**Міністерство освіти і науки України**

**«Київський національний університет імені Тараса Шевченка»**

**Факультет інформаційних технологій**

**Кафедра кібербезпеки та захисту інформації**

# ПОЯСНЮВАЛЬНА ЗАПИСКА

**Дипломної роботи**

***магістра***

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

**спеціальність** *125 Кібербезпека*
(код і назва спеціальності)

**освітній рівень** ***магістр***
(назва освітнього рівня)

**кваліфікація** _____
(код і назва кваліфікації)

**на тему:** *Розробка рекомендацій по вибору систем виявлення вторгнень для компаній малого та середнього бізнесу*

**Виконавець: студента** ***2*** **курсу, групи** ***КБм-21***

***Бистрова Олександра Володимировича***

(підпис) (прізвище ім'я по-батькові)

| | **Прізвище, ініціали** | **Оцінка** | **Підпис** |
|---|---|---|---|
| **Науковий керівник** | *Лукова-Чуйко Н.В.* | | |
| **Рецензент** | _____ | | |
| **Нормоконтроль** | _____ | | |

**Київ 2021**

**Міністерство освіти і науки України**

**«Київський національний університет імені Тараса Шевченка»**

**Факультет інформаційних технологій**

**Кафедра кібербезпеки та захисту інформації**

**ЗАТВЕРДЖЕНО:**

завідувач кафедри

кібербезпеки та захисту інформації

_____ Лукова-Чуйко Н.В.

«_____»_____20___року

**ЗАВДАННЯ**

**на виконання дипломної роботи**

**спеціальності** *125 Кібербезпека*

(код і назва спеціальності)

**студенту** *КБм-21* *Бистров Олександр Володимирович*

(група) (прізвище ім'я по-батькові)

**Тема дипломної роботи** *Розробка рекомендацій по вибору систем виявлення вторгнень для компаній малого та середнього бізнесу*

**1. ПІДСТАВИ ДЛЯ ПРОВЕДЕННЯ РОБОТИ**

Рішення засідання кафедри кібербезпеки та захисту інформації факультету інформаційних технологій протокол №_____ від _____

**2. МЕТА ТА ВИХІДНІ ДАНІ ДЛЯ ПРОВЕДЕННЯ РОБІТ**

**Об'єкт досліджень** *Процес розробки рекомендацій по вибору системи виявлення вторгнень*

**Предмет досліджень** *Методи та засоби вибору систем виявлення вторгнень*

**Мета** *Розробити рекомендації по вибору системи виявлення вторгнень для малого та середнього бізнесу*

**Вихідні дані для проведення роботи** *Сучасне законодавство України в сфері кібербезпеки, Технічні вимоги до систем виявлення вторгнень,*

## 3. ОЧІКУВАНІ НАУКОВІ РЕЗУЛЬТАТИ

**Наукова новизна** *Розробка методу вибору системи виявлення вторгнень для малого та середнього бізнесу*

**Практична цінність** *Використання рекомендацій по вибору системи виявлення вторгнень*

## 4. ВИМОГИ ДО РЕЗУЛЬТАТІВ ВИКОНАННЯ РОБОТИ

## 5. ЕТАПИ ВИКОНАННЯ РОБОТИ

| **Найменування етапів робіт** | **Строки виконання робіт (початок-кінець)** |
|---|---|
| 1. Уточнення постановки задачі | 20.09.2020 – 19.10.2020 |
| 2. Збір даних | 22.10.2020 – 14.01.2021 |

| | |
|---|---|
| 3. Розробка 1 розділу | 15.01.2021 – 25.03.2021 |
| 4. Розробка 2 розділу | 26.03.2021 – 02.04.2021 |
| 5. Розробка 3 розділу | 03.04.2021 – 25.04.2021 |
| 6. Оформлення атестаційної роботи | 26.04.2021 – 02.05.2021 |

## 6. РЕАЛІЗАЦІЯ РЕЗУЛЬТАТІВ ТА ЕФЕКТИВНІСТЬ

**Економічний ефект** *Зниження затрат на впровадження систем виявлення вторгнень на підприємстві малого та середнього бізнесу*

**Соціальний ефект** *Покращення стану захищеності інформаційних систем на конкретному підприємстві*

## 7. ДОДАТКОВІ ВИМОГИ

Завдання видав _____ _____

(підпис) (прізвище, ініціали)

Завдання прийняв

до виконання _____ _____

(підпис) (прізвище, ініціали)

Дата видачі завдання: _____

Термін подання дипломної роботи до ЕК _____

# РЕФЕРАТ

Пояснювальна записка має 7 рисунків, 1 таблицю, 1 додаток та 40 джерела.

Загальний обсяг роботи складає 77 сторінок.

Об’єкт дослідження – процес розробки рекомендацій по вибору системи виявлення вторгнень.

Предмет дослідження - методи та засоби вибору систем виявлення вторгнень.

Мета роботи – розробити рекомендацій по вибору системи виявлення вторгнень для малого та середнього бізнесу.

Методи дослідження – методи порівняння, структурний аналіз, системний підхід.

У роботі досліджено сучасні систем виявлення вторгнень, комплекс вимог до їх функціоналу; комплекс вимог до структури ефективної системи виявлення вторгнень.

Практичне значення роботи полягає у використанні розроблених критеріїв по вибору системи виявлення вторгнень та надання рекомендацій для підприємств малого та середьного бізнесу. Результати здійснених у дипломній роботі досліджень можуть бути використані на підприємствах малого та середьного бізнесу.

Наукова новизна дослідження полягає у розробці рекомендацій по вибору системи виявлення вторгнень на підприємстві малого та середнього бізнесу.

Напрямки подальших досліджень: вдосконалення методу виявлення вторгнень для малого та середнього бізнесу.

Ключові слова: системи виявлення вторгнень, загрози, аналіз трафіку, IDS, персональні дані, мережеві атаки.

# ПЕРЕЛІК УМОВНИХ СКОРОЧЕНЬ

| | |
|---|---|
| **БД** | база даних |
| **ІБ** | інформаційна безпека |
| **ІС** | інформаційна система |
| **ІТС** | інформаційно-телекомунікаційна система |
| **КЗЗ** | комплекс засобів захисту |
| **ОС** | операційна система |
| **СВО** | Система виявлення вторгнень |

# ЗМІСТ

# ВСТУП

Стрімка популяризація і, відповідно, розвиток мереж значно ускладнила обчислювальні системи і зробили їх пов'язаними відносно один одного, отже, менш захищеними від шкідливої діяльності. Зростання рівня автоматизації процесів обробки, зберігання і передачі інформації також позначається на виникненні проблем щодо забезпечення безпеки, а витрати на покриття збитків від діяльності зловмисників постійно збільшуються.

Варто відзначити, що складається стійка тенденція до збільшення кількості атак на обчислювальні системи і мережі - способи і методики віддаленого впливу постійно вдосконалюються, а існуючі системи захисту не дозволяють своєчасно реагувати на зміни в цій сфері, тому що спочатку потрібно виявити, а потім і вивчити мережеву атаку. Через це немає можливості повністю виключити шкідливий трафік. Ці обставини надають великого значення питанням вироблення ефективних методик виявлення несанкціонованого трафіку і розробки актуальних засобів захисту інформації.

Актуальність обраної теми обумовлена тим, що на поточний момент активно розробляються і застосовуються різні методи по виявленню і запобіганню вторгнень, але вони не завжди є ефективними на практиці. Внаслідок цього всі технології захисту постійно вивчаються і поліпшуються. Існуючі системи об'єднує спільна риса - захист локальної мережі від зловмисного впливу ззовні.

У даній роботі розглядається побудова аналітики внутрішнього трафіку таким чином, щоб на основі неї адміністратор міг прийняти рішення про прийняття своєчасних дій і тим самим захистити зовнішню мережу від впливу з локальної мережі. Якщо поширити таку схему в роботі більшості підмереж, то забезпечення безпеки мережевої інфраструктури вийде на новий рівень.

Метою роботи є розробка методу вибору системи виявлення вторгнень для малого та середнього бізнесу.

Мета обумовлена вирішенням наступних задач:

провести аналіз сучасних систем виявлення вторгнень;

визначити комплекс вимог до сучасних систем виявлення вторгнень;

визначити проблематику вибору систем виявлення вторгнень для малого та середнього бізнесу

розробити базові критерії по вибору системи виявлення вторгнень для підприємств;

розробити план вибору системи виявлення вторгнень;

розробити базовий план впровадження системи виявлення вторгнень на підприємстві

розробити рекомендації по вибору системи виявлення вторгнень на підприємстві малого та середнього бізнесу.

Об’єктом дослідження є процес розробки рекомендацій по вибору системи виявлення вторгнень..

Предметом дослідження є методи аналізу систем виявлення вторгнень.

Методом дослідження є методи порівняння, структурний аналіз, системний підхід.

Практичне значення роботи полягає у використанні розроблених критеріїв по вибору системи виявлення вторгнень та надання рекомендацій для підприємств малого та середьного бізнесу. Результати здійснених у дипломній роботі досліджень можуть бути використані на підприємствах малого та середьного бізнесу.

Наукова новизна дослідження полягає у розробці рекомендацій по вибору системи виявлення вторгнень на підприємстві малого та середнього бізнесу.

Апробація результатів роботи та публікації надаються в додатку А.

# РОЗДІЛ 1
# АНАЛІЗ СУЧАСНИХ СИСТЕМ ВИЯВЛЕННЯ ВТОРГНЕНЬ

Системи виявлення вторгнень (СВВ) (Intrusion Detection System (IDS)) – це сукупність програмних і/або аппаратних засобів, що слугують для виявлення фактів несанкціонованого доступу в комп'ютер або компьютерну мережу, а також запобігання неавторизованого управління ними.

Виявлення вторгнень – атак) - це процес моніторингу подій, що відбуваються в комп'ютерній системі мережі з метою пошуку ознак можливих інцидентів.

## **1.1.** Види систем виявлення вторгнень

Системи виявлення вторгнень використовуються для виявлення деяких типів шкідливої активності, яка може негативно вплинути на безпеку комп'ютерної системи. До такої активності відносяться мережеві атаки проти вразливих сервісів, атаки, спрямовані на підшення привілеїв, неавторизований доступ до важливих файлів, а також дії шкідливого програмного забезпечення (комп'ютерних вірусів, троянів і черв'яків).

Традиційні методи виявлення вторгнень засновані на великих знаннях про атаку, наданих експертами-людьми. База даних підписів повинна бути переглянута вручну для кожного нового виявленого вторгнення. Істотне обмеження методів, заснованих на підписах, полягає в тому, що вони не можуть виявити нові атаки. Крім того, хоча виявляється нова атака та розробляється її підпис, часто існує значна затримка при його розгортанні. Ці обмеження призвели до зростання інтересу до методів виявлення вторгнень, заснованих на аналізі даних.

Метою системи виявлення вторгнень є попередження системного адміністратора щоразу, коли зловмисник намагається проникнути в мережу. IDS

визначає атаки через таблицю сигнатур: якщо поточна діяльність відповідає сигнатурі, піднімається сигнал тривоги. Тисячі організацій залежать від таких систем, оскільки їх легко зрозуміти, дозволити адміністраторам налаштувати базу даних підписів та надати конкретну інформацію про події, що відбулися.

На жаль, дослідження та досвід показали, що зловмисники можуть ефективно уникнути майже будь-яку IDS.

Зловмисники можуть приховати атаку двома основними способами:

- змінити спосіб доставки атаки, наприклад, розділивши атаку на безліч мережевих пакетів.
- змінити корисне навантаження атаки таким чином, що воно більше не відповідає підпису IDS, наприклад, використовуючи інше кодування URL-адрес.

На відміну від аналітиків протоколів безпеки, які використовують формальні моделі загроз для оцінки стійкості протоколу проти атак, аналітики IDS проводять свою оцінку за допомогою спеціальних методів та інструментів.

Останнім часом застосування користувачами систем виявлення вторгнення активно набирає популярність. IDS – найважливіший елемент інформаційної безпеки, необхідний кожному далекоглядному користувачеві. Система виявлення вторгнень дозволяє не тільки виявити комп'ютерну атаку і блокувати її, але і виконати це в зручному графічному інтерфейсі – від користувача не потребується спеціальних знань про мережеві протоколи і можливі вразливості.

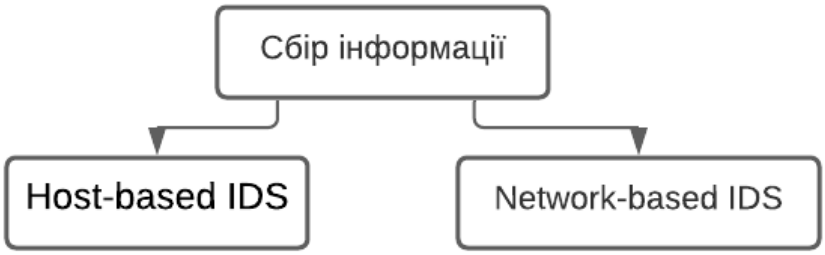


Рисунок 1.1 - Типи систем виявлення вторгнень

Host-based IDS (хостова, або локальна) HIDS теоретично може працювати з будь-яким типом трафіку, включаючи початково зашифрований.

Network-based IDS (мережева) мережева IDS не використовує ресурси процесора і пам'ять, що захищаються.

Системи на основі хостів (HIDS) були першим типом IDS, який було розроблено та впроваджено. Ці системи збирають та аналізують дані, що надходять на комп’ютері, на якому розміщена послуга, наприклад, веб-сервер. Після того як ці дані агрегуються для даного комп’ютера, їх можна або проаналізувати локально, або надіслати на окрему центральну машину аналізу. Одним із прикладів системи, що базується на хості, є програми, які працюють у системі та отримують журнали аудиту програми або операційної системи. Ці програми є високоефективними для виявлення зловживань інсайдерами. З нижньої сторони системи на основі хостів можуть стати громіздкими. Маючи кілька тисяч можливих кінцевих точок у великій мережі, збір та агрегування окремої конкретної комп’ютерної інформації для кожної окремої машини може виявитись неефективним.

Можливі реалізації IDS на основі хоста включають журнали подій безпеки Windows NT/2000, джерела аудиту RDMS, Enterprise Management, дані аудиту систем (наприклад, Tivoli) та UNIX Syslog у вихідних формах або у захищених формах, таких як BSM Solaris; комерційні продукти, що базуються на хості, включають RealSecure, ITA, Squire та Entercept.

На відміну від моніторингу діяльності, що відбувається в певній мережі, мережеве виявлення вторгнень аналізує пакети даних, які рухаються по фактичній мережі. Ці пакети вивчаються та іноді порівнюються з емпіричними даними, щоб перевірити їх природу: шкідливі чи доброякісні. Вони мають інтерактивний інтерфейс у безладному режимі. Оскільки вони відповідають за моніторинг мережі, а не одного хоста, мережеві системи виявлення вторгнень (NIDS), як правило, більш розподілені, ніж IDS, що базуються на хості. Замість аналізу інформації, яка походить і знаходиться на комп'ютері, мережеві IDS витягують дані з TCP/IP або інших пакетів протоколів, що рухаються по мережі. Це спостереження за зв’язками

між комп’ютерами робить мережеві IDS чудовими для виявлення спроб доступу поза межами надійної мережі. Загалом, мережеві системи найкраще виявляють такі дії:

- Несанкціонований доступ сторонніх: коли неавторизований користувач успішно входить у систему або намагається увійти, їх найкраще відстежувати за допомогою IDS на основі хосту. Однак виявлення неавторизованого користувача перед спробою входу в систему найкраще здійснити за допомогою мережевих IDS.
- Крадіжка пропускної здатності, відмова в обслуговуванні: Ці атаки поза мережею виділяють мережеві ресурси на зловживання або перевантаження. Пакети, що ініціюють / несуть ці атаки, найкраще помітити за допомогою мережевих IDS.

Деякі можливі недоліки мережевих IDS включають зашифровані корисні навантаження пакетів і високошвидкісні мережі, які обидва стримують ефективність перехоплення пакетів і стримують інтерпретацію пакетів. Прикладами мережевих IDS є Shadow, Snort!, Dragon, NFR, RealSecure та NetProwler.

## 1.2. Типи систем виявлення вторгнень

На сьогоднішній день IDS прийнято класифікувати за кількома параметрами до числа яких можна віднести спосіб збору інформації, метод аналізу інформації, спосіб реагування на загрози і спосіб реалізації.

У мережевої СВВ, сенсори розташовані на важливих для спостереження точках мережі, часто в демілітаризованій зоні, або на кордоні мережі. Сенсор перехоплює весь мережевий трафік і аналізує вміст кожного пакета на наявність шкідливих компонентів. Протокольні СВВ використовуються для відстеження трафіку, що порушує правила певних протоколів або синтаксис мови (наприклад, SQL). У хостових СВВ сенсор зазвичається програмним агентом, який веде

спостереження за активністю хоста, на який встановлений. Також існують гібридні версії перерахованих видів СВВ.

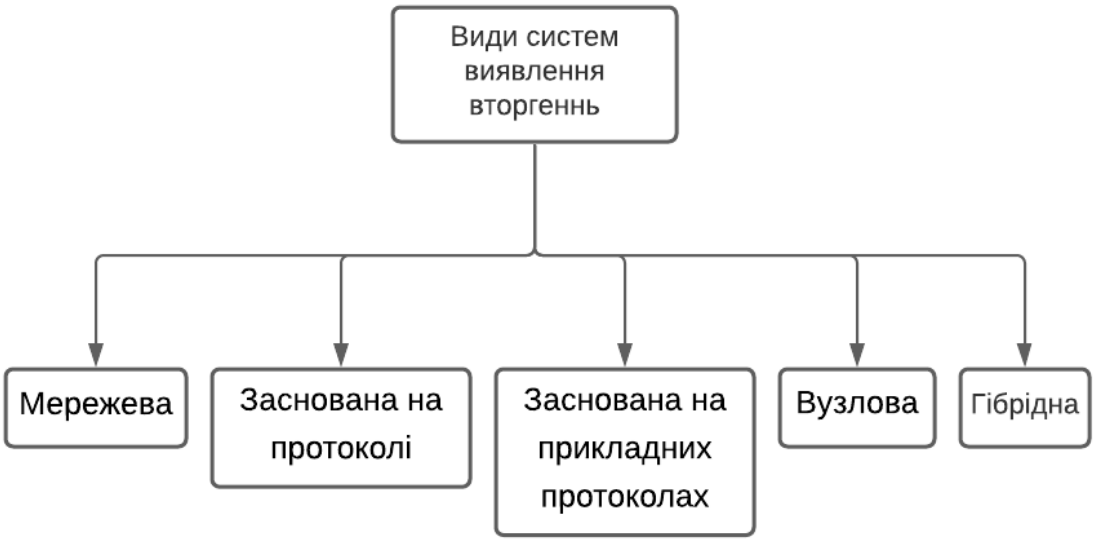


Рисунок 1.2. - Види систем виявлення вторгнень

Мережева СВВ (Network-based IDS, NIDS) відстежує вторгнення, перевіряючи мережевий трафік і веде спостереження за декількома хостами. Мережева система виявлення вторгнень отримує доступ до мережевого трафіку, підключаючись до хабу або свитчу, налаштованому на відзеркалення портів, або мережевий TAP пристрій. Прикладом мережевої СВВ є Snort.

Заснована на протоколі СВВ (Protocol-based IDS, PIDS) являє собою систему (або агента), яка відстежує і аналізує комунікаційні протоколи з пов'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 передається з використанням специфічних для визначених додатків протоколів. Наприклад, на веб-сервері з SQL базою даних СВВ буде відстежувати вміст SQL

команд, що передаються на сервер.

Вузлова СВВ (Host-based IDS, HIDS) – система (або агент), розташована на хості, що відслідковує вторгнення, використовуючи аналіз системних викликів, логів додатків, модифікацій файлів (виконуваних, файлів паролей, 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. В якості прикладу гібридної СВВ можна привести Prelude.

Виходячи з того, що в гетерогенній мережі з високою ймовірністю можуть бути присутні клієнти з різними ОС, помітним мінусом мережевий IDS стає потенційна вразливість до атак, що враховує особливості реалізації різних TCP/IP-стеків, наприклад, при обробці фрагментированного мережевого трафіку.

Відомо кілька різновидів таких атак:

1) FragmentationReassemblyTimeoutattacks – це атаки, що базуються на відмінності тимчасових інтервалів («тайм-аутів») стеків TCP/IP різних ОС при збірці фрагментів. Якщо значення тайм-аутів дефрагментатора IDS відрізняються від відповідних значень на стороні системи, що атакується, для подальшого аналізу буде зібран неправильний потік.

2) TTL Basedattacks – в основному такі атаки реалізуються шляхом генерації помилкових фрагментів, які по задуму не будуть отримані жертвою, але будуть перехоплені і помилково враховані дефрагментатором IDS для поточної сесії. Ситуацію легко відтворити, якщо IDS і об'єкт, що атакується, розташовані в різних мережевих сегментах.

3) OverlappingFragments – при такій атаці відбувається (або не відбувається) перезапис вже отриманих фрагментів дублікатами, що поступають, які мають аналогічний порядковий номер. В результаті сесія на стороні IDS може бути дефрагментована інакше, ніж на боці жертви атаки.

Мережева система виявлення вторгнень може захистити від атак, які

проходять через міжмережевий екран у внутрішню ЛОМ (локальна обчислювальна мережа). Міжмережеві екрани можуть бути неправильно сконфігуровані, пропускаючи в мережу небажаний трафік деяких додатків, який може бути небезпечним. Порти часто переправляються з міжмережевого екрана внутрішнім сервером з трафіком, призначеним для поштового або іншого загальнодоступного сервера. Мережева система виявлення вторгнень може відстежувати цей трафік і сігналізувати про потенційно небезпечних пакетах. Правильно сконфігурована мережева система виявлення вторгнень може перевіряти правила мережевого екрану і надавати додатковий захист для серверів додатків.

Типові особливості системи виявлення вторгнень:

- контролює та аналізує діяльність користувача та системи.
- здійснює аудит системних файлів та інших конфігурацій та операційної системи.
- оцінює цілісність файлів системи та даних
- проводить аналіз закономірностей на основі відомих атак.
- виявляє помилки в конфігурації системи.
- виявляє та попереджає, якщо системі загрожує небезпека.

Мережеві системи виявлення вторгнень корисні при захисті від зовнішніх атак, проте одним з їхніх головних переваг є здатність виявляти внутрішні атаки і підозрілу активність користувачів.

Активні IDS, крім усього перерахованого вище, намагаються протистояти вторгненню. Їх дії можуть включати в себе як розрив поточного зловмисного з'єднання, так і повне блокування атакуючого шляхом зміни конфігурації брандмауера або іншим способом

Пасивні системи в разі ідентифікації вторгнення зазвичай створюють детальний звіт про події, що включає лог мережевої атаки, сповіщають службу безпеки, наприклад, по електронній пошті, і надають рекомендації щодо усунення виявленої уразливості.

За способом реалізації IDS можна розділити на програмні і апаратні. В даний

час більшість виробників програмних засобів захисту для домашніх і корпоративних користувачів пропонують інтегровані рішення, куди включені такі компоненти, як антивірус, антиспам, проактивний модуль і міжмережевий екран, в поєднанні з вбудованою системою виявлення вторгнень.

Підкласи мережевих систем виявлення вторгнень:

- Прозорі мережеві IDS (Transparent Network

IDS – TNIDS) встановлюються в розрив мережевого підключення.

- Сенсорні мережеві IDS (Sensor Network IDS – SNIDS) підключаються до сегменту мережі одним портом і прослуховують трафік, що потрапляє на цей порт. Якщо локальна мережа є комутованою, то підключення сенсорних IDS проводять до дзеркальних портів комутаторів, на які спрямовується необхідний для прослуховування трафік.

### 1.2.1 Системи виявлення аномальної поведінки

Системи виявлення аномальної поведінки (від англ. anomaly detection) засновані на тому, що СОВ відомі ознаки, що характеризують правильне Допустиме поведінку об'єкта спостереження. Під "нормальною»" правильною " поведінкою розуміються дії, що виконуються об'єктом і не суперечать політиці безпеки [3]. Системи виявлення зловмисної поведінки (misuse detection) засновані на тому, що заздалегідь відомі ознаки, що характеризують поведінку зловмисника. Найбільш поширеною реалізацією технології виявлення зловмисної поведінки є експертні системи (наприклад, системи Snort, RealSecure IDS, Enterasys Advanced Dragon IDS). Розглянемо більш детально технології, використовувані в даних системах (рисунок 3) [11].


Рисунок 1.3 - існуючі технології СОВ

Датчики-сенсори аномалій ідентифікують незвичайну поведінку, так звані аномалії, у функціонуванні окремого об'єкта. Тому головна складність в застосуванні їх на практиці пов'язана з нестабільністю самих захищаються об'єктів, а також і взаємодіючих з ними зовнішніх об'єктів. В якості об'єкта спостереження може виступати мережа в цілому, окремий комп'ютер, Мережева служба (наприклад, файловий сервер FTP), користувач і так далі Датчики спрацьовують за умови, що напади відрізняються від «звичайної» (законної) діяльності. Тут варто відзначити, що в різних реалізаціях своє визначення допустимого відхилення для спостережуваного поведінки від дозволеного і своє визначення для «порога спрацьовування» сенсора спостереження. Заходи і методи, зазвичай використовувані у виявленні аномалії, включають в себе наступні [11, с.22]: − порогові значення: спостереження за об'єктом виражаються у вигляді числових інтервалів. Вихід за межі цих інтервалів вважається аномальною поведінкою.

В якості спостережуваних параметрів можуть бути, наприклад: кількість файлів, до яких звертається користувач в даний період часу, число невдалих спроб входу в систему, завантаження центрального процесора тощо. Пороги можуть бути статичними і динамічними (тобто змінюватися, підлаштовуючись під конкретну систему). − параметричні: для виявлення атак будується спеціальний «профіль

нормальної системи» на основі шаблонів (тобто деякої політики, якої зазвичай повинен дотримуватися даний об'єкт); - непараметричні: профіль будується на основі спостереження за об'єктом в період навчання; − статистичні заходи: рішення про наявність атаки робиться за великою кількістю зібраних даних шляхом їх статистичної передобробки; − заходи на основі правил (сигнатур): вони дуже схожі на непараметричні статистичні заходи. У період навчання складається уявлення про нормальну поведінку об'єкта, яке записується у вигляді спеціальних «правил». Виходять сигнатури "хорошого" поведінки об'єкта; - інші заходи: нейронні мережі, генетичні алгоритми, що дозволяють класифікувати деякий набір видимих сенсору-датчику ознак. У сучасних системах виявлення аномалій в основному використовують перші два методи.

Слід зауважити, що існують дві крайності при використанні даної технології: − виявлення аномального поведінки, яке не є атакою, і віднесення його до класу атак (помилка другого роду); − пропуск атаки, яка не підпадає під визначення аномального поведінки (помилка першого роду). Цей випадок набагато небезпечніший, ніж помилкове зарахування аномальної поведінки до класу атак. Тому при установки і експлуатації систем такої категорії звичайні користувачі і фахівці стикаються з двома досить нетривіальними завданнями: − визначення граничних значень характеристик поведінки суб'єкта для зниження ймовірності появи одного з двох вищеописаних крайніх випадків; − побудова профілю об'єкта – це важко формалізуема і витратна за часом завдання, що вимагає від фахівця безпеки великої попередньої роботи, високої кваліфікації і досвіду. Як правило, системи виявлення аномальної активності використовують журнали реєстрації та поточну діяльність користувача як джерело даних для аналізу.

До переваг систем виявлення атак на основі технології виявлення аномальної поведінки можна віднести те, що вони:

- не потребують оновлення сигнатур і правил виявлення атак;
- здатні виявляти нові типи атак, сигнатури для яких ще не розроблені;
- генерують інформацію, яка може бути використана в системах

виявлення зловмисної поведінки.

Недоліками цих систем є наступне:

- генерують багато помилок другого роду
- вимагають тривалого і якісного навчання;
- азвичай занадто повільні в роботі і вимагають великої кількості обчислювальних ресурсів.

### 1.3 Підходи до побудови систем виявлення вторгнень

Існує два підходи до побудови систем виявлення вторгнень:

Виявлення аномалії: Методи виявлення аномалій передбачають, що всі нав'язливі дії обов’язково є аномальними. Це означає, що якби ми могли встановити "нормальний профіль діяльності" для системи, ми могли б, теоретично, позначити всі стани системи, що відрізняються від встановленого профілю, статистично значущими сумами як спроби вторгнення. Однак у цих системах вищий рівень помилкових спрацьовувань (Аномальна діяльність, яка не є нав'язливою, позначається як нав'язлива).

Виявлення неправомірного використання або підпис: Концепція схем виявлення зловживань полягає в тому, що існують способи представити атаки у формі шаблону або підпису, щоб можна було виявити навіть варіації тієї самої атаки. Це означає, що ці системи не схожі на системи виявлення вірусів – вони можуть виявити багато або всі відомі схеми атак, але вони поки мало корисні для поки невідомих методів атак.

### 1.4 Переваги та недоліки різних типів IDS

Переваги IDS:

- Мережа або комп’ютер постійно контролюється на предмет

вторгнення чи нападу.

- Система може бути модифікована та змінена відповідно до потреб конкретних клієнтів і може допомогти зовні, а також внутрішнім загрозам для системи та мережі.
- Ефективно запобігає пошкодженню мережі.
- Забезпечує зручний інтерфейс, який дозволяє керувати системами безпеки.
- Будь-які зміни файлів та каталогів у системі можна виявити та повідомити про них.

Єдиним недоліком систем виявлення вторгнень є те, що вони не можуть виявити джерело атаки, і в будь-якому випадку атаки вони просто блокують всю мережу.

Переваги HIDS:

- може аналізувати зашифровані дані та комунікаційну діяльність;
- повідомляє успішний напад чи ні;
- легко розгортається, оскільки не вимагає додаткового обладнання, отже, це не впливає на усю архітектуру.

Недоліки HIDS:

- Припинить роботу, якщо зламається ОС в результаті атаки;
- не здатні виявляти мережеві шахрайства або атаки DOS;
- як правило, потребує ресурсів.

Переваги NIDS:

- незалежне від навколишнього середовища, тому NIDS не впливатиме на роботи, що проводяться у системі, що захищається.

Недоліки NIDS:

- не вказує, напад був успішним чи ні.
- неможливо аналізувати зашифрований трафік.
- має дуже обмежену видимість всередині хост-машини.

### 1.4.1 Ключові проблеми управління системами NIDS та HIDS

1) Забезпечення ефективного розгортання

Для досягнення високого рівня видимості загроз організації повинні забезпечити правильну установку та оптимізацію технології виявлення вторгнень. Через бюджетні та моніторингові обмеження може не бути практичним розміщувати датчики NIDS та HIDS в IT-середовищі. Однак багатьом організаціям не вистачає повного огляду своєї IT-мережі, ефективне впровадження IDS може бути складним завданням, і якщо воно не буде зроблено належним чином, це може залишити незахищеними критично важливі активи.

2) Управління великим обсягом попереджень

HIDS та NIDS зазвичай використовують комбінацію методів виявлення на основі сигнатур та аномалій. Це означає, що попередження генеруються, коли датчик або виявляє активність, яка відповідає відомій схемі атаки, або позначає трафік, який не входить до списку звичайної поведінки. Аномальна діяльність може включати споживання пропускної здатності та нерегулярний трафік інтернету або DNS.

Величезна кількість попереджень, що генеруються в результаті виявлення вторгнень, може бути значним навантаженням для внутрішніх команд. Багато системних сповіщень є помилковими спрацьовуваннями, але рідко в організацій є час і ресурси для перевірки кожного попередження, а це означає, що підозріла діяльність часто може прослизнути під радаром.

Більшість систем виявлення вторгнень завантажуються набором заздалегідь визначених сигнатур оповіщення, але для більшості організацій їх недостатньо, необхідна додаткова робота для базової поведінки, специфічної для кожного середовища.

3) Розуміння та вивчення попереджень

Попередження IDS складаються з інформації базового рівня безпеки, яка, якщо розглядати її ізольовано, може означати дуже мало. Отримавши

попередження, часто не відразу стає очевидним, що його спричинило, або які дії потрібні, щоб встановити, чи представляє воно справжню загрозу чи ні.

Дослідження попереджень IDS може зайняти дуже багато часу та ресурсів, вимагаючи додаткової інформації від інших систем, яка допоможе визначити, чи є тривога серйозною. Для інтерпретації результатів роботи системи необхідні навички спеціалістів, і багатьом організаціям не вистачає спеціалістів з безпеки, здатних виконувати цю найважливішу функцію.

4) Знання того, як реагувати на загрози

Типовою проблемою для організацій, які впроваджують IDS, є те, що їм бракує відповідної можливості реагування на інциденти. Виявлення проблеми – це половина успіху, однаково важливо знати, як правильно реагувати, і мати на це ресурси.

Ефективне реагування на інциденти вимагає кваліфікованого персоналу служби безпеки, який знає, як швидко усунути загрози, а також надійні процедури вирішення проблем, не впливаючи на повсякденні операції. У багатьох організаціях існує великий розрив між людьми, відповідальними за сповіщення про моніторинг, та тими, хто керує інфраструктурою, а це означає, що швидкого відновлення може бути важко досягти.

Щоб підкреслити важливість створення відповідного плану реагування на події, вхідний Загальний регламент про захист даних (GDPR) вимагає від організацій, які обробляють будь-який тип персональних даних, мати належний контроль, щоб повідомляти про порушення у відповідний орган протягом 72 годин, або ризикувати великим штрафом.

Для вирішення цих проблеми перш ніж застосовувати систему виявлення вторгнень, організації повинні розглянути можливість введення незалежної оцінки ризику, щоб краще зрозуміти своє оточення, включаючи ключові активи, що потребують захисту. Озброєння цими знаннями допоможе забезпечити належний обсяг системи IDS, щоб забезпечити найбільшу цінність та переваги.

Беручи до уваги проблеми постійного обслуговування системи, моніторингу

та розслідування сповіщень, багато організацій, можливо, захочуть залучити керовану службу для виконання всіх важких робіт. Керована служба IDS уникає необхідності набирати спеціалізований персонал служби безпеки, а за необхідності може також включати всі необхідні технології, обходячи потребу в попередніх капітальних витратах.

### 1.4.2 Проблеми технологій виявлення вторгнень

Але і у найкращих технологій виявлення атак виникають проблеми. Основні з них - наступні.

**Розподілене за часом сканування**

Через великий обсяг мережевого трафіку NIDS стає тяжко підтримувати реєстрацію тривалого трафіку. Таким чином, важко виявити "розподілене за часом сканування" (ping sweeps або Port scans), при якому порушники сканують один порт / адресу щогодини.

**Завантажені сегменти**

В даний час NIDS не можуть підтримувати сильно завантажені сегменти, наприклад, 10-Гбіт/сек. Таким чином, в той час як вони яв-ляются придатними для незначно завантажених мереж або WAN-зв'язків, вони мають проблеми з сильно завантаженими сегментами.

**Комутовані мережі**

Комутовані мережі ставлять безліч проблем перед NIDS, а також перед мережевим аналізом взагалі. Є багато рішень цієї проблеми, але вони не завжди є задовільними.

**Вбудовані механізми**

Деякі продукти впроваджені безпосередньо в сам комутатор. Однак це просто посилює проблему, зазначену вище, у випадку сильно завантажених сегментів.

Об'єднавчі плати на задній панелі коммутатора працюють на швидкостях кілька Гбіт / сек.

**Порт зеркалювання**

Багато Комутатори мають " monitor port "(span port, mirror port, managed port) для установки мережевих аналізаторів. NIDS також може бути легко приєднана до цього порту. Очевидна проблема полягає в тому, що порт запускається на набагато нижчій швидкості, ніж об'єднувач-ная плата на комутаторі, тому NIDS не зможе побачити весь трафік на сильно завантаженому сегменті.

**Inter-switch з'єднання**

Оскільки багато комутаторів конфігуруються ієрархічним об-разом, якісне виявлення може бути забезпечене шляхом установки NIDS на з'єднання між комутаторами. Однак більшість NIDS можуть тільки обробляти обмежений обсяг смуги пропускання, і Віро-ятно насичуються в таких випадках.

**Скоординовані атаки з невисокою пропускною здатністю**

Іноді хакери збираються разом і запускають повільне сканування з численних IP-адрес. Це ускладнює діагностику атаки з метою виявлення атак.

Першим комерційним продуктом став в 1990 році Stalker (Haystack Labs) - система виявлення атак на рівні хоста. В цей же час SAIC (Science Applications International Corporation) запропонувала свою версію host-based IDS-CMOS Computer misuse Detection System. Одночасно організацією Air Force Cryptologist Support Center був запропонований продукт ASIM Automated Security Measurement System для відстеження атак на рівні се - ти в підмережі ВПС США. Як це часто трапляється, група, яка вела даний проект, організувала компанію-Wheel Group, першим продуктом ко-торою був IDS NetRanger. Ринок систем IDS почав бурхливо розвиватися з 1997 року. Саме в цей час компанія ISS запропонувала свій продукт під назвою Real Secure. Рік по тому компанія CISCO, усвідомивши доцільність розробки систем IDS, купила продукт NetRanger разом з Wheel Group [16]. Також не

можна обійти увагою об'єднання підрозділів-творців IDS від SAIC і Haystack Labs в компанію з розробки систем IDS - Centrax Corporation.

Необхідно відзначити, що розглянуті системи досить своєчасно відстежують ознаки, за якими можна судити про початок атаки, працюючи за принципом антивірусних програм: відоме ловимо, невідоме немає, тому не має сенсу чекати від таких систем виявлення не-відомих на сьогоднішній день атак. Виявлення невідомої атаки до теперішнього моменту є завданням тяжковирішуваним і межує з областю створення штучного інтелекту і систем адаптивного управління безпекою. Сучасні системи виявлення атак здатні контролювати в реальному масштабі часу мережу і діяльність операційної системи, виявляти несанкціоновані дії і автоматично реагувати на них також практично в реальному масштабі часу. Дані системи можуть аналізувати поточні події з урахуванням подій, що вже відбулися, що дозволяє ідентифікувати атаки, рознесені в часі, і тим самим прогнозувати майбутні події.

## Висновки за розділом 1

Отже, на сьогоднішній день існує дуже багато систем виявлення вторгнень. Такі системи виконують дуже великий спектр задач, від статичного аналізу трафіку і до виявлення атак базуючись на аномальній поведінці і аномальному трафіку. Вибір таких систем великий, але узагальнено вони поділяються на:

- Мережева
- Хостова
- Заснована на протоколі
- Заснована на прикладному протоколі
- Гібридна

Окрім цього, за способом реалізації IDS можна розділити на програмні і апаратні. В даний час більшість виробників програмних засобів захисту для корпоративних користувачів пропонують інтегровані рішення, куди включені такі

компоненти, як антивірус, антиспам, проактивний модуль і міжмережевий екран, в поєднанні з вбудованою системою виявлення вторгнень.

# РОЗДІЛ 2
# ВИЗНАЧЕННЯ ПРОБЛЕМАТИКИ ВИБОРУ СИСТЕМ ВИЯВЛЕННЯ ВТОРГНЕНЬ ТА РОЗРОБКА КРИТЕРІЇВ ОЦІНЮВАННЯ

## 2.1 Проблематика по вибору систем виявлення вторгнень для малого та середнього бізнесу

Коли компанія досягає певних успіхів у своєму бізнесі, виникає реальна загроза її інформаційній безпеці і безперервності бізнесу, пов'язаної з інтересом, який до неї починають проявляти конкуренти. Дані аспекти не тільки визначають актуальність захисту інформації, а й стають найважливішою частиною формування сучасної системи безпеки і безперервності бізнесу. Це питання особливо актуальне в період інформаційної епохи, яка активними темпами змінює постіндустріальну епоху. Технологічну революцію переживає весь світ, що змушує компанії відповідати на її виклики [1-7]. Цілком очевидно, що для успішної протидії загрозам інформаційній безпеці та безперервності бізнесу необхідно, перш за все, зрозуміти основу даного явища, а потім-шукати шляхи вирішення. Дані аспекти визначили актуальність і мету дослідження, яка заключається у виявленні проблем забезпечення інформаційної безпеки і безперервності бізнесу і пошуку можливих напрямків їх вирішення. Як показало дослідження даної проблеми, сучасний бізнес не може існувати без інформаційних технологій [8, 9].

Загальновідомий факт, що близько 70% світового сукупного національного продукту певним чином залежить від інформації, яка зберігається в інформаційних системах. Ні в кого не викликає сумніву і той факт, що повсюдне впровадження комп'ютерів крім безумовної зручності призвело до серйозних проблем, однією з яких є про-блема захисту інформації та забезпечення безпеки бізнесу. Говорячи про вітчизняний бізнес в даному аспекті, відзначимо, що в Росії, на жаль, не проводяться дослідження, спрямовані на виявлення порушень інформаційної безпеки бізнесу.

Пов'язано це з тим, що компанії, постраждалі від хакерських атак, намагаються не афішувати дані факти, а це не дозволяє виявити несанкціоновані проникнення в їх ін-формаційні мережі. Разом з тим з з'являються в засобах масової інформації даних з цієї проблеми випливає, що є велика різноманітність слабких точок в захисті інформаційних атак [10-12]. Крім того, хакерами часто виступають люди, які не мають навіть спеціальної освіти в даній сфері.

Отже, перш за все, необхідно визначитися з тим, яка саме інформація може становити інтерес для конкурентів. Важливість вирішення даного завдання полягає в тому, що від її вирішення залежить ефективність формованої системи захисту безпеки і безперервності. В даному аспекті необхідно провести SWOT-аналіз бізнесу, який дозволить виявити конкурентні переваги, що представляють інтерес як для власного бізнесу, так і для конкурентів [13].

При цьому необхідно врахувати, що в якості конкурентних переваг можуть бути технології, схеми руху фінансових і матеріально-них потоків, стратегії розвитку, нові продукти, персонал, клієнти, партнери і т. д. Крім того, потрібно врахувати, що ця діяльність буде мати сенс тільки в тому випадку, якщо інформація, яку слід захищати, являє дійсний інтерес з боку конкурентів і зусилля по її захисту будуть економічно доцільними. Також необхідно виявити, яку інформацію, в якому обсязі, з якою періодичністю і в якому вигляді все-таки потрібно представляти, щоб уникнути інших негативних наслідків, серед яких найбільш серйозні – поява недовіри з боку контактної аудиторії (споживачі, партнери, органи державного управління і регулювання, ділове середовище бізнесу, інвестори).

Що стосується виявлення осіб і організацій, для яких представляє інтерес інформація про бізнес, то тут слід зазначити, що основну небезпеку для бізнесу з точки зору забезпечення його інформаційної безпеки представляють саме конкуренти, які прагнуть завоювати якомога більші обсяги ринку [14, 15].

Також необхідно окрему увагу приділити таким елементам безпеки і безперервності бізнесу, як можливість знищення та перекручення інформації,

копіювання конфіденційної інформації, за-вкриті або обмеження доступу до інформації, необхідної компанії, несанкціонований доступ до неї і т. д. Окремо слід врахувати той факт, що в компаніях малого і середнього бізнесу досі питання захисту інформації та безперервності бізнесу вирішуються в рамках автоматизації діяльності і не виділяються в окремий напрям [16].

При такому підході в даних компаніях IT-керівники одночасно відповідають і за інформаційну безпеку. Крім того, не всі подібні компанії мають IT-керівників у своїй організаційній структурі. Дослідження дозволило виявити два найбільш актуальні питання, вирішення яких безпосередньо впливає на реалізацію проектів компаній, спрямованих на забезпечення інформаційної безпеки та безперервності бізнесу:

- вартість необхідних продуктів і послуг;
- збереження бюджету на безпеку.

За останні три роки вартість необхідних продуктів і послуг зросла в середньому на 10-20% в основному за рахунок зростання цін по галузі на програмне забезпечення.

Разом з тим має місце і той факт, що продавці ІБ-продуктів (захищені з точки зору вимог інформаційної безпеки продукти) практикують гнучку цінову політику, коли ціна регулюється виходячи з бюджету і потреб конкретного замовника. Такий гнучкий підхід дозволяє продавцям ІБ-продуктів утримувати прийнятний для се-бя рівень прибутковості і зберігати ринкову частку. З іншого боку, підвищення вартості ІБ-продуктів змусило замовників змінити і власний підхід до вибору конкретних управлінських рішень, спрямованих на забезпечення інформаційної безпеки і безперервності бізнесу.

Так, у кожній п'ятій компанії збільшилися терміни реалізації ІБ-проектів, а також подовжився процес вибору ІБ-продуктів. При цьому 14% замовників почали в обов'язковому порядку тестувати рішення до їх набуття, чого раніше не практикувалося. 11% компаній стали замовляти пілотний проект, що дозволяє

замовникам або переконатися в правильності зробленого вибору, або порівняти кілька пропонованих ринком продуктів. Основна перевага пілотного проекту полягає в тому, що він, як правило, є безкоштовним для замовника. Крім того, фахівці компанії-замовника мають можливість в максимальному ступені познайомитися з можливостями впроваджуваних ІБ-продуктів, освоюють і налаштовують їх під власну інфраструктуру. Вони також можуть відмовитися з мінімальними негативними наслідками від експлуатації тих ІБ-продуктів, які не відповідають вимогам. Також фахівці компанії мають можливість оцінити відповідність ДБЖ технічним завданням і власним очікуванням, вони розуміють і оцінюють зручність користування системою.

Слід зазначити, що за кілька останніх років змінилися критерії вибору ІБ-продуктів у двох напрямках: компанії-замовники стали більше уваги приділяти локалізації. Незважаючи на відсутність прямої заборони на поставку іноземних рішень, вітчизняні розробники виявляються в більш вигідній ситуації; предметом предметом більш вдумливого вивчення для компанії-замовника стала вартість рішення. При цьому мова йде не про» прайсову вартість", а про сукупну вартість володіння (ТСО – Total Cost of Ownership).

Зі свого боку відзначимо важливість саме вартісного підходу до вибору рішення. Але незважаючи на це більшість компаній-замовників не використовують не тільки вартісну оцінку, але і ще одну таку важливу метрику, як ROI (return of investment – окупність інвестицій), яка, крім іншого, враховує ще й ефективність закуповуваного ІБ-продукту. Таке ставлення до розглянутих Метриків з боку компаній-замовників викликано перш за все тим, що між «прайсовою ціною» і ТСО різниця досить велика. Збільшення вартості ІБ-продукту викликане, з одного боку, подовженням ланцюжка "Розробник-споживач", а з іншого – і тактикою самих розробників, які роблять ціну привабливою для замовників з одночасним збільшенням плати за технічну підтримку, а також обмежують термін дії ліцензії. Такий підхід з боку розробників призводить до більш високої загальної вартості ТСО. Для ілюстрації вищенаведеної інформації відзначимо, що, наприклад, в

сегменті DLP вартість технічної підтримки варіюється від 20-30% (більшість вендорів) до 50% річної вартості ліцензій.

При цьому і вартість технічної підтримки розбивається також на частини шляхом відділення вартості робіт з оновлення ІБ-продуктів і вартості робіт власне на підтримку. Саме такий підхід розробників до політики ціноутворення на свої продукти і послуги, коли враховуються додатково послуги з установки, налаштування рішень та інших робіт, веде до того, що вартість ТСО стає істотно вище початкової «прайсової вартості» ІБ-продуктів навіть безпосередньо від розробників. Таким чином, з метою скорочення витрат і розробники, і споживачі намагаються більше користуватися прямими каналами. Не варто залишати без уваги таку проблему, як кваліфікація партнерів або відсутність інтересу з їх боку.

Дана обставина не дозволяє впроваджувати дійсно складні рішення корпоративного рівня. Ще одна важлива проблема-політика фінансування інформаційної безпеки та безперервності бізнесу компанії. Дослідження показало, що в цілому більшість компаній не схильна скорочувати витрати на ІБ на шкоду рівню інформаційної небезпеки і безперервності свого бізнесу. Не можна залишити без уваги і такий важливий аспект, як кадри для забезпечення інформаційної безпеки і безперервності бізнесу. У багатьох компаніях відчувається не-хватка кваліфікованих кадрів, а в деяких компаніях взагалі відсутні виділені в організаційній структурі ІБ-підрозділи. Також проблематично знайти якісного ІБ-фахівця з належним досвідом і необхідною для відповідності посади освітою.

Ще один важливий момент, пов'язаний з кадровим забезпеченням, – конфіденційність інформації, до якої має доступ ІБ-фахівець. Особливо даний фактор робить серйозний вплив в разі звільнення даних працівників. Також значущою проблемою є збільшення обсягу роботи ІТ-фахівців, викликане кількома об'єктивними факто-рами, які керівництво компаній не беруть до уваги, оцінюючи витрати на забезпечення інформаційної безпеки та безперервності бізнесу:  збільшення кількості та якості загроз; небажання керівництва з метою економії автоматизувати частину робіт або віддавати їх на аутсорсинг;

- ускладнення і подовження процесу вибору необхідних ІБ-продуктів і ІБ послуг, що викликано великою кількістю пропозицій з боку розробників;
- недостатня кількість співробітників Служби ІБ, за рахунок чого зростає навантаження на кожного з фахівців.

Окремої уваги та відповідного рішення потребує проблема мережевих засобів забезпечення інформаційної безпеки та безперервно-сті бізнесу, які можна розглядати з позиції двох аспектів:  сертифікація засобів криптографічного захисту інформації, що забезпечують захист усіх каналів зв'язку учасників взаємодії; сертифікація міжмережевих екранів, що забезпечують захист доступу до електронних сервісів інформаційних систем учасників взаємодії. Особливо дана проблема стосується необхідності забезпечення безпеки системи Міжвідомчої електронної взаємодії єдиної мережі, що об'єднує Всі федеральні і регіональні інформаційні системи і забезпечує доступність державних електронних послуг. При цьому основні проблеми пов'язані зі збільшенням числа підключаються Систем. При цьому слід зазначити, що дана проблема породжена таким фактором, як стандартизація.

Незважаючи на спроби стандартизації, підключаються системи бувають часто різними, що призводить до численних проблем в процесі їх інтеграції в єдину мережу. Складність вирішення даної проблеми полягає в тому, що досвід вирішення напрацьовується фактично в діючій сесії, що гальмує її роботу. Крім того, в результаті такого оперативного втручання знижується керованість і надійність функціонування окремих елементів системи. У підсумку-реалізована архітектура мережі, в якій центральний вузол грає ключову роль і бере участь практично у всіх етапах взаємодії, стає дуже вразливим до відмов будь-яких систем даного вузла. Крім того, проблема ускладнюється за рахунок того, що в міру збільшення числа підключених систем буквально в геометричній прогресії зростає кількість звернень, оброблюваних в єдиній мережі. Це стосується також розширення переліку

інформації, яка повинна передаватися між організаціями-учасниками в електронному вигляді.

Для більш реального осмислення складності і масштабності даної проблеми відзначимо, що система Міжвідомчої Електронної взаємодії сьогодні включає 85 федеральних, 1300 регіональних і 8600 муніципальних органів влади, а також більше 1000 кредитних організацій, що в цілому становить понад 12 тисяч учасників з тенденцією зростання їх числа. Така кількість учасників єдиної мережі в підсумку дає більше 5 мільярдів запитів на рік, яке також має тенденцію до активного зростання.

Збільшення кількості запитів веде до збільшення кількості звернень до системи, яке становить в середньому більше одного мільйона на годину. Така кількість звернень і запитів робить негативний вплив на діяльність всіх учасників єдиної системи, призводить до більш частої появи порушень в роботі окремих компонентів системи, і особливо її центрального вузла. Таким чином, ми бачимо, що дана проблема породжує нову – необхідність підвищення надійності засобів забезпечення інформаційної безпеки і безперервності бізнесу, якій до сьогоднішнього часу ще не приділяється необхідної уваги. Але ж рішення даної проблеми може бути не найскладнішим – необхідно передбачати наявність резервних каналів зв'язку, які можна і нуж-но використовувати не тільки при виникненні відмови основного каналу, але і як превентивну міру – для балансування навантаження між каналами.

Також хорошим рішенням має стати виявлення пріоритетних трафіків і управління смугою пропускання інформації, проведення повномасштабного навантажувального тестування і перевірка роботи кластерів гарячого резервування пристроїв безпеки. Відзначимо, що подібні роботи з модернізації систем Міжвідомчої електронної взаємодії спрямовані на вирішення цілого ряду важливих завдань, пов'язаних із забезпеченням інформаційної безпеки і безперервності бізнесу: підвищення надійності процесів електронної взаємодії і про-пускової здатності єдиної системи; удосконалення механізмів контролю та моніторингу

єдиних мереж; зниження трудовитрат на підключення нових елементів (компонентів) до єдиної системи.

Так, вже заплановані і певним чином вирішуються питання переходу на георозподілену архітектуру, в результаті чого кожен вузол системи здатний замикати на себе обслуговування частини учасників взаємодії, зберігаючи при цьому інформаційну та функціональну цілісність єдиної системи. Розглянуті проблеми є найбільш істотними і вимагають пошуку відповідних рішень. Як бачимо, всі виявлені методи захисту інформації та безперервності бізнесу слід умовно поділити на такі великі групи, як технічні, організаційно-економічні та управлінські. Не вдаючись в особливості технічних методів, відзначимо, що в основі організаційно-економічних і управлінських методів повинні бути комплексні і економічно обгрунтовані програми забезпечення безперервності бізнесу. При цьому слід розділяти бізнес-процеси компанії: Основні, які орієнтуються на виробництво продукції/послуг, становлять цінність для споживача і забезпечують отримання доходу для компанії; забезпечують, які, по суті, є допоміжними і призначені для забезпечення виконання основних бізнес-процесів.

## 2.2 Визначення критеріїв для вибору систем виявлення вторгнень

Для визначення оптимальної СВВ для підприємства, потрібно розробити критерії за якими будуть порівнюватися ті чи інші системи. Такі критерії умовно можна поділити на 3 групи:

- Критерії менеджменту
- Критерії функціональності
- Тести відповідності

Дані групи критерії дозволять всебічно розглянути СВВ та зрозуміти власникам підприємств чи відповідальним особам, яка з систем підходить саме конкретному підприємству. Неможливість обрати для рекомендації лише одну

систему пов’язана з тим, що при обмеженому бюджеті який виділяється на ІБ, завжди будуть присутні ті, чи інші компроміси і кожне підприємство має робити вибір опираючись поточну ситуацію та можливості.

До критеріїв менеджменту відносяться:

- Поставка
- Ціна
- Можливість надання розробником технічної підтримки
- Наявність офіційного дилера у країні, де знаходиться підприємство
- Компоненти
- Що потрібно для оцінки вартості СВВ

До критеріїв функціональності можна віднести:

- Можливість автоматизованої інвентаризації вузлів мережі
- Стандартні бібліотеки виявлення мережевих аномалій на основі правил
- Створення і зміна користувачем правил виявлення вторгнень мережевого та прикладного рівня
- Виявлення інцидентів і аномалій на прикладному рівні
- Групування подій по типу інцидентів
- Управління групами нових пристроїв на карті топології мережі
- Можливість додавання сигнатур, які створені користувачем у інтерфейсі системи
- Очистка журналу подій
- Можливість резервного копіювання подій
- Ідентифікація та автентифікація користувачів
- Інтеграція з зовнішніми системами класу SIEM
- Кореляція подій безпеки
- Аналіз трафіку без безпосереднього впливу на нього (можливість роботи з копією трафіку через SPAN/TAP порт)
- Формування звітів

Остання група критеріїв, це тести відповідності, по яким можна зробити висновки, чи реагує система на певні події. До таких тестів відносяться:

- Тест на реєстрацію інцидента сканування портів
- Тест на реєстрацію атаки проти веб додатку
- Тест на виявлення атаки проти хоста
- Тест на виявлення нестандратних пакетів

### 2.2.1 Критерії менеджменту

Критерії менеджменту містять в собі метрики, які важливі на стадії планування, тому в основному в них зацікавлений саме менеджмент компанії так, як саме йому першочергово потрібно проаналізувати можливі варіанти. В основному ці критерії орієнтовані на економічні аспекти вибору СВО, а саме:

- Поставка – Вигляд в якому поставляється та чи інша система. Якщо розглядати мережеві СВВ, то вони зазвичай поставляються у вигляді окремого апаратного комплексу з власним ПЗ. Також існують варіанти поставки системи у вигляді пакету ПЗ або образу віртуальної машини, якщо СВВ розгортається у системі віртуалізації
- Можливість надання розробником технічної підтримки – даний критерій часто є одним з ключових так як в такому випадку допускається робота менш кваліфікованого працівника, так як зі складними випадками налаштуванні може допомогти технічна підтримка розробника
- Наявність офіційного дилера у країні, де знаходиться підприємство – це важливий аспект, який дуже часто ігнорується при виборі СВВ. Якщо система поставляється у вигляді програмно-апаратного комплексу, саме офіційний дилер бере на себе частину логістики, та доставляє комплекс від виробника до кінцевого користувача, окрім цього регіональні представництва можуть надавати консультації та допомагати у технічному плані при впроваджені або підтримці СВВ. Окрім цього,

гарантійне обслуговування проводиться набагато швидше у офіційного дилера, ніж у безпосередньо розробника.

- Ціна – один з найважливіших критеріїв вибору СВВ якщо річ йде про малий та середній бізнес. У ціну доцільно включити не лише фактичну ціну при покупці СВВ, а і вартість щомісячного володіння нею, так як у цю вартість також може бути включена підписка на технічне обслуговування СУБД.
- Компоненти – кількість компонентів які відповідають за роботу СВВ. Більшість систем поставляються у вигляді єдиного програмного комплексу, але з розвитком контейнеризації багато розробників все частіше звертають увагу на мікросервісну архітектуру, коли єдина система розбивається на багато сервісів, які відповідають лише за єдину логіку.
- Додаткові засоби забезпечення інформаційної безпеки – наявність такого функціоналу зазвичай робить ціну впровадження набагато вищою. З іншого боку, впровадження комплексного рішення значно підвищує рівень інформаційної безпеки підприємства, а також у порівняні з окремим впровадженням кожного типу, зазвичай становить меншу загальну вартість
- Що потрібно для оцінки вартості СВВ – даний критерій безпосередньо впливає на ціну конкретної системи та відрізняється від розробника до розробника. Більшість вендорів використовують тарифікацію по кількості трафіку який потрібно проаналізувати. Також є варіанти по оцінці вартості за кількістю точок прослуховування трафіку, та кількістю вхідних портів у апаратно програмного комплексу. Наприклад у випадку розподіленої топології де є багато ізольованих один від одного контурів, варіант оцінки вартості за кількістю точок прослуховування трафіку не є економічно вигідним і краще обрати тарифікацію за кількістю трафіку. І навпаки, якщо у підприємства є ядро

мережі, через яке проходить весь трафік, то вигідніше обрати систему, де вартість оцінюється за кількістю точок прослуховування трафіку. У тому ж випадку, але для мереж з малою кількістю трафіку буде доцільно використати систему, де тарифікується кількість портів у апаратно-програмного комплексу.

Дані критерії допоможуть керівництву отримати повну картину того, яка система відповідає вимогам саме конкретного підприємства, та оцінити більшість витрат з якими може зштовхнутися менеджмент при виборі СВВ. Окрім цього для точнішого представлення буде доцільно включити до обговорення технічних спеціалістів так як, для оцінки пріоритетності деяких критеріїв потрібні знання топології мережі, кількості мережевого трафіку та можливі точки входу зловмисника у локальну мережу.

### 2.2.2 Критерії функціональності

Критерії функціональності системи слугують для того, щоб визначити можливості СВВ, та виконати аналіз того, чи відповідає дана система функціональним вимогам підприємства. Дані критерії дадуть змогу технічному спеціалісту зробити перші висновки по можливостям системи та наскільки зручно буде її використовувати для рішення задач ІБ які поставлені на конкретному підприємстві:

- Можливість автоматизованої інвентаризації вузлів мережі – Даний критерій дозволяє створити карту мережі, яка дає можливість спостереження за мережею та в майбутньому полегшити проведення аудиту мережі, так як . Цей критерій також дозволяє виявити вторгнення, коли зловмисник якимось чином отримує можливість підключити власний пристрій до локальної мережі.

- Стандартні бібліотеки виявлення мережевих аномалій на основі правил – цей критерій дозволяє набагато швидше впровадити систему виявлення вторгнень на достатньому рівні, так як зазвичай розробники ПО слідкують за тенденціями світу ІБ та впроваджують оновлення даних списків, яких вистачає для виявлення більшості вторгнень
- Створення і зміна користувачем правил виявлення вторгнень мережевого та прикладного рівня робить систему виявлення вторгнень більш зручною та гнучкою, що дає змогу адаптувати систему під вимоги та загрози конкретного підприємства. На даний момент більшість мають таку можливість.
- Виявлення інцидентів і аномалій на прикладному рівні дає можливість виявити набагато ширший спектр атак, тому бажано, щоб обрана система підтримувала цей критерій. Окрім цього дана функція дозволяє проводити більш глибокий аналіз трафіку, що позитивно впливає на загальний рівень захищеності підприємства
- Групування подій по типу інцидентів – даний критерій полегшує офіцеру ІБ роботу з системою виявлення вторгнень так як стає більш зрозумілим кількість подій які трапляються у мережі за певним типом інциденту. Окрім цього ця функція дає кращий огляд ситуації в системі та кількість унікальних інцидентів які відбулися.
- Управління групами нових пристроїв на карті топології мережі даний функціонал потрібен для правильного та зрозумілого логування подій.
- Контроль цілісності мережі – дає можливість виявити події коли до мережі яка аналізується під’єднуєтьтся новий пристрій, який по суті може бути пристроєм зловмисника. Або ж навпаки, критично важливий елемент мережі перестав відповідати, що також являється подією інформаційної безпеки.
- Можливість додавання сигнатур, які створені користувачем у інтерфейсі системи – цей критерій дозволяє в цілому полегшити роботу офіцера ІБ,

так як для того, щоб зробити це, не потрібно підключатися на самому системи та використовувати утиліти командного рядка, а використати веб-інтерфейс системи виявлення вторгнень або спеціально написаний графічний інтерфейс який взаємодіє з самою СВВ.

- Очистка журналу подій – даний критерій допомагає адміністратору ІБ тримати журнали подій у актуальному стані та видаляти застарілі події
- Можливість резервного копіювання подій – у багатьох систем виникає проблема, коли занадто багато подій накопичується в системі і потрібна більша потужність для того, щоб провести аналіз та кореляцію подій. У даному випадку доцільно мати можливість вивантажити події з системи у подальше місце зберігання (для проведення можливого аудиту в майбутньому ці дані подій потрібно зберегти), що дозволить в цілому розвантажити систему в цілому
- Ідентифікація та автентифікація користувачів – система має мати можливість створювати користувачів системи, бажано з можливістю керуванням правами користувача базуючись на ролях. Даний критерій важливий, так як часто не лише офіцеру ІБ потрібен доступ до системи, а надавати повний доступ некваліфікованому співробітнику не є хорошою ідеєю
- Інтеграція з зовнішніми системами класу SIEM – дозволяє значно розширити рівень безпеки та спостережливості мережі, так як SIEM має змогу накопичувати та корелювати дані з багатьох джерел і системи виявлення вторгнень є одним з найцінніших з джерел таких даних.
- Кореляція подій безпеки – дозволяє побачити взаємозв’язок двох або більше подій у мережі яка аналізується СВВ. Таким чином це дає краще уявлення офіцера інформаційної безпеки на те, що відбувається у підконтрольній йому системі.
- Аналіз трафіку без безпосереднього впливу на нього (можливість роботи з копією трафіку через SPAN/TAP порт) – дозволяє проводити аналіз в

режимі реального часу без впливу на сам трафік який циркулює в мережі. Може бути реалізований з допомогою SPAN/TAP технологію, або ж mirror port, у даному випадку увесь трафік який проходить через пристрій (наприклад маршрутизатор) перенаправляється у систему виявлення вторгнень де вже і відбувається аналіз трафіку та реєстрація подій

- Формування звітів – один з важливих критеріїв, так як часто офіцеру інформаційної безпеки потрібно формувати звіти для керівництва, або для надання групі аудиту. Дана можливість є однією з найважливіших серед функціональних критеріїв.

Дані критерії дозволять оцінити наявність базового функціоналу у інтерфейсі систем виявлення вторгнень та зробити вибір щодо того, чи підходять дані системи для виконання поставлених задач у сфері забезпечення інформаційної безпеки підприємства

### 2.2.3 Тести на відповідність

Дані тести повинні допомогти офіцерам інформаційної безпеки підприємства оцінити базові можливості системи виявлення вторгнень. Кейсів тестування насправді є багато, але у даній роботі доцільно буде проаналізувати лише основні із них. Дані тести спрямовані на тестування основного функціоналу систем виявлення вторгнень, а саме:

- Виявлення сканування портів
- Виявлення атаки проти веб-додатку
- Виявлення атаки прости хоста
- Виявлення нестандартних пакетів

Для того, щоб успішно протестувати усі ці кейси, було використане таке програмне забезпечення як:

- Nmap
- Burp suite
- WebGoat

Отже, для того щоб протестувати основні можливості системи виявлення вторгнень потрібно виконати 4 тести:

- Тест на реєстрацію події сканування портів – Потрібно виконати сканування цільової машини використовуючи утиліту nmap. Сканування потрібно провести в режимах TCP SYN-ACK, TCP SYN сканування, щоб перевірити роботу системи з TCP трафіком, а також UDP сканування, для перевірки того, як система працює з UDP трафіком
- Тест на реєстрацію події проти веб-додатку – виконується з допомогою додатку Burp Suite на атакуючій машині та завідомо вразливого програмного забезпечення WebGoat на цільовій машині. Для цього тесту потрібно провести декілька видів атак, а саме – SQL Injection, Burp Suite crawling, Brute-Force. Даний тест показує те, як система виявлення вторгнень працює на прикладному рівні, та її ефективність
- Тест на виявлення атаки проти хоста – даний тип тесту проводиться проти цільового хоста використовуючи програмне забезпечення nmap. Nmap проводить сканування хоста у режимі low rate scan, таким чином система виявлення вторгнень перевіряється на можливість виявлення таких атак
- Тест на виявлення нестандартних пакетів проводиться для того, щоб перевірити чи виявить СВВ неправильні пакети TCP чи UDP, а також пакети з невідомого до цього IP адреса.

Ці тести повинні допомогти офіцерам ІБ провести тестування обраних систем виявлення вторгнень на відповідність того, які задачі вони повинні будуть вирішувати в подальшому, а також в цілому оцінити зручність роботи з системою.

## 2.3 Розробка плану по вибору систем виявлення вторгнень

Для ефективного вибору системи виявлення вторгнень потрібно задіяти спеціалістів як з менеджменту так і з технічного відділу служби інформаційної безпеки. За відсутністю окремої служби, чи особи яка займається конкретно питаннями інформаційної безпеки на підприємстві, потрібно залучити технічного працівника, який відповідає за існуючу інфраструктуру. Це зумовлено тим, що для вибору цільової системи потрібно розглянути як і економічні та організаційні моменти, так і технічну частину усього процесу.

Першим кроком процесу вибору та впровадженню системи виявлення вторгнень буде збір даних про інфраструктуру та топологію існуючої мережі, так як від даного аспекту залежить вибір цільової системи. Так, наприклад, якщо на підприємстві, більшість даних проходять у одному місці (у так званому ядрі мережі), то доцільно буде обрати до порівняння, системи де кінцева плата буде залежати від кількості впроваджених пристроїв, тому що у цьому варіанті достатньо лише одного пристрою на який буде відправлятися дублікат трафіку.

Окрім цього, потрібно оцінити поточний стан інформаційної безпеки на підприємстві. Даний процес являється другим кроком в процесі вибору СВВ. Так, якщо на підприємстві уже є впроваджені деякі засоби захисту інформації, доцільним буде розглянути можливість вибору системи того ж розробника, якщо він пропонує інтеграцію продуктів між собою, яка може підвищити загальний рівень інформаційної безпеки на підприємстві. Окрім цього, багато розробників у такому випадку пропонують більш економічно вигідні рішення та варіанти.

Третім кроком, має стати заповнення опитувальника про поточний стан інфраструктури та мережі, на даному етапі акумулюються усі дані, які були зібрані на попередніх кроках, для того, щоб команда, яка займається вибором та впровадженням системи виявлення вторгнень отримали, свого роду, короткий опис поточної ситуації на підприємстві. Проста наявність такого опитувальника з базовими питаннями, робить процес вибору в рази простішим

Після того, як було проаналізовано поточний стан інформаційної безпеки підприємства та зібрані дані про поточний стан мережі та інфраструктури, потрібно провести обґрунтування доцільності впровадження саме системи виявлення вторгнень, а не іншого методу забезпечення інформаційної безпеки. На даному кроці, повинні брати участь як технічні фахівці, так і керівництво підприємства. Дуже часто, для забезпечення достатнього рівня інформаційної безпеки на підприємстві потрібно зовсім інші інструменти, таким чином, підприємство може добитися максимально ефективного вирішення нагальних проблем в області інформаційної безпеки.

Одним з найважливіших кроків, по вибору системи виявлення вторгнень є визначення критеріїв для такого вибору. Чудовою базою являються критерії, які були розроблені у розділі номер 2.2 даної роботи. Критерії описані у цьому розділі дають базове розуміння того, якими можливостями та характеристиками повинна володіти цільова система виявлення вторгнень. Дані критерії не являються закінченим списком, та можуть бути відкоректовані в залежності від конкретних вимог підприємстві. Для зручності, критерії потрібно оформити у вигляді порівняльної таблиці.

Наступним кроком буде аналіз ринку систем виявлення вторгнень, та вибір серед них тих, які на перший погляд відповідають обраним критеріям. На даному кроці, буде доцільно скористатися послугами системних інтеграторів, які можуть запропонувати ті чи інші варіанти в залежності від ваших вимог. Окрім цього, можна орієнтуватися на видання які регулярно публікують матеріали та порівняння тих, чи інших інструментів захисту інформації (наприклад Gartner)

Після того, як команда вибрала декілька систем виявлення вторгнень потрібно провести тестування та проаналізувати можливості кожної системи. Якщо ми говоримо про системи з відкритим програмним кодом, то це зробити відносно просто, так як технічні фахівці можуть власноручно розгорнути та протестувати системи які їх цікавлять. З комерційними рішенням складніше так як, рідко коли розробники представляють свої рішення з термінами для тестування, а коли мова

йде про апаратно-програмні комплекси, самостійно виконати це неможливо. У даному випадку, можуть допомогти компанії системні інтегратори, або ж офіційні представництва розробника в країні. Такі компанії можуть надати тимчасові ліцензії або навіть апаратно-програмні комплекси для проведення «Proof-of-concept». Дану стадію вибору зазвичай проводять технічні фахівці і з боку менеджменту потрібна допомога лише у тому випадку, якщо для тестування потрібно звертатися до компаній системних інтеграторів або офіційних представництв розробників.

Завершальним кроком усього процесу являється порівняльний аналіз даних базуючись на заповненій таблиці відповідності критеріям обраних систем. На даному кроці вибір повинно приймати саме керівництво базуючись на виконаній роботі технічних фахівців. Окрім цього, варто знову звернутися до опитувальника який був складений на початку усього процесу вибору системи виявлення вторгнень, так як з заповненою таблицею стає зрозуміло, чи відповідає та чи інша система на питання та проблеми які вказані у опитувальнику.

Таким чином усі кроки для по вибору системи виявлення вторгнень можна представити у вигляді списку:

1. Збір даних про інфраструктуру та топологію мережі
2. Аналіз поточної ситуація з ІБ
3. Заповнення опитувальника про поточний стан інфраструктури
4. Обґрунтування доцільності впровадження системи виявлення вторгнень
5. Вибір систем виявлення вторгнень для порівняння
6. Заповнення таблиць відповідності систем визначеним критеріям
7. Порівняльний аналіз даних базуючись на відповіді опитувальника

## Висновок за розділом 2

У даному розділі була проаналізована проблематика забезпечення інформаційної безпеки на підприємствах малого та середнього бізнесу та вибору системи виявлення вторгнень в цілому. Як можна побачити, дані проблеми не

обмежуються лише невеликими системами, а і актуальні для корпорацій, які не надають цьому аспекту достатньо увагу.

Окрім цього були сформовані критерії для порівняння при виборі системи виявлення вторгнень. Дані критерії згруповані по таким групам як:

- Критерії менеджменту
- Критерії функціональності
- Тести відповідності

Також у даному розділі був сформований список кроків, які повинна виконати компанія для вибору ефективної системи виявлення вторгнень

# РОЗДІЛ 3
# РОЗРОБКА РЕКОМЕНДАЦІЙ ПО ВИБОРУ СИСТЕМ ВИЯВЛЕННЯ ВТОРГНЕНЬ ДЛЯ МАЛОГО ТА СЕРЕДНЬОГО БІЗНЕСУ

## 3.1 Складання опитувальника для вибору системи виявлення вторгнення

При виборі системи для малого та середнього бізнесу, власник або відповідальна особа повинна перш за все відповісти на декілька питання, що стосуються інформаційної безпеки підприємства.

Для того, щоб вірно оцінити ситуацію, скоріш за все менеджменту потрібно буде підключити до обговорення технічого фахівця, який знає нюанси нинішньої роботи інфраструктури та мережі. До таких питань відносяться:

- Топологія мережі – яким чином зараз організована робота мережі? Чи можна явно виділити ядро мережі, через яке проходить основна частина трафіку? На скільки «зон» поділена мережа?
- Які засоби захисту інформації уже впроваджені на підприємстві? Чи є впроваджений SIEM, куди система виявлення вторгнень зможе надсилати дані?
- Бюджет який керівництво готове виділити на впровадження системи виявлення вторгнень? Безпосредньо на вровадження, та наступну підтримку у місяць.
- Системи з якими уже знайомі офіцери інформаційної безпеки? Плюсом даних систем буде те, що співробітникам потрібно буде значно менше часу на адаптацію та приведення системи до «бойового стану»
- Чи потрібна буде технічна підтримка для системи виявлення вторгнень?
- Кількість мережевого трафіку який циркулює у мережі?

- Чи розглядається можливість впровадження не лише системи виявлення вторгнень, а і додаткових засобів захисту, які не тільки виявляють, а і запобіганню успішного виконання цих атак?

Дані питання чудово корелюються з критеріями які були розроблені у попередньому, так як давши відповідь на ці питання, можна буде уже сформувати думку про те, яка саме система підходить для впровадження на конкретному підприємстві.

Дані питання можна перенести у таблицю, для зручності роботи та наглядності. Таким чином буде сформований опитувальник, який буде слугувати як подальший орієнтир при виборі системи виявлення вторгнень.

Окрім цього, варто зазначити, що при розробці плану впровадження системи виявлення вторгнень, варто не обмежуватися лише цим конкретним переліком питань, а і за необхідності розширити питаннями які важливі для конкретно підприємства, так як питання описані у цьому розділі являються базовими, та покликані створити перше враження про потрібну систему

Даний опитувальник буде складений у вигляді таблиці з двома колонками – Запитання та Відповідь. Заповнений опитувальник потрібно буде зафіксувати при описані усієї процедури вибору системи виявлення вторгнень так як ним, у майбутньому можливо буде обґрунтувати свій вибір. Приклад опитувальник зображений у таблиці 1.

Дані питання не є закінченим переліком, та можуть бути розширений відповідно до вимог конкретного підприємства. Для цього можуть бути залучені як технічні працівники підприємства, так і зовнішні експерти.

Таблиця 3.1

Опитувальник по вибору системи виявлення вторгнень

| Питання | Відповідь |
|---|---|
| Топологія мережі | |
| Які засоби захисту інформації уже впроваджені на підприємстві | |
| Чи є впроваджений SIEM, куди система виявлення вторгнень зможе надсилати дані | |
| Бюджет який керівництво готове виділити на впровадження системи виявлення вторгнень? Безпосередньо на врованження, та наступну підтримку у місяць. | |
| Бюджет який керівництво готове виділити на та наступну підтримку у місяць. | |
| Системи з якими уже знайомі офіцери інформаційної безпеки | |
| Чи потрібна буде технічна підтримка для системи виявлення вторгнень | |
| Кількість мережевого трафіку який циркулює у мережі | |
| Чи розглядається можливість впровадження не лише системи виявлення вторгнень, а і додаткових засобів захисту | |

Також під час заповнення опитувальника важливо спиратися на результати попередніх аудитів, якщо такі проводилися

## 3.2 Вибір систем виявлення вторгнень для порівняльного аналізу

Для впровадження ефективної системи виявлення вторгнень потрібно провести аналіз ринку таких систем та обрати серед них ті, що на перший погляд найбільше підходять для впровадження на конкретному підприємства.

Під час цього процесу варто користуватися заповненим опитувальником, так як більшість систем мають гарно описано документацію, а у випадку з комерційними рішеннями маркетингового матеріалу, дослідивши які можна буде зробити перші висновки того, чи може вирішити та чи інша система виявлення вторгнень проблеми пов’язані з інформаційною безпекою на підприємстві.

Навіть з достатнім бюджетом не варто орієнтуватися лише на комерційні рішення, так як можливо, для вирішення завдань на конкретному підприємстві буде достатньо і того, що можуть запропонувати системи виявлення вторгнень з відкритим програмним кодом. З іншої ж сторони, для підприємств з обмеженим бюджетом використання системи з відкритим програмним кодом не являється єдиним правильним рішенням. У випадку з Open-Source програмним забезпеченням варто пам’ятати, що впроваджується не продукт, а лише проект і якоїсь адекватної технічної підтримки очікувати не варто. У випадку малого та середьного бізнесу, деколи навіть вигідніше обрати комерційне рішення та віддати його обслуговування та впровадження на аутсорс.

Таким чином можна побачити, що при виборі системи виявлення вторгнень варто детально звернути увагу, чи є в штаті компанії людина, яка зможе впровадити та підтримувати систему на достатньому рівні, та при можливості виділити частину бюджету саме на те щоб навчити персонал, працювати з обраною системою.

### 3.2.1 Аналіз ринку систем виявлення вторгнень з відкритим програмним кодом

*Ринок систем виявлення вторгнень являється не особливо великим, більшість продуктів давно відомі так як їх розробка ведеться з початку двохтисячних. Серед найвідоміших таких систем можна виділити Suricata, Snort, Zeek. Дані системи розробляються та підтримуються великим суспільством розробників та мають достатньо велику базу документації.*

Snort-Мережева IDS з аналізом за шаблонами (Правилами) і виявленням аномалій (деякі модулі препроцесора). Система з відкритими текстами (GNU, компанія Sourcefire, 2.8.1 на 10 квітня 2008). Доступ до бази шаблонів обмежений (бажаючі можуть писати свої шаблони або шукати їх в інтернет). Користувачі діляться на:

- Підписник - платять гроші і мають повний доступ
- зареєстровані (for free) користувачі-мають доступ з 30-денною затримкою (Sourcefire VDB signatures)
- решта-мають доступ до набору правил на момент випуску версії і "аматорським" наборам (community signatures)

Може працювати в режимах прослуховування мережі, журналювання мережевої активності і IDS. Шаблони визначаються набором правил обробки пакетів і програм препроцесування (дефрагментація, збірка TCP потоку). Нові шаблони (правила) підтримуються тільки в новій версії. Правила діляться на типи і нумеруються (Sid - Sensor ID). Можливе написання своїх модулів, що підключаються. Графічний інтерфейс-Demarc / Puresecure (Unix) і IDScenter (MS Windows).

Для роботи потрібен великий і швидкий диск (RAID) - 100GB; багато оперативної пам'яті (170MB на інтерфейс для x86; 250mb - для x86-64); швидка мережева карта (zero copy transfer, підрахунок контрольних сум, опитування замість

обробки переривань, NAPI), бажано окрема мережева карта. Підтримувані ОС (потрібно libcap): Linux, FreeBSD, NetBSD, OpenBSD, MS Windows, Sparc Solaris, x86 Mac OS X, PowerPC Mac OS X, PA-RISC HP-UX. Входить до складу деяких Live CD: Auditor, Trinux, Bootable Snort Project, NST (Network Security Toolkit, сконфігурований Snort, MySQL і веб-інтерфейс). Snort-однопотокова система, для використання декількох процесорів можна запускати кілька з відповідними фільтрами захоплення. Бажано прив'язати процес і обробник переривань до одного і того ж процесора.

Основні архітектурні компоненти (відображають шлях пакета, є вбудованими модулями, крім захоплення):

- захоплення пакетів (є можливість читання з файлу у форматі tcpdump)
- Препроцесор (модулі: збірка TCP потоку (stream4, frag3); відстеження обміну( flow); сканування портів (sfPortscan), дефрагментація, RPC, HTTP, ...)
- детектор (зіставлення з набором правил: заголовок правила задає дію в разі збігу (записати в журнал або видати попередження), тип пакета, IP джерела і приймача, номери портів; опція правила визначає шаблон для порівняння)
- висновок (запис у файл у форматі tcpdump, текстовий журнал, СУБД (MySQL, Postgres) і видача попередження (SMB, SNMP), syslog
- додаткові утиліти для розбору журналів (SnortSnarf;Snortplot. php; Swatch-обробка журналів і посилка e-mail; Razorback-графічний інтерфейс Gnome; SneakyMan-графічний конфігуратор)

Suricata-це високопродуктивний механізм моніторингу мережевих ідентифікаторів, IP-адрес та мережевої безпеки. Він є відкритим вихідним кодом і належить некомерційному фонду, керованому спільнотою, Фонду відкритої інформаційної безпеки (OISF). Suricata розроблена OISF

Suricata являється ідентифікатор на основі підпису, і після його правильного налаштування Suricata може виконувати перевірку трафіку в режимі реального часу, щоб викликати сигнали тривоги при виявленні підозрілої активності у вашому середовищі. Suricata також пропонує дуже великий список функцій.

Suricata здатна запускати кілька потоків. Якщо у вас є обладнання з декількома процесорами / ядрами, інструмент можна налаштувати для розподілу робочого навантаження на кілька процесів одночасно. Ви можете почати роботу з одного потоку і обробляти Пакети по одному за раз. Тим не менш, з мого досвіду, багатопоточність-це набагато краща конфігурація і спосіб поліпшити продуктивність Suricata.

Suricata має чотири модулі потоків:

- Отримання пакетів: відповідає за читання пакетів з мережі.
- Декодування і потоковий рівень програми: декодує пакети і перевіряє додаток.
- Виявлення: порівнює сигнатури і може виконуватися в декількох потоках.
- Виходи: в цьому модулі обробляються всі сигнали тривоги.

Suricata може працювати в Linux, FreeBSD, OpenBSD, Mac OS і Windows. Тим не менш, потрібно перевірити обсяг трафіку, який ви будете обробляти для кожного інтерфейсу. Для його запуску немає конкретної конфігурації обладнання.

Suricata може бути встановлена на сервер Ubuntu з 2 ядрами і 8 ГБ оперативної пам'яті, чого буде достатньо, якщо ви плануєте протестувати інструмент в лабораторному середовищі і подивитися, як він працює. З іншого боку, якщо ви плануєте протестувати кілька інтерфейсів і відправити на них значний обсяг трафіку, вам знадобиться більше процесорів і більше пам'яті, щоб обробляти пакети і використовувати багатопоточність. Пам'ятайте, що якщо у вас недостатньо обладнання для обробки вхідного трафіку, Suricata зіткнеться з проблемами продуктивності.

Три пропоновані варіанти установки :

- Сервер Ubuntu: для цього дистрибутива Linux у сховищі Open Information Security Foundation (OISF) є стабільні двійкові пакети. Вам потрібно лише перевірити, які залежності від Suricata, а потім встановити його. Я б рекомендував цей варіант для вашої першої установки.
- pfSense -це брандмауер/маршрутизатор з відкритим кодом, який пропонує додатковий пакет Suricata. Ця опція може стати вашим наступним кроком, якщо ви хочете вивчити можливість додавання системи виявлення мережевих вторгнень в брандмауер.
- Виділений сервер Linux з 16 ядрами, 32 ГБ оперативної пам'яті і не менше 2 мережевих карт. Ця запропонована конфігурація забезпечить хорошу продуктивність, і ви зможете протестувати режими виконання Suricata без проблем.

Так як Suricata має можливість надавати результати аналізу у JSON форматі, даний продук легко інтегрується як і з SIEM, так і просто аналізаторами логів, наприклад Logstash (рисунок 3.1)


Рисунок 3.1 -– Інтеграція Suricata з аналізатором лог файлів Logstash та засобом візуалізації Kibana

Zeek-це пасивний аналізатор мережевого трафіку з відкритим вихідним кодом. Багато операторів використовують Zeek в якості монітора мережевої безпеки (NSM) для підтримки розслідувань підозрілих або шкідливих дій. Zeek також підтримує широкий спектр завдань аналізу трафіку за межами області безпеки, включаючи вимірювання продуктивності та усунення неполадок.

Перша перевага, яку новий користувач отримує від Zeek, - це великий набір журналів, що описують мережеву активність. Ці журнали включають в себе не тільки повний запис кожного з'єднання, побаченого на дроті, але і розшифровки на рівні додатків. До них відносяться всі http-сеанси з запитаними URI, заголовками ключів, типами MIME і відповідями сервера; DNS-запити з відповідями; SSL-сертифікати; вміст ключів SMTP-сеансів і багато іншого. За замовчуванням Zeek записує всю цю інформацію в добре структуровані файли журналів з розділенням вкладок або JSON, які підходять для подальшої обробки за допомогою зовнішнього програмного забезпечення. Користувачі також можуть вибрати, щоб зовнішні бази даних або продукти SIEM споживали, зберігали, обробляли і представляли дані для запитів.

На додаток до журналів, Zeek поставляється з вбудованою функціональністю для цілого ряду завдань аналізу і виявлення, включаючи вилучення файлів з сеансів HTTP, виявлення шкідливих програм шляхом взаємодії з зовнішніми реєстрами, повідомлення про вразливі версії програмного забезпечення, помічених в мережі, ідентифікацію популярних веб-додатків, виявлення грубого примусу SSH, перевірку ланцюжків сертифікатів SSL і багато іншого.

На додаток до доставки такої потужної функціональності "з коробки", Zeek-це повністю настроювана і розширювана платформа для аналізу трафіку. Zeek надає користувачам специфічну для домену, повну за Тьюрингом мову сценаріїв для вираження довільних задач аналізу. Подумайте про мову Zeek як про " специфічну для домену Python "(або Perl): як і Python, система поставляється з великим набором готових функцій ("стандартна бібліотека"), але користувачі також можуть використовувати Zeek новими способами, написавши користувальницький код.

Дійсно, всі аналізи за замовчуванням Zeek, включаючи ведення журналу, виконуються за допомогою скриптів; ніякий конкретний аналіз жорстко не закодований в ядрі системи.

Zeek працює на власному обладнанні і, отже, забезпечує недорогу альтернативу дорогим комерційним рішенням. Багато в чому Zeek перевершує можливості інших інструментів моніторингу мережі, які зазвичай обмежуються невеликим набором жорстко запрограмованих завдань аналізу. Zeek не є класичною системою виявлення вторгнень на основі сигнатур (IDS); хоча вона також підтримує таку стандартну функціональність, мова сценаріїв Zeek полегшує набагато ширший спектр найрізноманітніших підходів до виявлення шкідливої активності. До них відносяться виявлення семантичного неправильного використання, виявлення аномалій та поведінковий аналіз.

Велика різноманітність сайтів використовують Zeek для захисту своєї інфраструктури, включаючи багато університетів, дослідницькі лабораторії, суперкомп'ютерні центри, спільноти відкритих наук, великі корпорації та урядові установи. Zeek спеціально націлений на високошвидкісний моніторинг мереж з великим обсягом, і все більше число сайтів в даний час використовують систему для моніторингу своїх мереж 10GE, а деякі вже переходять на посилання 100ge.

Zeek підтримує високопродуктивні налаштування, підтримуючи масштабоване балансування навантаження. Великі сайти зазвичай запускають "кластери Zeek", в яких високошвидкісний балансувальник навантаження на передньому кінці розподіляє трафік між відповідною кількістю внутрішніх комп'ютерів, причому всі вони запускають виділені екземпляри Zeek на своїх окремих зрізах трафіку. Система централізованого диспетчера координує процес, синхронізуючи стан по всіх серверних частинах і надаючи операторам Центральний інтерфейс управління для налаштування і доступу до агрегованих журналів. Інтегрована структура управління Zeek, ZeekControl, підтримує такі налаштування кластера"з коробки".

Кластерні функції Zeek підтримують односистемні та мультисистемні Налаштування. Це частина переваг масштабованості Zeek. Наприклад, адміністратори можуть масштабувати Zeek в одній системі якомога довше, а потім прозоро додавати нові системи, коли це необхідно.

Коротше кажучи, Zeek оптимізований для інтерпретації мережевого трафіку та створення журналів на основі цього трафіку. Він не оптимізований для зіставлення байтів, і користувачам, які шукають підходи до виявлення сигнатур, було б краще скористатися системами виявлення вторгнень, такими як Suricata. Zeek також не є аналізатором протоколів у сенсі Wireshark, який прагне відобразити кожен елемент мережевого трафіку на рівні кадру, або системою зберігання трафіку у формі захоплення пакетів (PCAP). Швидше за все, Zeek сидить у "щасливому середовищі", що представляє компактні, але високоякісні мережеві журнали, забезпечуючи краще розуміння мережевого трафіку та використання.

Окрім цього, важливо зазначати, що Zeek складається з багатьох компонентів, які ти чи іншим способом полегшують роботу як з самим програмним забезпеченням так і з результатами його роботи. Дані компоненти можна знайти на рисунку 3.2

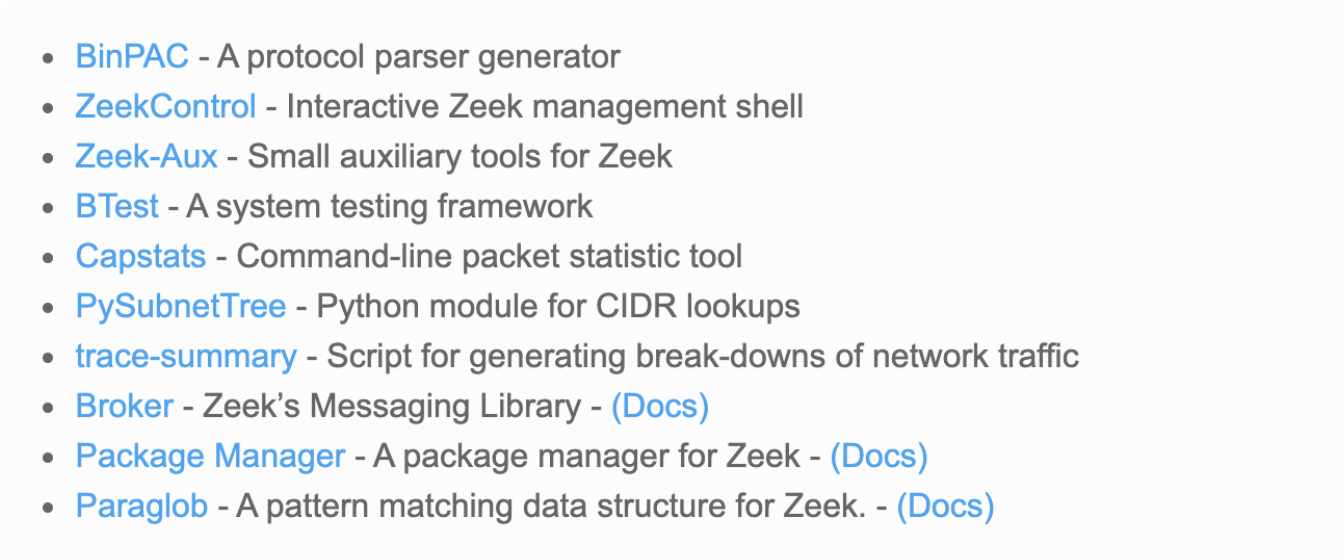


Рисунок 3.2 – Компоненти Zeek

Таким чином, для подальшого порівняння було обрани три системи виявлення вторгнень з відкритим програмним кодом:

1. Zeek
2. Snort
3. Suricata

### 3.2.2 Аналіз ринку комерційних систем виявлення вторгнень

Серед комерційних систем виявлення вторгнень також існує досить великий вибір та висока конкуренція між ними. Саме по цій причині окремо системи виявлення вторгнень рідко зустрічаються останім часом. У погоні за клієнтами розробники в більшості своїй почали додавати до них додатковий функціонал для того, щоб вирішувати більшу кількість проблем інформаційної безпеки. Окрім цього функціонал виявлення вторгнень також додають до інших інструментів забезпечення інформаційної безпеки.

Для вибору систем для порівняння у даній роботі були використані дані від видавництва Gartner. Дане видавництво кожного року порівнює ті чи інші комерційні інструменти забезпечення інформаційної безпеки одного типу між собою. Нажаль Gartner не випускає Magic Quadrant лише для систем виявлення вторгнень через те, що дані системи на даний момент майже не виробляються у «чистому» вигляді комерційними компаніями. Тому для порівняняя була обрана стаття за 2017 рік для фаєрволів наступного покоління (Next-generation firewall) так як до їх функціоналу входять системи виявлення вторгнень, але це не являється їх головним завданням.

Як ми бачимо, одним з найбільш економічно вигідних варіантів являється Fortinet. Також явними фаворитами є продукти компанії Check Point та Cisco. Серед усіх пристроїв які є у даних розробників, найцікавішими для малого та середнього

бізнесу є Fortinet FortiGate 600D, Check Point 1550 та Cisco Firepower 2130 NGFW Appliance.

CheckPoint Infinity-це єдина повністю консолідована Архітектура кібербезпеки, яка захищає бізнес та IT-інфраструктуру від кібератак Gen V у всіх мережах, кінцевих точках, хмарах і мобільних пристроях. Архітектура призначена для вирішення складнощів, пов'язаних зі зростаючим зв'язком і неефективною безпекою. Він забезпечує повне запобігання загрозам, яке усуває прогалини в безпеці, забезпечує автоматичний, негайний обмін інформацією про загрози у всіх середовищах безпеки і єдине управління безпекою для максимально ефективної роботи системи безпеки. Контрольна точка Нескінченність доставляє безпрецедентний захист від поточних і потенційних атак-сьогодні і в майбутньому.

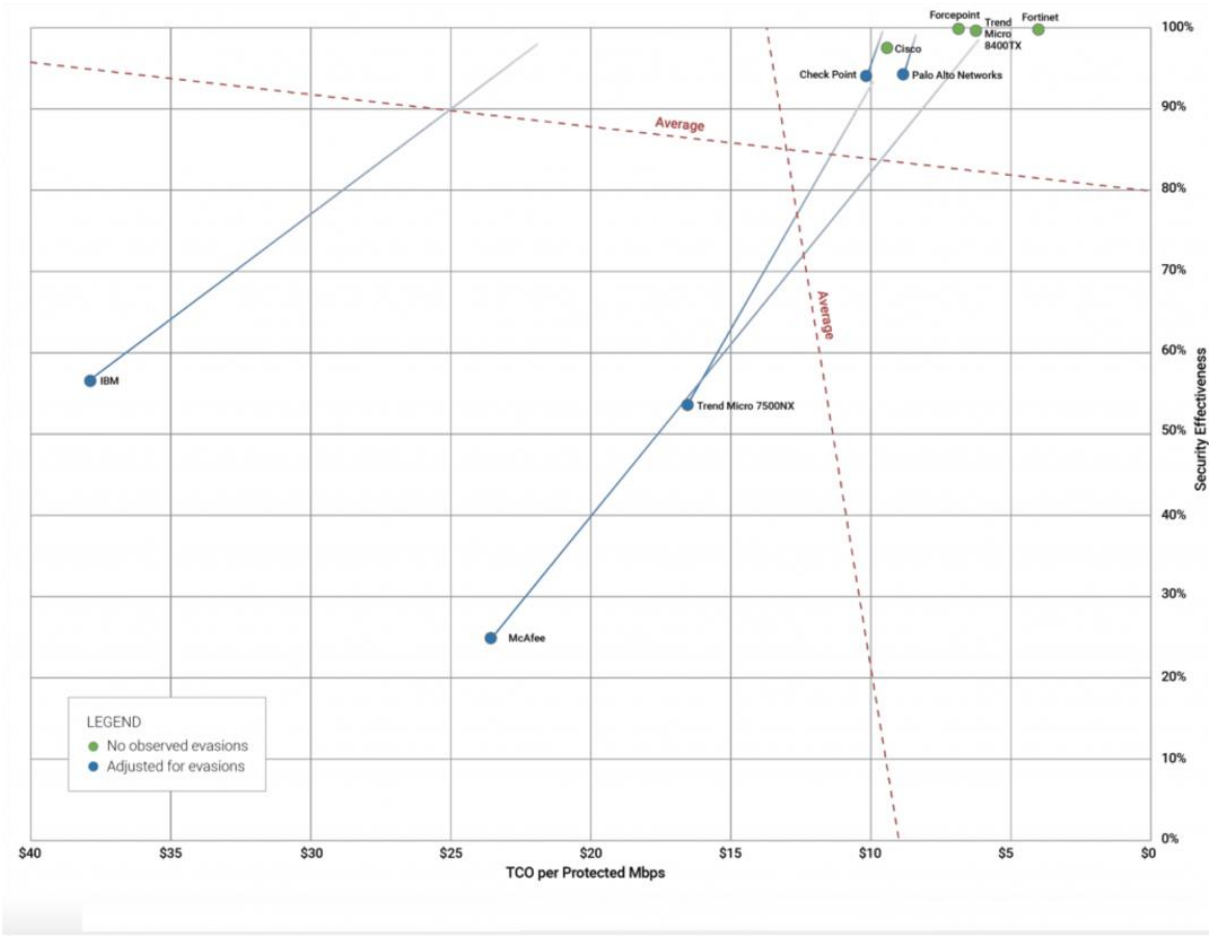


Рисунок 3.3 – Gartner magic Quadrant 2017

Швидке зростання шкідливих програм, зростаюча витонченість зловмисників і поява нових невідомих загроз нульового дня вимагають іншого підходу до забезпечення безпеки корпоративних мереж і даних. Check Point забезпечує повністю інтегроване, всебічне запобігання загрозам для боротьби з цими виникаючими загрозами при одночасному зниженні складності і підвищенні операційної ефективності. Рішення для запобігання загрозам Check Point включає в себе потужні функції безпеки, такі як firewall, IPS, Anti-Bot, Antivirus, Application Control і фільтрація URL - адрес для боротьби з відомими кібератаками і погрозами - тепер воно доповнено відзначеною нагородами емуляцією загроз SandBlast і витяганням загроз для повного захисту від найскладніших загроз і вразливостей нульового дня.

В рамках рішення для захисту Check Point SandBlast Zero-Day Хмарний механізм емуляції загроз виявляє шкідливе ПЗ на етапі експлойта, навіть до того, як хакери зможуть застосувати методи ухилення, намагаючись обійти пісочницю. Файли швидко поміщаються в карантин і перевіряються, запускаються у віртуальній пісочниці, щоб виявити шкідливу поведінку до того, як воно потрапить у вашу мережу. Це інноваційне рішення поєднує в собі хмарну перевірку на рівні процесора і пісочницю на рівні ОС для запобігання зараження від найбільш небезпечних експлойтів, а також атак нульового дня і цільових атак. Крім того, Sandblast threat Extraction видаляє експлуатований контент, включаючи активний контент і вбудовані об'єкти, відновлює файли для усунення потенційних загроз і оперативно доставляє очищений контент користувачам для підтримки бізнес-потоку.

| | | | |
|---|---|---|---|
|  Scalable Platforms | Deployment | Data center, Telco, Carrier | Maestro |
| | Form Factor | 6RU and up | 64000 |
| | Interfaces | 1, 10, 40, 100 GbE | 44000 |
| | Throughput | 90 to 1,500 Gbps Threat Prevention | |
| | Special Features | DC power, Active/Active Clustering | |
|  Data Center | Deployment | Large enterprise, Data center | 28000 |
| | Form Factor | 2RU | 26000 |
| | Interfaces | 1, 10, 25, 40, 100 GbE | 16200 |
| | FW Throughput | 78.3 to 145 Gbps (Enterprise Test) | |
| | Special Features | 25/40/100 GbE, DC power, LOM | |
|  Enterprise | Deployment | Enterprise | 7000, 6900 |
| | Form Factor | 1RU | 6700, 6600 |
| | Interfaces | 1, 10, 40 GbE | 6400, 6200 |
| | FW Throughput | 9 to 48 Gbps (Enterprise Test) | |
| | Special Features | Flexible IO options, LOM | |
|  Branch, Small Office | Deployment | Branch or Small Office | 3800, 3600 |
| | Form Factor | Desktop | 1800, 1600 |
| | Interfaces | 1 GbE, Wi-Fi, DSL, 3G/4G/LTE | 1500 |
| | FW Throughput | 1 to 7.5 Gbps (Enterprise Test) | |
| | Special Features | Web management | |
|  Rugged | Deployment | Harsh environments | 1570R |
| | Form Factor | Desktop, DIN and wall mount | |
| | Interfaces | 1 GbE, 3G/4G/TE support | |
| | FW Throughput | 4 Gbps | |
| | Special Features | AC/DC power | |

Рисунок 3.4 – Специфікація усіх лінійок CheckPoint Next-Generation Firewall

Пристрій FortiGate 600D забезпечує чудову продуктивність завдяки поєднанню спеціально побудованих процесорів FortiASIC , високої щільності портів з 10 портами GE і об'єднаним функціям безпеки операційної системи FortiOS. Він забезпечує в 5 разів кращу продуктивність брандмауера наступного покоління в порівнянні з альтернативними продуктами і забезпечує кращу ціну / продуктивність в галузі.

Ця проривна продуктивність запобігання загрозам дозволяє організаціям запускати рекомендації лабораторії NSS щодо запобігання вторгнень і контролю додатків, а також сертифіковані можливості захисту від шкідливих програм VB100 для більш глибокої перевірки. Розширені представлення консолі і звіти разом з гнучким механізмом політики забезпечують видимість і контроль для розширення можливостей співробітників і забезпечення безпеки Вашого підприємства.

Нарешті, ці функції платформи мережевої безпеки FortiOS FortiGate регулярно перевіряються незалежними тестами в реальному світі і незмінно отримують вищі оцінки ефективності безпеки.

Основні переваги:

- у 5 разів швидший апаратно прискорений брандмауер наступного покоління пропонує найкраще в своєму класі співвідношення ціни і продуктивності
- Інтегрована висока щільність портів забезпечує максимальну гнучкість і масштабованість
- NSS Labs, рекомендовані ngfw і ngips з консолідованою безпекою, забезпечують першокласний захист
- Контроль додатків, а також застосування політики на основі ідентифікації та пристроїв забезпечує більш детальний захист
- Інтуїтивно зрозумілий інтерфейс управління забезпечує широку і глибоку видимість, яка масштабується від одного до тисяч

Cisco Firepower серії 2100-це сімейство з чотирьох платформ безпеки, орієнтованих на загрози, які забезпечують стійкість бізнесу і чудовий захист від загроз. Вони забезпечують виняткову стійку продуктивність при включенні розширених функцій загроз. Ці платформи унікально включають інноваційну двоядерну архітектуру процесора, яка оптимізує функції брандмауера, криптографії та перевірки загроз. Діапазон пропускної здатності брандмауера серії адресує варіанти використання від краю Інтернету до центру обробки даних. Стандарти побудови мережевого обладнання( NEBS) - відповідність підтримується платформою Cisco Firepower 2130. Платформи серії 2100 працюють або з програмним забезпеченням Cisco Secure Firewall ASA, або з програмним забезпеченням захисту від загроз (FMC). Вони можуть бути розгорнуті як в режимі брандмауера, так і в режимі виділеної IP-адреси.

Отже, для порівняння на відповідність критеріям серед комерційних систем виявлення вторгнень було обрано 3 апаратно-програмні комплекси:

- Fortinet FortiGate 600D;
- Check Point 1550;
- Cisco Firepower 2130 NGFW Appliance.

## 3.3 Заповнення таблиці відповідності конкретних систем виявлення вторгнень до визначених критеріїв

Таблиця відповідності конкретних систем виявлення вторгнень до визначених критеріїв потрібна для наглядного порівняння систем виявлення вторгнень які були взяті до розгляду. У даній таблиці будуть використані системи які були описані у другому розділі даної дипломної роботи.

Також для наглядності результатів попередньо потрібно заповнити опитувальник, який був представлений у попередньому підрозділі.

В рамках виконання цієї роботи при заповнені таблиці допускаються певні неточності у даних, так як відсутній відкритий доступ до комерційних пропозицій.

Таблиця відповідності конкретних систем виявлення вторгнень до визначених критеріїв для зручності розбита на три окремих таблиці відповідно до умовного розподілення критеріїв на групи.

Відповідність систем виявлення до критеріїв менеджменту зображені у додатку Б.

Як можна побачити у результаті ми отримали такі дані, що комерційні рішення коштують достатньо дорого, але серед них явно вибивається вперед рішення від компанії Fortinet. Окрім цього слід звернути увагу, що комерційні рішення пропонують не чисту систему виявлення вторгнень, а і мережевий екран та систему запобігання вторгненням.

Окрім цього, CheckPoint  пропонує і SandBlast компонент який виступає в ролі пісочниці, що є ефективною технологією для протидії загрозам нульового дня. У той же час системи виявлення вторгнень з відкритим кодом, являються безплатним, але жодна з них не пропонує хочаб якусь технічну підтримку, що може бути вирішальним фактором для деяких підприємств.

Окрім цього варто зважати на те, що комерційні рішення пропонують цілий комплекс який може вирішити багато існуючий проблем підприємства в плані інформаційної безпеки.

Відповідність систем виявлення до критеріїв функціональності зображені у додатку В.

По результатам заповненням таблиці критеріїв функціональності можна побачити, що результати схожі з таблицею відповідності для менеджменту. В загалом усі вони мають подібний функціонал, а суттєві відмінності спостерігаються між комерційними рішенням та рішенням з відкритим кодом.

Також ми бачимо, що у комерційних варіантів немає можливості саме автоматичної інвентаризації мережі, так як вони орієнтовані саме на роботу з цільовим трафіком, виявлення та блокування атак. Також ми можемо побачити, що лише в Zeek немає можливості кореляції подій.

Тести на відповідність внесли додаткову ясність у порівняння систем виявлення вторгнень. За результатами тестування, можна побачити, що комерційні рішення можуть ефективно виявляти як атаки на рівні мережі, так і атаки на прикладному рівні. У систем з відкритим кодом спостерігаються проблеми з виявленням атак на прикладному рівні. Так лише Suricata змогла впоратися з виявленням SQL ін’єкцією направленою проти веб-додатку. Також варто відмітити, що Zeek не впорався з IP Spoofing атакою, та не зміг її виявити.

## 3.4 Формування рекомендацій щодо впровадження систем виявлення вторгнень для малого та середнього бізнесу

Даних які були отримані у результаті заповнення опитувальника та таблиць відповідності вистачає для того, щоб сформувати рекомендації щодо впровадження систем виявлення вторгнень для малого та середнього бізнесу.

Так як системи виявлення вторгнень тісно пов’язані з IT-інфраструктурою підприємства в цілому, першочергово потрібно розробити чітку стратегію розвитку

Для того, щоб впровадити ефективну систему виявлення вторгнень, потрібно чітке планування усього процесу, починаючи з дослідження уже існуючої мережі та інфраструктури підприємства.

Коли йде мова про малий і середній бізнес, потрібно бути готовим до компромісів, так як рішення, які одночасно задовільнять усі вимоги зазвичай коштують більше ніж можуть собі дозволити компанії

Якщо компанія має бюджет біля 10.000$ та досі впроваджувала лише прості фаєрволи, кращим вибором буде Fortinet FortiGate 600D, так як окрім системи виявлення вторгнень, даний апаратно-програмний комплекс має функціонал як виявлення вторгнень, так і запобігання їх. Також дана система надає можливості для впровадження SSL інспекції та IPSec VPN, що є актуальним на період пандемії. Варто зазначити, що FortiNet пропонує багато інших засобів у сфері інформаційної безпеки, які об’єднуються у одну екосистему в якій можна централізовано спостерігати за станом інформаційної безпеки підприємства.

У випадку, коли ми говоримо про малий бізнес, зазвичай компанії використовують звичайні фаєрволи, та намагаються забезпечити вимоги інформаційної безпеки з мінімальним бюджетом. У цьому випадку ідеальним варіантом будуть системи виявлення вторгнень з відкритим кодом. Серед них виділяється Suricata так як дана система однаково добре впоралась з тестами як на прикладному рівні, так і на мережевому. Окрім цього, Suricata конфігурується з допомогою YAML, що робить її відносно простою у використані. Також цей вибір

дозволить вкласти бюджет у навчання співробітників роботі з даною СВВ.

Окрім цього, компаніям варто зважати на досвід співробітників по роботі з тою чи іншою системою. Таким чином, підприємство може заощадити значну кількість бюджету, який був направлений на навчання, а також швидше привести підприємство до бажаного стану інформаційної безпеки.

Як показує практика, впровадження апаратно-програмного комплексу, являється економічно вигіднішим та зручнішим, ніж впроваджувати кожен засіб захисту інформації окремо, тому все ж краще одним продуктом вирішувати декілька проблем які існують у підприємства в сфері інформаційної безпеки.

## Висновок за розділом 3

Отже, у даному розділі були вибрані системи виявлення вторгнень для порівняння. Для розгляду брались як комерційні рішення, так і рішення з відкритим програмним кодом, що дало змогу надати ширші рекомендації по вибору систем виявлення вторгнень.

Також був складений опитувальник , який необхідно заповнити в залежності від існуючих потреб підприємства, та того як нині функціонує як мережа, так і інфраструктура компанії в цілому.

Окрім цього були використані критерії для порівняння цільових систем виявлення вторгнень, що були визначені у попередньому розділі. Обрані системи були досліджені, та результати були внесені у таблиці відповідності критеріям для систем виявлення вторгень.

Базуючись на результатах, які були отримані в результаті перевірки на відповідність критеріям системи виявлення вторгнень, були надані рекомендації, щодо впровадження таких систем на підприємствах малого та середнього бізнесу.

# ВИСНОВКИ

У зв'язку з активним вдосконаленням інформаційних технологій і поширенням локальних і глобальних мереж, все більшого значення набуває наявність системи виявлення вторгнень. Це життєва необхідність, оскільки система яка виконує постійний аналіз мережевого, та не тільки, трафіку, дозволяє підняти рівень інформаційної безпеки на підприємстві на зовсім інший рівень. Окрім цього, дані системи дають офіцерам інформаційної безпеки та системним адміністратором розуміння того, який трафік та яка інформація циркулює у мережі підприємства.

Системи виявлення вторгнень поділяються за способом реалізації и на програмні і апаратні. В даний час більшість виробників програмних засобів захисту для корпоративних користувачів пропонують інтегровані рішення, куди включені такі компоненти, як антивірус, антиспам, проактивний модуль і міжмережевий екран, в поєднанні з вбудованою системою виявлення вторгнень.

Тому у дипломній роботі розв’язано актуальне наукове завдання щодо розробки рекомендацій по вибору систем виявлення вторгнень для малого та середнього бізнесу.

В ході розв’язання поставленої задачі були отримані наступні наукові та практичні результати:

1. проведено аналіз сучасних систем виявлення вторгнень;
2. Визначено комплекс вимог до сучасних систем виявлення вторгнень;
3. Визначено проблематику вибору систем виявлення вторгнень для малого та середнього бізнесу
4. Розроблено базові критерії по вибору системи виявлення вторгнень для підприємств;
5. Розроблено план вибору системи виявлення вторгнень;

6. Розроблено базовий план впровадження системи виявлення вторгнень на підприємстві
7. Розроблені рекомендації по вибору системи виявлення вторгнень на підприємстві малого та середнього бізнесу.

# СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. kompjuternye-terminologii https://elhow.ru/kompjutery/kompjuternye-terminologii/chto-takoe-ids?utm_source=users&utm_medium=ct&utm_campaign=ct

2. Виктор Сердюк «Вы атакованы — защищайтесь!» [HTML] (http://inform.p-stone.ru /libr/nets/security/data/public7/).

3. Проблема «нулевого дня» [HTML] (http://itc.ua/article.phtml? ID= 26845&IDw =38&pid =57).

4. Intrusion Detection Systems (IDS) Part 2 — Classification; methods; techniques [HTML] (http://www.windowsecurity.com/articles/IDS-Part2-Classification-methods-techniques.html

5. S. Rubin, S. Jha, and B. P. Miller. Automatic generation and analysis of NIDS attacks. In the Annual Computer Security Applications Conference (Tucson, AZ, December 2004). (pdf). This paper won the Student Paper Award and the Best Paper Award in ACSAC 2004.

6. Daniel Barbara, Ningning Wu, and Sushil Jajodia. Detecting novel network intrusions using bayes estimators. In Proceedings of First SIAM Conference on Data Mining, Chicago, IL, 2001.

7. Eric Bloedorn, Alan D. Christiansen, William Hill, Clement Skorupka, Lisa M. Talbot, and Jonathan Tivel. Data mining for network intrusion detection: How to get started. Technical report, The MITRE Corporation, 2001.

8. Eric Bloedorn, Alan D. Christiansen, William Hill, Clement Skorupka, Lisa M. Talbot, and Jonathan Tivel. Data mining for network intrusion detection: How to get started. Technical report, The MITRE Corporation, 2001.

9. Jianxiong Luo. Integrating fuzzy logic with data mining methods for intrusion detection. Master’s thesis, Department of Computer Science, Mississippi State University, 1999.

10. Stefanos Manganaris, Marvin Christensen, Dan Zerkle, and Keith Hermiz. A data mining analysis of rtid alarms. In Proceedings of the 2nd International Workshop

11. Платонов В. програмно-апаратні засоби захисту інформації. М.: Академія, 2013. 336 с.

12. IDS Snort [Електронний ресурс]: офіц. сайт. URL: http://snort.org

13. IDS Suricata [Електронний ресурс]: офіц. сайт. URL: http://suricata-ids.org

14. Астахов, А.Актуальні питання виявлення мережевих атак / а. Астахов, CISA // Інформаційний бюлетень Jet Info. – 2002. – № 3 (106). - 28 С.

15. Костров, Д. системи виявлення атак / Д.Костров // Byte/Росія. – 2002. – № 8. - С. 20-22, 24-26.

16. IDS / IPS - системи виявлення та запобігання вторгнень [Електронний ресурс]: стаття. Режим доступу: http://netconfig.ru/server/ids-ips/.

17. IDS / IPS-системи виявлення і запобігання вторгнень і хакерських атак [Електронний ресурс]: стаття // сайт компанії «Альтель». - Режим доступу: http://www.altell.ru/solutions/by_technologies/ids/.

18. WinPcap Documentation [Електронний ресурс]: документація. - Режим доступу: http://www.winpcap.org/docs/docs_412/html/main.html

19. Аналіз загроз мережевої безпеки [Електронний ресурс]: стаття / / Лабораторія мережевої безпеки. – 2016. - Режим доступу: http://ypn.ru/138/analysis-of-threats-to-network-security/.

20. Басараб, М. А. аналіз мережевого трафіку корпоративної мережі Університету методами нелінійної динаміки [Електронний ресурс]: стаття / М.А. Басараб, а. в. Колесніков, і. п. Іванов // Наука і освіта: наукове видання / МГТУ ім. Н. Е. Баумана. – 2013. - Режим доступу: http://technomag.bmstu.ru/doc/587054.html.

21. Лукацький, А.запобігання мережевих атак: технології та рішення [Електронний ресурс]: стаття / А. Лукацький // IT-портал. – 2006. - Режим доступу: http://citforum.ru/security/articles/ips/.

22. Мустафаєв, А.Г. Нейромережева система виявлення комп'ютерних атак на основі аналізу мережевого трафіку [Електронний ресурс]: стаття / А. Г,

Мустафаєв. – 2016. - Режим доступу: http://e-notabene.ru/nb/article_18834.html.

23. Новий підхід до захисту інформації-системи виявлення комп'ютерних загроз [Електронний ресурс]: стаття // Jet Info : щомісячне ділове IT видання. - Інфосистеми Джет; Москва, 2007. – № 4. - Режим доступу: http://www.jetinfo.ru/jetinfo_arhiv/novyj-podkhod-k-zaschite-informatsiisistemy-obnaruzheniya-kompyuternykh-ugroz/2007.

24. Snort 3.0 [Електронний ресурс]. URL: http://www.opennet.ru/opennews/art.shtml?num=41255;

25. WinPcap Documentation [Електронний ресурс]: документація. - Режим доступу: http://www.winpcap.org/docs/docs_412/html/main.html

26. Амітан В. Н., Тіміргалєєва Р. Р., Пілюшенко В. Л. Логістизація процесів в організаційно-економічних системах. - Донецьк, 2003.

27. Аналіз загроз мережевої безпеки [Електронний ресурс]: стаття / / Лабораторія мережевої безпеки. – 2016. - Режим доступу: http://ypn.ru/138/analysis-of-threats-to-network-security/.

28. Астахов, А.Актуальні питання виявлення мережевих атак / а. Астахов, CISA // Інформаційний бюлетень Jet Info. – 2002. – № 3 (106). - 28 С.

29. Булдакова Т.і., Джалолов А. Ш. аналіз інформаційних процесів і вибір технологій обробки і захисту даних в ситуаційних центрах. Науково-технічна інформація. Серія 1, 2012, № 6, с. 16-22.

30. Булдакова Т.і., Міков Д. А. Метод підвищення адекватності оцінок інформаційних ризиків. Інженерний журнал: наука та інновації, 2012, вип.

31. Інформаційне суспільство: інформаційні війни. Інформаційне управління. Інформаційна безпека / під ред. М. А. Вуса. – М.: Вид-во СПб. ун-ту, 2006.

32. Костров, Д. системи виявлення атак / Д.Костров //. – 2002. – № 8. - С. 20-22, 24-26.

33. Круглов в.в., Дли м. і., Голунов р. Ю. нечітка логіка і штучні нейронні мережі. Москва, Фізматліт, 2001, 224 с.

34. Лукацький А. В. виявлення атак. 2-е вид. СПб.; БХВ-Петербург, 2003, 596 с.

35. Лукацький, А.запобігання мережевих атак: технології та рішення [Електронний ресурс]: стаття / А. Лукацький // IT-портал. – 2006. - Режим доступу: http://citforum.ru/security/articles/ips/.

36. Атаки на основі аналізу мережевого трафіку [Електронний ресурс]: стаття / А.Г, Мустафаєв. – 2016. - Режим доступу: http://e-notabene.ru/nb/article_18834.html.

37. Новий підхід до захисту інформації-системи виявлення комп'ютерних загроз [Електронний ресурс]: стаття // Jet Info : щомісячне ділове IT видання. - Інфосистеми Джет; Москва, 2007. – № 4. - Режим доступу: http://www.jetinfo.ru/jetinfo_arhiv/novyj-podkhod-k-zaschite-informatsiisistemy-obnaruzheniya-kompyuternykh-ugroz/2007.

38. Платонов В. програмно-апаратні засоби захисту інформації. М.: Академія, 2013. 336 с.

39. Таланов А.Я., Тіміргалєєва Р. Р. використання системного підходу при розробці стратегії підприємства – 2015. - Т. 2. – № 2. - С. 365-370.

40. Тіміргалєєва Р. Р., Гришин і. Ю. інформаційно-логістичне забезпечення процесу управління складними організаційно-економічними системами. - Сімферополь, 2013. - 2-е вид., перероб. і доп.

# ДОДАТКИ

## ДОДАТОК А

**(копії наукових публікацій)**

**Nataliia Lukova-Chuiko**

Doctor of Technical Science, Professor of the Department of Cybersecurity and Information Protection

**Alexander Bystrov**

Student

*Taras Shevchenko National University of Kyiv*

### ADVICE ON SELECTING AN INTRUSION DETECTION SYSTEM FOR SMALL AND MEDIUM-SIZED BUSINESSES

This article provides recommendations for choosing an intrusion detection system for small and medium-sized businesses. These recommendations can be applied in practice by employees of the information security department of the enterprise. These recommendations can significantly increase the level of information security of the enterprise and minimize possible losses in the future.

Keywords: Open-Source, SIEM, Intrusion Detection, Monitoring

In the modern information field, there is an acute problem of information security. This problem includes both protection from attacks and their detection at an early stage in order to minimize the consequences of an attack and respond to it in time. One of the main tools to detect attacks is SIEM-systems, which, if properly configured, reduce the response time to an attack to a minimum. Typically, efficient systems are expensive, and their implementation and support are heavily funded, which can be afforded by an Enterprise or Medium-Business companies. For small companies, SIEM implementation

and maintenance becomes an impossible burden, as usually the means to purchase an SIEM system are bigger than possible losses from a successful attack, which can paralyze the whole business for an indefinite period of time. The way out of this situation are open source applications that can be adapted to штекгішщт detection systems and perform their functions.

This application can be Osquery, the software was developed in 2014 by Facebook. This application is distributed under MIT license, so it can be used for commercial purposes, without any usage fees [1]. The software uses a client architecture, so the application must be installed on each server from which data is to be received. The essence of this application is that the operating system is perceived as a relational database with tables displaying information about the system. These data can be conveniently obtained with the help of SQL language and record both in the log file and sent to a remote syslog-server, which will accumulate data from different endpoints to present a complete picture of the infrastructure security. One example of using this application is the detection of one of the most popular tactics for launching malware, namely deleting the executable file after the process has already been created, making it difficult to detect the attack. So to search for these processes, you need to form a simple SQL query - "SELECT * FROM processes WHERE on_disk = 0", after executing this query, Osquery will display all the processes whose executable files have been removed from the file system. Thus, with the help of this software it is possible to create many markers that will trigger the presence of malicious software in the system. All settings for information security markers are recorded in a configuration file, which also contains settings for information output (syslog-server, log file, etc.) and the frequency of marker checks. Thus, these configuration files are conveniently distributed between a large number of endpoints using automation tools such as Ansible.

The problem with Osquery is that the application does not provide a user-friendly interface to analyze all incidents that have been collected from different parts of the infrastructure, so to use it effectively you need to implement an application to analyze and display this data. This application is ELK-Stack which is also distributed under MIT

license, so it can be used for commercial purposes [2]. This software consists of three components, each of which is responsible for different purposes and tasks. Elasticsearch is the main component of the system, which accumulates data and analyzes them. Kibana - is responsible for managing the components in the web browser interface and building charts, maps and other graphical means of displaying information using data stored in Elasticsearch. The last component used in the system is Logstash. This component is responsible for converting data to provide them in a format understandable to Elasticsearch for further analysis. Together, all these components form a powerful stack of technologies that can be used to analyze and visualize information from different sources. In addition, this software can be used not only for analysis and displaying information security events, but also for its intended purpose, namely as software for analysis and aggregation of log files and collection of metrics for information system operation. It may also be noted that the data is stored in a document-centric database, with effective indexing and mechanisms for managing this data using the API and Index Lifecycle Management. The whole set of tasks for which ELK-Stack can be adapted makes it attractive for implementation in companies with small IT departments and limited financing.

In combination, these software tools provide an opportunity to constantly monitor the entire infrastructure and identify possible attacks, which will minimize losses from them. In addition, the cost of implementing this software package is minimal, as only an information security officer with knowledge of the software is needed. At the same time, this software complex can be developed together with the company that has implemented it and scaled up together with information systems of enterprises.

**References:**

1. Osquery license. Available: https://github.com/osquery/osquery/blob/master/LICENSE-Apache-2.0
2. ELK license. Available: https://github.com/elastic/elasticsearch/blob/master/LICENSE.txt