеві пристрої використовуються сервера аутентифікації, такі як, Cisco ACS, що розміщуються в зоні серверів аутентифікації та управління.

Однією з рекомендацій є розміщення зовнішніх серверів (SMTP, WWW, Proxy) та внутрішніх серверів також в окремі мережеві зони, що контролюються міжмережевими екранами. Це рішення має на меті забезпечити безпечне підключення та безпечний доступ до публічної мережі.

Наприклад, доступ в Інтернет і до електронної пошти здійснюється за допомогою серверів Proxy через так звані Proxy або SMTP - relay агенти.Їх принцип функціонування взагалі полягає в тому, що всі запити від внутрішніх клієнтів перенаправляються на внутрішні сервера WWW і SMTP, потім вже внутрішні сервери WWW і SMTP взаємодіють через міжмережеві екрани зовнішніх серверів WWW і SMTP що розміщуються в зовнішній зоні. І тільки зовнішні сервера WWW і SMTP зв`язуються безпосередньо з Інтернет серверами через міжмережевий екран.

Цим способом можливе здійснення повного контролю над інформацією, що проходить, виключаючи взаємодію користувачів локальної мережі з Інтернет мережею. Це дозволяє значно збільшити загальну безпеку корпоративної мережі.

**Щоб забезпечити захист в офісах, які є віддаленими від головного та для дистанційних співробітників пропонується використовувати три типові побудови системи для забезпечення інформаційної безпеки:**

- рішення на базі інтегрованої в маршрутизатор функції міжмережевого екрану і систему виявлення атак, який дозволяє забезпечити надійний рівень безпеки в порівнянні з базовими системами безпеки. Цей варіант рекомендується застосовувати при обмежених коштах і в бюджетних рішеннях. В таких випадках можна використовувати маршрутизатори серій Cisco 800, 1800, 2800 і вище. Щоб реалізувати функції систем виявлення атак можливе використання спеціалізованого модуля мережної системи виявлення атак NM-CIDS-K9 для серій Cisco 2800 і вище.

- рішення, яке базується на окремих компонентах та володіє більшою надійністю і безпекою, оскільки функції маршрутизації і забезпечення безпеки реалізовані на різних пристроях. Таке рішення рекомендується для використовування в разі необхідності забезпечити високой рівень безпеки корпоративної мережі. Для такого використання підійдуть маршрутизатори серії Cisco 800, 1800 і вище, а в якості міжмережевих екранів Cisco PIX-501, Cisco PIX-506Е або вище.

Якщо потрібно, то можна встановити мережеві системи виявлення/запобігання атак (IDS / IPS) або host based IDS (Security Agent).

Щоб організувати підключеннядистанційних користувачів, рекомендується використання зовнішнього VPN пристрою, Cisco PIX Firewall або маршрутизатора зі спеціалізованим ПЗ в центральному офісі та програмним забезпеченням Cisco VPN клієнтів, на робочих місцях користувачів. Це дозволить забезпечити захищене підключення, в тому числі і по публічним каналам зв'язку в Інтернеті. Важливим є те, що дане рішення є одним з типових, а в реальних проектах можливе використання інших схем та методик забезпечення безпеки в залежності від бажаного результату, поставлених цілей та бюджету.

**Висновки до третього розділу**

У третьому розділі розглянуті та надані рекомендації щодо можливого захисту корпоративної мережі для запобігання мережевих або комп’ютерних атак на інформаційну систему і інформацію, що циркулює в ній, - на прикладі компанії «Sitronics Telecom Solutions Ukraine (STSU)».

Було рекомендовано раціональне використання, в залежності від необхідності, таких пристроїв як Cisco PIX-515Е, Cisco PIX-525,що дозволяє розробляти гнучкі політики безпеки, створити велику кількість нейтральних зон (DMZ), поряд з високою продуктивністю і надійністю будь-якого критичного вузла в мережі.

Проведений аналіз та запропоновані рекомендації дозволяють побудувати захищену систему безпеки, якщо використовувати на вибір з

де-кілька досліджених їх варіантів, в залежності від спеціальних потреб.

**ВИСНОВКИ**

1. В результаті роботи були досліджені методичні матеріалі щодо характеристик систем виявлення мережевих вторгнень і виявлення ознак комп`ютерних атак на підприємстві. Було вивчено види мережевих вторгнень і ознаки сучасних комп`ютерних атак та досвід використання їх виявлення на підприємстві. Такими найпоширенішими атаками з DoS і DDoS атак є: повені TCP SYN атака , smurf атака, teardrop атака, атака пінг - смерті та ботнети. З атак Man-in-the-middle розповсюджені: викрадення сесії, спуфінг, фішинг атаки, підслуховування.

Також, ознайомившись з можливостями систем виявлення, стало зрозумілим як можуть орудувати зловмисники та як саме можна протидіяти атакам на інформаційну безпеку. Так система виявлення вторгнень, яка відстежує такі види шкідливої ​​діяльності, як DoS атаки, сканування портів або навіть спроби проникнення в мережу, Дієвою СВВ слід вважати ту, яка функціонує в реальному часі та здійснює моніторинг трафіку мережі, а також відстежує аномалії, як в трафіку так і в діях користувачів і системи. Для цього в системі відповідно повинні діяти системи моніторингу та прогнозу network-based (NIDS) і host-based (HIDS).

2. Були переглянуті основні методичні підходи щодо використання систем виявлення мережевих вторгень і виявлення ознак комп`ютерних атак на підприємстві. Засоби, за допомогою яких проводяться сучасні атаки, можна поділити на три групи: віруси та хробаки, троянські програми, мережеві атаки. Були проаналізовані основні системи для виявлення вторгнень від різноманітних компаній, які дозволяють виявити атаки, такі як трасування мережі, розпізнавання портів, стеків ТСР, атаки типу відмови в обслуговуванні, використання вірусів і хробаків,атаки на вразливості операційної системи чи окремих додатків. Також, була визначена класифікація атак, їх види, ознаки та механізми реалізації. Проаналізована сучасна СВВ, яка повинна включати такі підсистеми: підсистема збору інформації про систему, яка підлягає захисту; підсистема аналізу для пошуку атак та вторгнень в систему; підсистема представлення даних для контролю системи в режимі реального часу. Був розглянутий підхід використання систем виявлення вторгнень. Даний підхід дає можливість зіставляти різні засоби захисту і вибрати найбільш раціональні та діючі, з позиції їх можливостей і необхідного рівня захисту інформаційної системи.

3. На основі методичних матеріалів і результату дослідження щодо розробки систем виявлення вторгнень запропонован типовий варіант побудови корпоративної мережевої системи із забезпеченням безпеки на на конкретному прикладі компанії «Sitronics Telecom Solutions Ukraine». Запропоновані рекомендації дозволяють побудувати захищену систему безпеки, якщо використовувати на вибір з де-кілька досліджених їх варіантів, в залежності від спеціальних потреб.

Структурнми елементами впровадження СВВ для компанії «Sitronics Telecom Solutions Ukraine» пропонуються:

* Моделі «міжмережевих екранів» з функцією резервування даних
* Системи виявлення атак або системи запобігання вторгнень
* Належна система захисту на рівні серверів
* Комплексне управління елементами забезпечення безпеки
* Використання сервера аутентифікації
* Забезпечення безпечного підключення та доступу до публічної мережі (Інтернет і електронної пошти )
* Забезпечення захисту в офісах, віддалених від головного, та для дистанційних співробітників (побудова системи забезпечення інформаційної безпеки)

4. Мета роботи досягнута:було проаналізовано та розроблено рекомендації, щодо використання можливостей систем виявлення мережевих вторгнень та ознак комп’ютерних атак в забезпеченні захисту інформації підприємства. Практична значимість дипломної роботи полягає в тому, що її матеріали та результати можуть бути використані при проектуванні системи виявлення вторгнень і раціонального підбору засобів для її побудови.

**СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ**

1. Поляков Д.А. Методичнi пiдходи до аналiзу систем виявлення мережевих вторгнень і виявлення ознак комп'ютерних атак безпеки **/** Д.А. Поляков, Ю.М. Якименко, //Конференція «Цифрова трансформація кібербезпеки», 26 квітня 2020 року. Тези доповідей. — Київ: ДУТ(ННІЗІ), 2020. — С. Х.

2. Поляков Д.А.Застосування системного підходу при організації захисту інформації безпеки **/** Д.А. Поляков, Ю.М. Якименко, //Інтернет-конференція «Актуальні проблеми інформаційної та кібернетичної безпеки», 26 жовтня 2018 року. Тези доповідей. — Київ: ДУТ(ННІЗІ), 2018. — С. 44-45.

3. Global Market Insights Inc. —global market research and management consulting company [URL]: <https://www.gminsights.com/>.

4. Невойт Я.В. Аналіз загроз інформаційної безпеки в період 2015-2016 років /Я.В. Невойт //Сучасний захист інформації №2 .- Київ: ДУТ,– 2017 С.79-84.

5. Головний сайт центру виявлення кіберзагроз . [URL]: http://cert.gov.ua.

6. Бєрковський В.В. Аналіз та класифікація методів виявлення вторгнень в інформаційну систему /В.В. Бєрковський, О.С. Безсонов//Системи обробки інформації, випуск 6 (122).- Харків: 2013- С.122-124.

7. Сєвєрінов О.В. Аналіз сучасних методів атак на автоматизовані системи управління військами та інформаційні мережі/О.В. Сєвєрінов, А.Г. Хрєнов1, А.О. Поляков //Системи обробки інформації, випуск 9.- Харків: 2015, - С.101-104

8. Радченко М.М. Аналіз системи виявлення вторгнень та комп’ютерних атак / М.М.Радченко,О.І. Іванов, С.І., Прохорський, К.К. Мужеський - М.: 2013. [URL]: https://revolution.allbest.ru/programming/00880596\_0.html

9. ЗавадаА.А. Аналіз сучасних систем виявлення атак і запобігання вторгненням / А.А. Завада, О. В. Самчишин, В. В. Охрімчук /М. – 2012 [URL]: <http://ela.kpi.ua/bitstream/123456789/17609/1/meshkov.pdf>

10. Консалтингова компанія Сітронікс Телеком Солюшнс Україна. [URL]: <https://www.stsua.com/ua/>

11. Awake Security —advanced network traffic analysis company that delivers a privacy-aware solution capable of detecting and visualizing behavioral, mal-intent and compliance incidents with full forensics context.

[URL]: <https://awakesecurity.com/glossary/network-intrusion/>.

12. Cloudflare, Inc.—an American web-infrastructure and website-security company, providing content-delivery-network services, DDoS mitigation, Internet security, and distributed domain-name-server services.

[URL]: <https://www.cloudflare.com/learning/ddos/what-is-a-ddos-attack/>.

13.ResearchGate GmbH— company whichallows users to discover scientific knowledge, share and access publications and publish data.

[URL]:https://www.researchgate.net/publication/51910046\_Studying\_and\_Classification\_of\_the\_Most\_Significant\_Malicious\_Software

14.Webopedia—an online tech dictionary for IT professionals, educators and students.

[URL]:<https://www.webopedia.com/TERM/A/application_gateway.html>

15.Imperva Inc.— a cyber security software and services company which provides protection to enterprise data and application software.

[URL]:https://www.imperva.com/learn/application-security/phishing-attack-scam/