**МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ**
**НАЦІОНАЛЬНИЙ АВІАЦІЙНИЙ УНІВЕРСИТЕТ**
**КАФЕДРА КОМП'ЮТЕРИЗОВАНИХ СИСТЕМ ЗАХИСТУ ІНФОРМАЦІЇ**

ДОПУСТИТИ ДО ЗАХИСТУ
Завідувач кафедри
_____ С.В. Казмірчук
«_____»_____ 2020 р.

На правах рукопису
УДК

**ДИПЛОМНА РОБОТА**

**ВИПУСКНИКА ОСВІТНЬОГО СТУПЕНЯ**
**«МАГІСТР»**

**Тема**: Система моніторингу мережевого трафіку для захисту локальної інформації на підприємстві

| | |
|---|---|
| **Автор:** | А.В. Колбушков |
| **Науковий керівник:** к.т.н., доц. | к.т.н., доц. А.В. Ільєнко |
| **Нормоконтролер:** к.т.н., доц. | к.т.н., доц. А.В. Ільєнко |

**Київ 2020**

# ВСТУП

Існування і розвиток інформаційного суспільства на сучасному етапі неможливе без використання інформаційних мереж, глобальних комп'ютерних мереж і мереж зв'язку - радіо, телебачення, фіксованих і мобільних телефонних мереж, Інтернет і т.д. У зв'язку з цим забезпечення довіри і безпеки неможливо без пред'явлення до цих мереж не тільки вимог щодо забезпечення надійності передачі даних, стабільності роботи, якості і масштабів охоплення, а й щодо забезпечення інформаційної безпеки.

Питання інформаційної безпеки, захисту інформації і даних нерозривно пов'язані з безпекою програмно-апаратних комплексів та мережевих пристроїв, що утворюють ІС і мережі різного призначення. Такі системи повинні відповідати суворим вимогам по забезпеченню надійності збору, обробки, архівування та передачі даних по відкритим і закритим мереж і забезпечення їх максимального захисту

Мета роботи – реалізація системи моніторингу мережевого трафіку для захисту локальної інформації на підприємстві

Об'єкт дослідження – процедура та процеси реалізації захисту інформації в інформаційно- комунікаційних системах і мережах

Предмет дослідження – системи та програмні засоби моніторингу мережевого трафіку для захисту локальної інформації на підприємстві

Методи досліджень. Проведені дослідження в даній роботі базуються на сучасних методах побудови захищених інформаційних мереж та методах реалізації систем моніторингу мережевого трафіку для захисту локальної інформації.

Виходячи з мети, завданням даної дипломної роботи є:

дослідження сучасних систем та програмних продуктів проведення моніторингу мережевого трафіку для захисту локальної інформації на підприємстві ;розробка програмного модуля моніторингу мережевого трафіку для виявлення атак та інтеграція його в локальну інформаційну систему

підприємства;тестування системи моніторингу мережевого трафіку.

Практична значимість роботи полягає у авторській розробці програмного модулю реалізації клієнт-серверної системи моніторингу мережевого трафіку для захисту локальної інформації на підприємствіз використанням об'єктно-орієнтованої мови програмування Java на базі використанням редактору вихідного коду Visual Studio Code.

Наукова новизна. Удосконалено систему моніторингу мережевого трафіку , за рахунок гнучкості реалізації програмного засобу, а саме впровадження модульності програми, фільтрації, сортування та можливості підтримки різними операційними системам, що дозволило проводити виявлення прихованих мереж та загроз бездротових мереж для захисту локальної інформації на підприємстві.

Колбушков А.В. Аналіз теоретичних аспектів захисту інформації в інформаційно-комунікаційних системах і мережах / Ільєнко А.В., Колбушков А.В. // MATERIÁLY XVI MEZINÁRODNÍ VĚDECKO - PRAKTICKÁ KONFERENCE ZPRÁVY VÝDECKÉ IDEJE -2020 22 - 30 října 2020 r. Volume 5 – P. 28-31.

Колбушков А.В. Програмні методи організації інфраструктури відкритих ключів / Ільєнко А.В., Колбушков А.В. // Nauka i inowacja – 2020: XVI miesdzynarodowej naukowi-praktycznej konferencji: abstracts. – Przemysl (Polska), 2020.

# РОЗДІЛ 1. АНАЛІЗ ТЕОРЕТИЧНИХ АСПЕКТІВ ЗАХИСТУ ІНФОРМАЦІЇ В ІНФОРМАЦІЙНО- КОМУНІКАЦІЙНИХ СИСТЕМАХ І МЕРЕЖАХ

## 1.1. Принципи побудови систем захисту інформації в інформаційно-комунікаційних системах і мережах

Питання організації захисту інформації повинні вирішуватися вже на стадії передпроектної розробки ІС.

Досвід проектування систем захисту ще не достатній. Однак вже можна зробити деякі узагальнення. Похибки захисту можуть бути в значній мірі усунені, якщо при проектуванні враховувати наступні основні принципи побудови системи захисту:

Простота механізму захисту. Цей принцип загальновідомий, але не завжди глибоко усвідомлюється. Механізми захисту повинні бути інтуїтивно зрозумілі і прості у використанні. Застосування засобів захисту не повинно бути пов'язане зі знанням спеціальних мов або з виконанням трудомістких процесів при звичайній роботі законних користувачів[1].

Сталість захисту. Надійний механізм, який реалізує цю вимогу, повинен бути постійно захищена від несанкціонованих змін. Жодна комп'ютерна система не може розглядатися як безпечна, якщо основні апаратні і програмні механізми, покликані забезпечувати безпеку, самі є об'єктами несанкціонованої модифікації або видозміни.

Всеохоплюючий контроль. Цей принцип передбачає необхідність перевірки повноважень будь-якого про рощення до будь-якого об'єкту і лежить в основі системи захисту.

Чи не таємність проектування. Механізм захисту повинен функціонувати досить ефективно навіть у тому випадку, якщо його структура і зміст відомі

зловмиснику. Не має сенсу засекречувати деталі реалізації системи захисту, призначеної для широкого використання. Ефективність захисту не повинна залежати від того, наскільки досвідчені потенційні порушники. Захист не повинна забезпечуватися тільки секретністю структурної організації та алгоритмів функціонування її підсистем. Знання алгоритмів роботи системи захисту не повинно сприяти її подолання (навіть автору).

Ідентифікація. Кожен об'єкт ІВ повинен однозначно ідентифікуватися. При спробі отримання доступу до інформації рішення про санкціонування його слід приймати на підставі даних претендента і визначення вищого ступеня секретності ін формації, з якої йому дозволяється працювати. Такі дані про ідентифікацію та повноваження повинні надійно зберігатися і оновлюватися комп'ютерною системою для кожного активного учасника системи, що виконує дії, що зачіпають її безпеку. Користувачі повинні мати відповідні повноваження, об'єкти (файли) - відповідний гриф, а система повинна контролювати всі спроби отримання доступу[2].

Поділ повноважень. Застосування декількох ключів захисту. Це зручно в тих випадках, коли право на доступ визначається виконанням ряду умов.

Мінімальні повноваження. Для будь-якої програми і будь-якого користувача повинен бути визначений мінімальний коло повноважень, необхідних для роботи.

Надійність. Система ЗІ повинна мати механізм, який дозволив би оцінити забезпечення достатньої надійності функціонування СЗІ (дотримання правил безпеки, секретності, ідентифікації та звітності). Для цього необхідні вивірені і уніфіковані апаратні і програмні засоби контролю. Метою застосування даних механізмів є виконання певних завдань методом, що забезпечує безпеку.

Максимальна відособленість механізму захисту означає, що захист повинен бути відокремлена від функцій управління даними.

Захист пам'яті. Пакет програм, що реалізують захист, повинен розміщуватися в захищеному поле пам'яті, щоб забезпечити системну локалізацію спроб проникнення ззовні. Навіть спроба проникнення з боку

програм операційної системи повинна автоматично фіксуватися, документуватися і відхилятися, якщо виклик виконаний некоректно.

Зручність для користувачів: схема захисту повинна бути в реалізації простої, щоб механізм захисту не створював для користувачів додаткових труднощів.

Авторизація користувача на підставі фізичного ключа дозволяє виключити ненавмисну дискредитацію його прав доступу.

Звітність. Необхідно захищати контрольні дані від модифікації та несанкціонованого знищення, щоб забезпечити виявлення і розслідування виявлених фактів порушення безпеки. Надійна система повинна зберігати відомості про всі події, що мають відношення до безпеки, в контрольних журналах. Крім того, вона повинна гарантувати вибір цікавлять подій при проведенні аудиту, щоб мінімізувати вартість аудиту та підвищити ефективність аналізу. Наявність програмних засобів аудиту або створення звітів ще не означає ні посилення безпеки, ні наявності гарантій виявлення порушень.

Доступність до виконання тільки тих команд операційної системи, які не можуть пошкодити операційну середу і результат контролю попередньої аутентифікації.

Наявність механізмів захисту від:

- ✓ несанкціонованого читання інформації;
- ✓ модифікації зберігається і циркулює в мережі інформації;
- ✓ нав'язування інформації;
- ✓ несанкціонованого відмови від авторства переданої інформації.

Системний підхід до захисту інформації передбачає необхідність врахування всіх взаємопов'язаних, взаємодіючих і змінюються в часі елементів, умов і факторів, істотних для забезпечення безпеки ІС.

Можливість нарощування захисту. Система захисту повинна будуватися з урахуванням не тільки всіх відомих каналів проникнення і несанкціонованого доступу до інформації, а й з урахуванням можливості появи принципово нових шляхів реалізації загроз безпеки.

Комплексний підхід передбачає узгоджене застосування різнорідних засобів захисту інформації.

Адекватність - забезпечення необхідного рівня захисту при мінімальних витратах на створення механізму захисту і забезпечення його функціонування. Важливо правильно вибрати той достатній рівень захисту, при якому витрати, ризик і масштаб можливих збитків були б прийнятними (завдання аналізу ризику) [3].

Мінімізація привілеїв в доступі, що надаються користувачам, тобто кожному користувачеві повинні надаватися тільки дійсно необхідні йому права за зверненням до ресурсів системи і даними.

Повнота контролю - обов'язковий контроль усіх звернень до захищається даними.

Караність порушень. Найбільш поширена міра покарання - відмова в доступі до системи.

Економічність механізму - забезпечення мінімальності витрат на створення і експлуатацію механізму.

Принцип системності зводиться до того, що для забезпечення надійного захисту інформації в сучасних ІС повинна бути забезпечена надійна і узгоджена захист у всіх структурних елементах, на всіх технологічних ділянках автоматизованої обробки інформації та в усі час функціонування ІС.

Спеціалізація, як принцип організації захисту, передбачає, що надійний механізм захисту може бути спроектований і організований лише професійними фахівцями із захисту інформації. Крім того, для забезпечення ефективного функціонування механізму захисту до складу ІС повинні бути включені відповідні фахівці.

Принцип неформальності означає, що методологія проектування механізму захисту і забезпечення його функціонування - неформальна. В даний час не існує інженерної (в традиційному розумінні цього терміна) методики проектування механізму захисту. Методики проектування, розроблені до теперішнього часу, з тримають комплекси вимог, правил, послідовність і зміст

етапів, які сформульовані на неформальному рівні, тобто механічне їх здійснення в загальному випадку неможливо.

Гнучкість системи захисту. Вжиті заходи та встановлені засоби захисту, особливо в початковий період їх експлуатації, можуть забезпечувати як через мірний, так і недостатній рівень захисту. Для забезпечення можливості варіювання рівнем захищеності, засоби захисту повинні мати певну гнучкість. Особливо важливо це властивість в тих випадках, коли встановлення засобів захисту необхідно здійснювати на працюючу систему, не порушуючи процесу її нормального функціонування[5].

Принцип безперервності захисту передбачає, що захист інформації - це не разовий захід і навіть не певна сукупність проведених заходів та встановлених засобів захисту, а безперервний цілеспрямований процес, який передбачає прийняття відповідних заходів на всіх етапах життєвого циклу ІС. Розробка системи захисту повинна здійснюватися паралельно з розробкою захищається системи. Це дозволить врахувати вимоги безпеки при проектуванні архітектури і, в кінцевому рахунку, створити більш ефективні захищені інформаційні системи.

## 1.2. Аналіз загроз безпеці та атак локальної інформації на підприємстві

Інформаційна безпека мереж являє собою "стан захищеності збалансованих інтересів виробників інформаційно-комунікаційних технологій і конкретно мереж, споживачів, операторів і органів державної влади в інформаційній сфері. У свою чергу інформаційна сфера являє собою сукупність інформації, інформаційної інфраструктури, суб'єктів, які здійснюють збір, формування, поширення і використання інформації, а також системи регулювання відносин, що виникають при використаний її мереж зв'язку " [6] .

Завдяки своїй відкритості і загальнодоступності комп'ютерні мережі та мережі зв'язку загального користування є зручним засобом для забезпечення взаємодії громадян, бізнесу та органів державної влади. Однак, чим більше відкриті мережі, тим більше вони уразливі. Можна виділити ряд особливостей, які роблять мережі уразливими, а порушників - практично невловимими:

- ✓ можливість дії порушників на відстані в поєднанні з можливістю приховування своїх справжніх персональних даних (зазначена особливість характерна, зокрема, для мережі Інтернет, радіомереж, мереж кабельного телебачення, незаконного використання ресурсів телефонних мереж);
- ✓ можливість пропаганди і поширення засобів порушення мережевої безпеки (наприклад, поширення в Інтернеті програмних засобів, що дозволяють реалізовувати НСД до інформаційних ресурсів, порушувати авторські права і т.д.);
- ✓ можливість багаторазового повторення атакуючих мережу впливів (наприклад, генерація в Інтернеті або телефонних мережах потоків викликів, що призводять до порушення функціонування вузлів мережі).

Більшість власників і операторів вживають необхідних заходів щодо забезпечення інформаційної безпеки своїх мереж. У той же час для сучасного стану інформаційної безпеки мереж характерні наступні причини, що призводять до великих проблем, що вимагають якнайшвидшого вирішення:

- ✓ використання неузгоджених методів забезпечення інформаційної безпеки для різних компонентів мережі, включаючи телекомунікаційні протоколи, IP і додатки;
- ✓ широке використання технічних засобів імпортного виробництва, потенційно мають декларованих можливостей ( "закладки");
- ✓ відсутність комплексних рішень по забезпеченню інформаційної безпеки при інтеграції та взаємодії мереж;
- ✓ недостатнє опрацювання методології документування функціонування мереж, необхідного для створення доказової бази правопорушень;

- ✓ широко поширене ставлення до забезпечення інформаційної безпеки як до товару чи послуги, які можна купити, а не як до процесу, який потрібно не тільки створити, але який потрібно впровадити в постійне користування та яким необхідно постійно управляти[7].

Найбільш часто зустрічаються такі дефекти захисту, відмічені компаніями, що працюють в області електронного бізнесу та захисту інформації:

- ✓ загальні проблеми в брандмауерах, ОС, мережах та стандартних додатках;
- ✓ непізнані машини або додатки в мережі;
- ✓ використання старих версій програмного забезпечення на машинах мережі;
- ✓ неповна інформація про всі точки входу в мережу із зовнішнього середовища;
- ✓ неповне вилучення прав доступу при звільненні співробітників, наявність ідентифікаторів користувачів, які використовуються за замовчуванням, невірно обслуговуються права доступу;
- ✓ невиправдано відкриті порти в брандмауерах;
- ✓ необґрунтований загальний доступ до файлових систем;
- ✓ недостатні вимоги до ідентифікації користувача, який збирається змінити реєстраційні записи користувачів;
- ✓ присутність непотрібних сервісів або додатків на машинах, що вимагають високого ступеня захисту;
- ✓ використання незахищених настановних параметрів, що привласнюються за замовчуванням при інсталяції додатків, через що стають відомі ідентифікатори і паролі користувачів, встановлені за замовчуванням;
- ✓ відсутність захисту від взаємодії внутрішнього і зовнішнього трафіку мережі;
- ✓ відсутність перевірок після внесення змін в середу (наприклад, після інсталяції нових програм або машин);
- ✓ відсутність контролю внесених змін;

- ✓ відсутність інформації про внутрішні загрози безпеці;
- ✓ відсутність інформації про слабкі місця різних методик аутентифікації при організації потужної захисту.

Будь-яка успішна атака порушника, спрямована на реалізацію загрози інформаційної безпеки мережі, спирається на отримані порушником знання про особливості її побудови і слабких місцях. Причинами появи вразливостей в мережах можуть бути:

- ✓ вразливі зони в поставляється програмний продукт;
- ✓ порушення технологій передачі інформації та управління;
- ✓ впровадження компонентів і програм, що реалізують недекларованих функції і порушують нормальне функціонування мереж;
- ✓ невиконання реалізованими механізмами захисту мережі заданих вимог до процесу забезпечення інформаційної безпеки або пред'явлення непродуманого набору вимог;
- ✓ використання несертифікованих відповідно до вимог безпеки вітчизняних і зарубіжних інформаційних технологій, засобів інформатизації та зв'язку, а також засобів захисту інформації та контролю їх ефективності[8].

Постійний аудит мереж зв'язку з метою виявлення вразливостей і можливих загроз забезпечує визначення "слабкої ланки", а рівень захищеності "слабкої ланки" визначає в кінцевому рахунку рівень інформаційної безпеки мережі в цілому.

Принциповим є розгляд впливів порушників або атак як неминучого фактора функціонування мереж зв'язку. У цих умовах забезпечення інформаційної безпеки мереж зв'язку стає триєдиної завданням, що включає в себе моніторинг функціонування, виявлення атак і прийняття адекватних заходів протидії. Адекватні заходи протидії можуть носити технічний характер і передбачати реконфігурацію інформаційної сфери мережі. Вони можуть бути також організаційними і передбачати звернення операторів мереж зв'язку до силових структур з наданням необхідної інформації для виявлення та притягнення до відповідальності порушників.

Забезпечення інформаційної безпеки мереж зв'язку означає створення процесу, яким необхідно постійно управляти і який є невід'ємною складовою частиною процесу функціонування мереж зв'язку. Побудувавши бізнес-модель функціонування мережі, що включає в себе процес управління забезпеченням інформаційної безпеки, необхідно далі визначити стандарти інформаційної безпеки, що підтримують цю бізнес-модель. Значення досліджень процесів стандартизації та вдосконалення нормативно-правової бази будуть постійно зростати.

Під загрозою безпеки розуміють потенційні дії або події, які можуть прямо чи опосередковано принести втрати – привести до розладу, спотворення чи несанкціонованого використання ресурсів мережі, включаючи інформацію, що зберігається, передається або обробляється, а також програмні і апаратні засоби.

Не існує єдиної загальноприйнятої класифікації загроз, хоча існує багато її варіантів. Приведемо перелік тем подібних класифікацій:

- ✓ по цілі реалізації;
- ✓ по принципу дії на систему;
- ✓ по характеру впливу на систему;
- ✓ по причині появи помилки захисту;
- ✓ по способу дії атаки на об’єкт;
- ✓ по об’єкту атаки;
- ✓ по використовуваних засобах атаки;
- ✓ по стану об’єкту атаки.

Загрози прийнято ділити на випадкові (або ненавмисні) і навмисні. Джерелом перших можуть бути помилки в забезпеченні, виходи з ладу апаратних засобів, неправильні дії користувачів або адміністрації локальної обчислювальної мережі і, так далі. Навмисні загрози, на відміну від випадкових, прагнуть нанести шкоду користувачам (абонентам) локальної обчислювальної мережі і, в свою чергу, діляться на активні і пасивні. Пасивні загрози, як правило, спрямовані на несанкціоноване використання інформаційних ресурсів локальної обчислювальної мережі, не впливаючи при цьому на її функціонування.

Нормальне загрозою є, наприклад, спроба отримання інформації, що циркулює в каналах передачі даної локальної обчислювальної мережі, шляхом підслуховування. Активні загрози прагнуть порушити нормальне функціонування локальної обчислювальної мережі шляхом цілеспрямованого впливу на її апаратні, програмні і інформаційні ресурси. До активних загроз відносяться, наприклад, порушення або радіоелектронне заглушення ліній зв'язку локальної обчислювальної мережі, вивід з ладу ЕОМ або її операційної системи, спотворення відомостей в користувацьких базах даних або системної інформації локальної обчислювальної мережі і т.д. Джерелами активних загроз можуть бути безпосередні дії зловмисників, програмні віруси і, так далі.

До основних загроз безпеки інформації відносяться:

- ✓ розкриття конфіденційної інформації:
- ✓ компрометація інформації;
- ✓ несанкціоноване використання ресурсів локальної обчислювальної мережі;
- ✓ помилкове використання її ресурсів;
- ✓ несанкціонований обмін інформацією;
- ✓ відмова від інформації;
- ✓ відмова в обслуговуванні.

Засобами реалізації загрози розкриття конфіденційної інформації може бути несанкціонований доступ до баз даних, прослуховування каналів локальної обчислювальної мережі і, так далі. В кожному випадку, отримання інформації, що є власністю деякої особи (чи групи), наносить її власникам суттєву шкоду[9].

Компрометація інформації, як правило, здійснюється шляхом внесення несанкціонованих змін в бази даних, в результаті чого її користувач змушений або відмовитись від неї або витратити додаткові зусилля для виявлення змін і відновлення істинних відомостей. У випадку використання скомпрометованої інформації користувач може прийняти невірні рішення з усіма наслідками, що звідси випливають.

Несанкціоноване використання ресурсів локальної обчислювальної мережі, з однієї сторони, є засобом розкриття або компрометації інформації, а з іншої – має самостійне значення, оскільки, навіть не торкаючись користувацької або системної інформації, може нанести певні збитки абонентам або адміністрації локальної обчислювальної мережі. Обсяги збитків можуть змінюватися в широких межах – від скорочення поступлення фінансових ресурсів до повного виходу мережі з ладу.

Помилково санкціоноване використання ресурсів локальної обчислювальної мережі теж може призвести до знищення, розкриття або компрометації вказаних ресурсів. Така загроза найчастіше всього є наслідком помилок програмного забезпечення локальної обчислювальної мережі.

Несанкціонований обмін інформацією між абонентами локальної обчислювальної мережі може призвести до отримання одним із них відомостей, доступ до яких йому заборонений, що по своїх наслідках рівно сильно розкриттю інформації.

Відмова від інформації полягає в невизнанні адресатом чи відправником цієї інформації, фактів її отримання або відправки. Це, зокрема, може послужити аргументованим приводом до відмови однією з сторін від раніше підтриманої угоди (фінансової, торгової, дипломатичної тощо) «технічним шляхом», формально не відмовившись від неї, тим самим може нанести іншій стороні значні збитки[10].

Відмова в обслуговуванні – це дуже суттєва і достатньо розповсюджена загроза, джерелом якої є сама локальна комп’ютерна мережа. Подібна відмова особливо небезпечна в ситуаціях, коли затримка з наданням ресурсів мережі абоненту може привести до тяжких для нього наслідків. Наприклад, відсутність у абонента даних, необхідних для прийняття рішень може бути причиною його нераціональних або неоптимальних дій.

## 1.3. Аналіз засобів захисту в розподілених інформаційно – комунікаційних системах.

В цілому засоби забезпечення захисту інформації в частині запобігання навмисних дій залежно від способу реалізації можна поділити на групи:

Технічні (апаратні) засоби. Це різні за типом пристрою (механічні, електромеханічні, електронні та ін.), Які апаратними засобами вирішують завдання захисту інформації. Вони або перешкоджають фізичній проникненню, або, якщо проникнення все ж таки відбулося, перешкоджають доступу до інформації, у тому числі за допомогою засобів маскування. Першу частину завдання вирішують запірні пристрої, грати на вікнах, захисна сигналізація. Другу - мережеві фільтри, генератори шуму, скануючі радіоприймачі і безліч інших пристроїв, «перекривають» потенційні канали витоку інформації. Переваги технічних засобів пов'язані з їх надійністю, незалежністю від суб'єктивних факторів. Слабкі сторони підходу-недостатня гнучкість, відносно великі обсяг і маса, висока вартість.

Програмні засоби включають програми для ідентифікації користувачів, контролю доступу, шифрування інформації, видалення залишкової інформації типу тимчасових файлів, тестового контролю системи захисту та ін. Переваги програмних засобів - універсальність, гнучкість, надійність, простота установки, здатність до модифікації і розвитку. Недоліки групи - обмежена функціональність мережі, використання частини ресурсів файл-сервера і робочих станцій, висока чутливість до випадкових або навмисним змінам, можлива залежність від типів комп'ютерів.

Змішані апаратно-програмні засоби реалізують ті ж функції, що апаратні і програмні засоби окремо, і мають проміжні властивості.

Організаційні засоби складаються з організаційно-технічних (підготовка приміщень з комп'ютерами, прокладка кабельної системи з урахуванням вимог обмеження доступу) та організаційно-правових (національні законодавства і

правила роботи, встановлені керівництвом конкретного підприємства). Переваги організаційних засобів полягають у тому, що вони дозволяють вирішувати безліч різнорідних проблем, прості в реалізації, швидко реагують на небажані дії в мережі, мають широкі можливості модифікації і розвитку. Недоліки організаційних засобів - висока залежність від суб'єктивних факторів, у тому числі від загальної організації роботи із захисту інформації.

Апаратні засоби захисту інформації – це різноманітні за принципом дії, побудовою і можливостями технічні конструкції, що забезпечують припинення розголошення, захист від витоку і протидію несанкціонованому доступу до джерел конфіденційної інформації.

Апаратні засоби захисту інформації застосовуються для розв’язання таких задач:

- ✓ проведення спеціальних досліджень технічних засобів забезпечення виробничої діяльності на наявність можливих каналів витоку інформації;
- ✓ виявлення каналів витоку інформації на різних об’єктах і в приміщеннях;
- ✓ локалізація каналів витоку інформації;
- ✓ пошук і виявлення засобів промислового шпигунства;
- ✓ протидія несанкціонованому доступу до джерел конфіденційної інформації та іншим діям.

За функціональним призначенням апаратні засоби поділяються на:

- ✓ засоби виявлення;
- ✓ засоби пошуку і детальних вимірювань;
- ✓ засоби активної і пасивної протидії.

При цьому за своїми технічними можливостями засоби захисту інформації можуть бути загального призначення, розраховані на використання непрофесіоналами з метою одержання попередніх (загальних) оцінок, і професійні комплекси, що дозволяють проводити ретельний пошук, виявлення і точні вимірювання всіх характеристик засобів промислового шпигунства[11].

Прикладом перших є група індикаторів електромагнітних випромінювань типу “індикатор поля”, з широким спектром прийнятих сигналів і досить низкою чутливістю.

До других належить, наприклад, комплекс “Дельта”, який призначено для автоматичного виявлення і визначення місцезнаходження радіопередавачів, радіомікрофонів, телефонних закладок і мережевих радіопередавачів. Це вже складний сучасний пошуково-розвідувальний професійний комплекс.

Пошукова апаратура поділяється на апаратуру пошуку засобів знімання інформації та дослідження каналів її витоку.

Апаратура першого типу спрямована на пошук і локалізацію вже впроваджених зловмисниками засобів несанкціонованого доступу. Апаратура другого типу призначається для виявлення каналів витоку інформації.

Визначальними для такого типу систем є оперативність дослідження і надійність отриманих результатів.

Використання професійної пошукової апаратури вимагає високої кваліфікації оператора[12].

Як у будь-якій галузі техніки, універсальність тієї чи іншої апаратури приводить до зниження її параметрів для кожної окремої характеристики. З іншого боку, існує величезна кількість різних за фізичною природою каналів витоку інформації, а також фізичних принципів, на основі яких працюють системи несанкціонованого доступу. Ці фактори обумовлюють різноманіття пошукової апаратури, а її складність визначає високу вартість кожного приладу. В зв’язку з цим достатній комплекс пошукового устаткування можуть дозволити собі мати структури, що постійно проводять відповідні обстеження. Це або великі служби безпеки, або спеціалізовані фірми, що надають послуги стороннім організаціям.

Для самостійного пошуку використовуються в більшості випадків досить прості засоби, які дозволяють проводити профілактичні заходи в проміжку між серйозними пошуковими обстеженнями.

В особливу групу виділяються апаратні засоби захисту комп’ютерів і комунікаційних систем на їхній базі.

Апаратні засоби захисту застосовуються як в окремих комп’ютерах, так і на різних рівнях і ділянках мережі.

Для захисту центральних процесорів застосовується кодове резервування – створення додаткових бітів у форматах машинних команд (розрядів таємності) і резервних регістрів. Одночасно передбачаються два можливих режими роботи процесора, що відокремлюють допоміжні операції від операцій безпосереднього вирішення задач користувача. Для цього служить спеціальна система переривання, реалізована апаратними засобами. Для позначення ступеня конфіденційності програм і даних, категорій користувачів використовуються біти, що називаються бітами конфіденційності (це два-три додаткових розряди, за допомогою яких кодуються категорії таємності користувачів, програм і даних) [13].

Програми і дані, що завантажуються в оперативний запам’ятовувальний пристрій, мають потребу в захисті, що гарантує їх від несанкціонованого доступу. Часто використовуються біти парності, ключі, постійна спеціальна пам’ять. При зчитуванні з оперативної пам’яті необхідно, щоб програми не могли бути знищені несанкціонованими діями користувачів чи унаслідок виходу апаратури з ладу. Для запобігання зчитування даних, що залишилися після обробки в оперативній пам’яті, застосовується спеціальна схема стирання.

Рекомендуються такі заходи щодо захисту носіїв інформації:

- ✓ ведення контролю та перевірка реєстрів носіїв інформації;
- ✓ навчання користувачів правильним методам очищення та знищення носіїв інформації;
- ✓ нанесення міток на носії інформації для відображення рівня критичності інформації, що міститься на них;
- ✓ знищення носіїв інформації відповідно до плану організації;
- ✓ надання тільки авторизованим особам доступу до носіїв інформації для їхнього зберігання, передачі, нанесення міток і знищення;

- ✓ зберігання носіїв інформації в недоступному місці;
- ✓ доведення всіх керівних документів до співробітників.

Апаратні засоби захисту застосовуються також у терміналах користувачів. Для запобігання витоку інформації при підключенні незареєстрованого термінала необхідно перед видачею запитуваних даних здійснити ідентифікацію (автоматичне визначення коду чи номера ідентифікації) термінала, з якого надійшов запит. У багатокористувацькому режимі цього термінала недостатньо. Необхідно здійснити автентифікацію користувача, тобто встановити його дійсність і повноваження. Це необхідно і тому, що різні користувачі, зареєстровані в системі, можуть мати доступ тільки до окремих файлів і строго обмежені повноваження їхнього використання[14].

Для ідентифікації термінала найчастіше застосовується генератор коду, включений в апаратуру термінала, а для автентифікації користувача – такі апаратні засоби:

- ✓ ключі,
- ✓ персональні кодові карти,
- ✓ персональний ідентифікатор,
- ✓ пристрої розпізнавання голосу користувача чи форми його пальців.

Але найбільш розповсюдженими засобами автентифікації є паролі, що перевіряються не апаратними, а програмними засобами розпізнавання.

До програмних засобів зовнішнього захистуналежать програмні засоби забезпечення функціонування фізичних засобів, захисту території, приміщень, окремих каналів зв’язку й пристроїв ІС. У цей час випускається безліч систем охоронної сигналізації, що містять мікропроцесори та комп’ютери. Програмні засоби використовуються також у пристроях біометричного розпізнавання особистості.


Рис. 1.1. Класифікація програмних засобів захисту.

Основним методом захисту даних, що передаються по каналах зв'язку, є криптографічне закриття даних, яке реалізується програмними, апаратними і програмно-апаратними засобами[15].

Крім цього використовуються такі програмні засоби:

- розпізнавання користувачів;
- перевірка рівня таємності каналу;
- перевірка адрес користувачів;
- перевірка ідентифікаторів користувачів під час обміну великими обсягамиданих і т.д.

Ідентифікація – це процедура однозначного розпізнавання унікального імені суб'єкта інформаційної системи.

Автентифікація – це процедура підтвердження того, що пред'явлене ім'я відповідає даному суб'єктові (підтвердження дійсності суб'єкта).

Програмні засоби внутрішнього захистуохоплюють сукупність засобів і механізмів захисту даних, що знаходяться в апаратурі ІС. Їхнім основним призначенням є регулювання і контроль використання даних та ресурсів системи відповідно до встановлених прав доступу.

Типова схема функціонування цих програмних засобів складається з таких основних етапів:

✓ установлення дійсності суб'єкта, що звертається до ресурсів системи;

- ✓ перевірка відповідності характеру запиту наданим повноваженням даного суб’єкта;
- ✓ ухвалення рішення відповідно до результату перевірки повноважень.

Регулювання використання технічних засобів звичайно здійснюється за такими параметрами, як час доступу і запитувана дія при доступі.

Захист програмного забезпечення здійснюється такими методами, як, наприклад, контрольне підсумовування і шифрування.

Програмні засоби керування захистомпризначені для виконання таких завдань:

- ✓ керування користувачами мережі (реєстрація користувачів, генерування службової інформації для користувачів, розсилання службової інформації користувачам);
- ✓ керування базами даних (розподіл ресурсів захисту, координація роботи підсистем системи керування базами даних (СКБД);
- ✓ завдання прийняття рішень у позаштатних ситуаціях (система підтримки ухвалення рішення адміністратором СКБД, вироблення керувальних впливів для усунення порушення функціонування СКБД).

Програмні засоби забезпечення захистуфункціонування СКБД виконують функції контролю, реєстрації, знищення, сигналізації та імітації[16].

Засоби контролюздійснюють тестування елементів СУБД, а також постійний збір інформації про функціонування елементів СКБД. Ця інформація служить вихідними даними для засобів підтримки ухвалення рішення і вироблення керувальних впливів.

Засоби реєстраціїзабезпечують збирання, зберігання, оброблення і видачу даних про стан СКБД.

Засоби знищенняпризначені для знищення залишкових даних і можуть передбачати аварійне знищення даних у випадку прямої загрози несанкціонованого доступу, яке не може бути блоковано системою.

Засоби сигналізаціїпризначені для попередження користувачів при їхньому звертанні до захищених даних і для попередження адміністратора СКБД

при виявленні факту несанкціонованого доступу до даних, спотворення програмних засобів захисту, виході з ладу апаратних засобів захисту тощо.

Засоби імітаціїімітують роботу з порушниками при виявленні спроби несанкціонованого доступу до даних, що захищають. Імітація дозволяє збільшити час на визначення місця і характеру несанкціонованого доступу, що особливо важливо в територіально розподілених мережах, і "відвести" порушника вбік від даних, що захищаються.

Перевагами програмних засобів захисту інформації є:

- ✓ простота тиражування;
- ✓ гнучкість (можливість настроювання на різні умови застосування, що враховують специфіку загроз інформаційній безпеці конкретних ІС);
- ✓ простота застосування – одні програмні засоби, наприклад шифрування, працюють у "прозорому" (непомітному для користувача) режимі, а інші не вимагають від користувача ніяких нових (порівняно з іншими програмами) навичок;
- ✓ практично необмежені можливості їхнього розвитку шляхом внесення змін для врахування нових загроз безпеці інформації.

До недоліків програмних засобів захисту інформації належать:

- ✓ зниження ефективності ІС за рахунок споживання її ресурсів, необхідних для функціонування програм захисту;
- ✓ більш низька продуктивність виконання аналогічних функцій порівняно з апаратними засобами захисту;
- ✓ приєднання багатьох програмних засобів захисту, а не їхня вбудованість у програмне забезпечення, створює для порушника принципову можливість їхнього обходу;
- ✓ можливість злочинної зміни програмних засобів захисту в процесі експлуатації ІС.

Апаратно-програмні засоби, що забезпечують підвищений рівень захисту, можна розбити на п'ять основних груп, рис. 1.2.

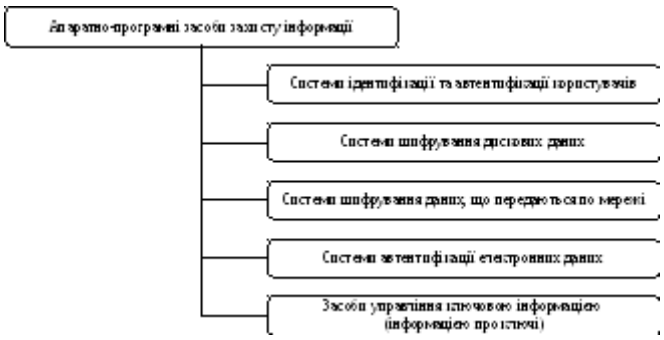


Рис. 1.2. Апаратно-програмні засоби захисту комп'ютерної інформації

Першу групу утворюють системи ідентифікації та автентифікації користувачів. Такі системи застосовуються для обмеження доступу випадкових та незаконних користувачів до ресурсів комп'ютерної системи. Загальний алгоритм роботи цих систем полягає в тому, щоб отримати від користувача інформацію, яка посвідчує його особу, перевірити її справжність і потім надати (чи не надати) цьому користувачу можливість роботи з системою. При побудові подібних систем виникає проблема вибору інформації, на основі якої здійснюються процедури ідентифікації та автентифікації користувача. Можна виділити наступні типи:

1) секретна інформація, якою володіє користувач (пароль, персональний ідентифікатор, секретний ключ тощо); цю інформацію користувач повинен запам'ятати або ж можуть бути застосовані спеціальні засоби зберігання такої інформації;

2) фізіологічні параметри людини (відбитки пальців, рисунок райдужної оболонки ока) чи особливості поведінки людини (особливості роботи на клавіатурі – „клавіатурний почерк" тощо).

Системи ідентифікації, що базуються на першому типі інформації, прийнято вважати традиційними. Системи ідентифікації, що використовують другий тип інформації, називають біометричними. Слід відзначити тенденцію все більшого використання біометричних систем ідентифікації[17].

Другу групу засобів, що забезпечують підвищений рівень захисту, складають системи шифрування дискових даних. Основна задача, що вирішується такими системами, полягає у захисті від несанкціонованого використання даних, розміщених на магнітних носіях інформації. Забезпечення

конфіденційності даних, що розміщуються на магнітних носіях, здійснюється шляхом їх шифрування з використанням симетричних алгоритмів шифрування. Основною класифікаційною ознакою для комплексів шифрування служить їх рівень вбудованості у комп'ютерну систему.

Робота прикладних програм з дисковими накопичувачами складається з двох етапів – логічного та фізичного.

Логічний етап відповідає рівню взаємодії прикладної програми з операційною системою (наприклад, виклик сервісних функцій читання/запису даних). На цьому рівні основним об'єктом є файл.

Фізичний етап відповідає рівню взаємодії операційної системи та апаратури. У якості об'єктів цього рівня виступають структури фізичної організації даних – сектори диску.

В результаті системи шифрування даних можуть здійснювати криптографічні перетворення даних на рівні файлів (захищаються окремі файли) та на рівні дисків (захищаються цілі диски).

Іншою класифікаційною ознакою систем шифрування дискових даних є спосіб їх функціонування. За способом функціонування системи шифрування дискових даних поділяються на два класи:

1) системи прозорого шифрування;
2) системи, які спеціально викликаються для здійснення шифрування.

У системах прозорого шифрування (шифрування „на льоту“) криптографічні перетворення здійснюються в режимі реального часу непомітно для користувача. Наприклад, користувач записує підготовлений у текстовому редакторі документ на захищуваний диск, а система в процесі запису здійснює його шифрування. Системи другого класу зазвичай представляють собою утиліти, які необхідно спеціально викликати для виконання шифрування. До них відносяться, наприклад, архіватори з вбудованими засобами парольного захисту.

До третьої групи засобів, що забезпечують підвищений рівень захисту, відносяться системи шифрування даних, що передаються по комп'ютерним мережам. Розрізняють два основних способи

шифрування: канальне шифрування та кінцеве (абонентське, термінальне) шифрування.

У випадку канального шифрування захищається уся інформація, що передається по каналу зв'язку, включаючи і службову. Відповідні процедури шифрування реалізуються, наприклад, за допомогою протоколу канального рівня семирівневої еталонної моделі взаємодії відкритих систем OSI [Error: Reference source not found]. Цей спосіб має суттєву перевагу – вбудовування процедур шифрування у канальний рівень дозволяє використовувати апаратні засоби, що сприяє підвищенню продуктивності системи. Однак у даного підходу є й суттєві недоліки:

- ✓ шифруванню на даному рівні підлягає уся інформація, включаючи службові дані транспортних протоколів, що ускладнює механізм маршрутизації мережних пакетів та вимагає розшифровування даних в пристроях проміжної комутації (шлюзах, ретрансляторах тощо);
- ✓ шифрування службової інформації, неминуче на даному рівні, може привести до появи статистичних закономірностей у шифруванні даних, що впливає на надійність захисту і накладає обмеження на використання криптографічних алгоритмів[18].

Кінцеве(абонентське) шифрування дозволяє забезпечити конфіденційність даних, що передаються між двома прикладними об'єктами (абонентами). Кінцеве шифрування реалізується за допомогою протоколу прикладного чи представницького рівня еталонної моделі OSI [Error: Reference source not found]. В цьому випадку захищається тільки зміст повідомлення, вся ж службова інформація залишається відкритою. Даний спосіб дозволяє уникнути проблем, пов'язаних із шифруванням службової інформації, але при цьому виникають інші проблеми. Зокрема, зловмисник, який має доступ до каналів зв'язку комп'ютерної мережі, отримує можливість аналізувати інформацію про структуру обміну повідомленнями, наприклад, про відправника і отримувача, про час і умови передачі даних, а також про об'єм даних, що передаються.

Четверту групу засобів захисту складають системи автентифікації електронних даних. При обміні електронними даними по мережах зв'язку виникає проблема автентифікації автора документу та самого документу – встановлення справжності автора та перевірка відсутності змін в отриманому документі. Для автентифікації електронних даних застосовують код автентифікації повідомлення (імітовставку) чи електронний цифровий підпис. При формуванні коду автентифікації повідомлення та електронного цифрового підпису використовують різні типи систем шифрування.

Код автентифікації повідомлення формують за допомогою симетричних систем шифрування даних. Зокрема, симетричний алгоритм шифрування даних DES при роботі в режимі зчеплення блоків шифру CBC дозволяє сформувати за допомогою секретного ключа та початкового вектора IV код автентифікації повідомлення MAC (Message Authentication Code) [Error: Reference source not found]. Перевірка цілісності прийнятого повідомлення здійснюється шляхом перевірки коду MAC отримувачем повідомлення. Аналогічні можливості надає алгоритм ГОСТ 28147-89 [Error: Reference source not found], в якому передбачено режим вироблення імітовставки, яка забезпечує імітозахист – захист системи шифрування зв'язку від нав'язування неправдивих даних. Імітовставка виробляється з відкритих даних шляхом спеціального перетворення шифрування з використанням секретного ключа і передається по каналу зв'язку в кінці зашифрованих даних. Імітовставка перевіряється отримувачем повідомлення, який володіє секретним ключем, шляхом повторення процедури, виконаної раніше відправником, над отриманими відкритими даними[19].

Електронний цифровий підпис (ЕЦП) представляє собою відносно невеликий об'єм додаткової автентифікуючої цифрової інформації, що передається разом із „підписаними" даними. Для реалізації ЕЦП використовуються принципи асиметричного шифрування. Система ЕЦП включає процедуру формування цифрового підпису відправником з

використанням секретного ключа відправника та процедуру перевірки підпису отримувачем з використанням відкритого ключа відправника.

П’яту групу засобів, що забезпечують підвищений рівень захисту, утворюють засоби управління ключовою інформацією. Під ключовою інформацією тут розуміється сукупність усіх використовуваних в комп’ютерній системі чи мережі криптографічних ключів. Безпека будь-якого криптографічного алгоритму визначається використовуваними криптографічними ключами. У випадку ненадійного управління ключами зловмисник може заволодіти ключовою інформацією та отримати повний доступ до всієї інформації в комп’ютерній системі чи мережі. Основною класифікаційною ознакою засобів управління ключовою інформацією є вид функції управління ключами. Розрізняють такі основні види функцій управління ключами: генерація ключів, зберігання ключів та розповсюдження ключів.

Способи генерації ключів розрізняються для симетричних і асиметричних криптосистем. Для генерації ключів симетричних криптосистем використовуються апаратні та програмні засоби генерації випадкових чисел, зокрема системи із застосуванням блочного симетричного алгоритму шифрування. Генерація ключів для асиметричних криптосистем є значно складнішою задачею у зв’язку з необхідністю отримання ключів з певними математичними властивостями[20].

Функція зберігання ключів передбачає організацію безпечного зберігання, обліку та знищення ключів. Для забезпечення безпечного зберігання та передачі ключів застосовують їх шифрування з використанням інших ключів. Такий підхід приводить до концепції ієрархії ключів. До ієрархії ключів зазвичай входять головний ключ (майстер-ключ), ключ шифрування ключів та ключ шифрування даних. Слід зазначити, що генерація та зберігання майстер-ключів є критичними питаннями криптографічного захисту.

Розповсюдження ключів є найвідповідальнішим процесом в управлінні ключами. Цей процес повинен гарантувати секретність розповсюджуваних ключів, а також оперативність і точність їх розповсюдження. Розрізняють два

основних способи розповсюдження ключів між користувачами комп’ютерної мережі:

- ✓ використання одного чи кількох центрів розповсюдження ключів;
- ✓ прямий обмін сеансовими ключами між користувачами.

Закони й нормативні акти виконуються тільки в тому випадку, якщо вони підкріплюються організаторською діяльністю відповідних структур, створюваних у державі, у відомствах, установах і організаціях. При розгляді питання безпеки інформації така діяльність ставиться до організаційних методів захисту інформації.

Закони й нормативні акти виконуються тільки в тому випадку, якщо вони підкріплюються організаторською діяльністю відповідних структур, створюваних у державі, у відомствах, установах і організаціях. При розгляді питання безпеки інформації така діяльність ставиться до організаційних методів захисту інформації.

Організаційні методи захисту інформації включають заходи та дії, які повинні здійснювати посадові особи в процесі створення й експлуатації системи для забезпечення заданого рівня безпеки інформації.

Відповідно до законів і нормативних актыв у міністерствах, відомствах, на підприємствах (незалежно від форм власності) для захисту інформації створюються спеціальні служби безпеки (на практиці вони можуть називатися й інакше). Ці служби підпорядковуються, як правило, керівництву установи. Керівники служб організують створення й функціонування систем захисту інформації. Повну відповідальність за стан інформаційної безпеки несуть керівники організації. На організаційному рівні вирішуються наступні завдання забезпечення безпеки інформації в системи:

- ✓ організація робіт з розробки системи захисту інформації;
- ✓ обмеження доступу на об'єкт і до ресурсів системи;
- ✓ розмежування доступу до ресурсів системи;
- ✓ планування заходів;
- ✓ розробка документації;

- ✓ виховання й навчання обслуговуючого персоналу й користувачів;
- ✓ сертифікація засобів захисту інформації;
- ✓ ліцензування діяльності по захисту інформації;
- ✓ атестація об'єктів захисту;
- ✓ удосконалювання системи захисту інформації;
- ✓ оцінка ефективності функціонування системи захисту інформації;
- ✓ контроль виконання встановлених правил роботи в системи.

Організаційні методи є базисом комплексної системи захисту інформації в системи. Тільки за допомогою цих методів можливе об'єднання на правовій основі технічних, програмних і криптографічних засобів захисту інформації в єдину комплексну систему. Конкретні організаційні методи захисту інформації будуть приводитися при розгляді протидії загрозам безпеки інформації. Найбільша увага організаційним заходам приділяється при викладі питань побудови й організації функціонування комплексної системи захисту інформації.

До методів і засобів організаційного захисту інформації відносяться організаційно-технічні й організаційно-правові заходи, проведені в процесі створення й експлуатації системи для забезпечення захисту інформації. Ці заходи повинні проводитися при будівництві або ремонті приміщень, у яких буде розміщатися системи; проектуванні системи, монтажі й налагодженню її технічних і програмних засобів; випробуваннях і перевірці працездатності системи[21].

Основні властивості методів і засобів організаційного захисту:

- ✓ обмеження фізичного доступу до об'єктів захисту та реалізація режимних заходів;
- ✓ обмеження можливості перехоплення ПЕМВН;
- ✓ розмежування доступу до інформаційних ресурсів і процесам (встановлення правил розмежування доступу , шифрування інформації при її зберіганні і передачі , виявлення та знищення апаратних і програмних закладок);
- ✓ резервне копіювання найбільш важливих з точки зору втрати масивів документів;

- ✓ перед проведенням наради необхідно проводити візуальний огляд приміщення на предмет виявлення закладних пристроїв;
- ✓ кількість осіб, що у конфіденційних переговорах має бути обмежена до мінімуму;
- ✓ вхід сторонніх осіб під час проведення наради має бути заборонений;
- ✓ повинна бути чітко розроблена охорона виділеного приміщення під час наради , а також спостереження за обстановкою на поверсі ;
- ✓ будь-які роботи в кімнаті , що проводяться поза часом проведення конфіденційних нарад, наприклад: прибирання , ремонт побутової техніки, невеликий косметичний ремонт, повинен проводитися в обов'язковій присутності працівника служби безпеки;
- ✓ після проведення наради кімната повинна ретельно оглядатися , закриватися і опечатуватися;
- ✓ між нарадами кімната повинна бути закрита і опечатана відповідальною особою;
- ✓ профілактику зараження комп'ютерними вірусами.

Основою проведення організаційних заходів є використання й підготовка законодавчих і нормативних документів в області інформаційної безпеки, які на правовому рівні повинні регулювати доступ до інформації з боку користувачів.

**Висновки до розділу**

Комп’ютерні мережі внаслідок притаманних їм особливостей створюють умови для виникнення численних загроз безпеці інформації. Розподіл ресурсів та інформації у просторі робить можливим специфічний вид атак – так звані мережеві, або віддалені атаки (англ. *–network attacks, remoteattacks*). Під віддаленою атакою розуміють атаку на розподілену обчислювальну систему, що здійснюється програмними засобами по каналах зв’язку. Така атака може

здійснюватись як на протоколи і мережеві служби, так і на операційні системи і прикладні програми вузлів мережі.

Одною з фундаментальних причин потенційної вразливості мереж є принцип їхнього функціонування. Інформаційний обмін у мережі здійснюється за допомогою механізму повідомлень. Людина практично не бере участь у штатному функціонуванні мережі. У вузлах мережі знаходяться апаратні і програмні засоби, які діють автоматично, без втручання оператора. Ці засоби призначені для того, щоби передавати і приймати дані з мережі. Для цього вони повинні відповідати на повідомлення-запити, які надходять з мережі і регламентуються протоколами взаємодії. Спеціальним чином створені запити можуть викликати такі відповіді автоматичних засобів, які призведуть до порушення політики безпеки. Крім того, атака може бути спрямованою не на комп'ютер у мережі, а на інформацію, що по мережі передається.

Мережа Інтернет становить особливу небезпеку через свою доступність і глобальний масштаб. В цій мережі присутні і активно діють численні зловмисники – як професіонали, так і просто допитливі підлітки, які знайшли інструменти злому – відповідне програмне забезпечення доступно у мережі – і тепер намагаються їх випробувати. В глобальній мережі одночасно діють численні представники кримінальних структур, різних політичних партій і течій, правоохоронних органів і спецслужб різних країн. Атака на систему, що підключена до мережі, може бути мотивована матеріально чи політично. А зловмисники, навіть якщо вдасться їх вистежити, можуть знаходитись у іншому правовому полі (в іншій державі) і бути недосяжними для покарання.

# РОЗДІЛ 2. ХАРАКТЕРИСТИКА СИСТЕМ МОНІТОРИНГУ ТА ВИЯВЛЕННЯ АТАК

## 2.1. Методи моніторингу та виявлення атак

Термін «виявлення вторгнень» вперше з'явився в роботах американських вчених Д. Андерсона і Д. Деннинг в 1980-і рр. Недивлячись на досить велику кількість наявних публікацій, говорити про створення теорії виявлення вторгнень і аномалій кіберсистем поки рано. Питання аксіоматики, термінології, методології та зв'язку теорії виявлення вторгнень і аномалій з іншими науковими дисциплінами знаходяться в стадії становлення. Порівняльний аналіз відомих моделей і методів виявлення вторгнень і аномалій показав наступне. Найбільший вплив на властивості груп методів виявлення вторгнень і аномалій існує за двома системами класифікацій: за рівнем оброблюваних даних і за схемою прийняття рішень про наявність факту порушення (алгоритму вирішальної схеми).Класифікація за рівнем оброблюваних даних поділяє на методи, що аналізують:

- ✓ Двійкове представлення даних чи кодів команд;
- ✓ Команди, операції, події та/або їх параметри (окремо від їх фізичного представлення в засобах обчислювальної техніки);
- ✓ Характеристики системи, прямо чи опосередковано відображаючі її цільове призначення, наприклад, статистику задіяних ресурсів, кількість оброблених даних за одиницю часу запитів, швидкість та інші характеристики мережевого обміну.

Алгоритми низькорівневого (машинно-залежного) аналізу, як правило, набагато більш прості в реалізації, мають високу швидкодію і найменш вимогливі до ресурсів. З іншого боку, більш цілеспрямованим потоком інформації, що потенційно підвищує якість прийнятих рішень при тих же витратах обчислювальних потужностей, а крім того має певний ступінь від

платформи незалежності. Найбільш високий рівень аналізу стану АС (клас У.3) зазвичай інформує про наявні відхилення опосередковано, що часто вимагає залучення експерта з метою виявлення справжньої причини нештатного функціонування АС.

Однак в деяких випадках він може бути єдиним джерелом відомостей про що проводиться деструктивному інформаційно-технічним впливі (наприклад, при розподіленої атаки типу «відмова в обслуговуванні» шляхом формування великої кількості коректних, але ресурсномістких запитів і схожих випадках).

Класифікація за схемою прийняття рішення про факт деструктивного інформаційно-технічного впливу противника представляється найбільш адекватною в розрізі підходу з позицій теорії розпізнавання образів, до якої в загальному випадку стосується ця задача[22].

Структурні методи розпізнавання формують строгу модель або свідомо коректного стану або впливу, або свідомо злочинного впливу. Інші варіанти дій, в т. Ч. Можливо коректні або шкідливі (але невідомі на момент створення моделі), не аналізуються і призводять або до помилок I-го роду, або до помилок II-го роду в залежності від обраного алгоритму аналізу. До переваг методів даного класу відноситься повна відсутність помилкових спрацьовувань в області, описуваної моделлю, до недоліків - принципова неможливість опису нових, невідомих раніше, або не укладаються в розроблену модель методів злочинних дій.

Контроль корректності стану. Алгоритми інспектування виконують найбільш жорсткий контроль над системою: перевірка цілісності файлів (реалізовані в системах Tripwire, AIDE і аналогічних), областей пам'яті або більш складних структур даних (наприклад, баз префіксів мережевих маршрутів, на основі тих чи інших записів про завідомо коректному їхньому фінансовому стані: розмір файлів, контрольні суми, криптостійкі хеш-суми і т. п.

Алгоритми контролю графа станів / графа переходів моделі системи або протоколу є найбільш широко досліджуваний підклас структурних методів. Аналізу піддаються значущі події, що відбуваються в системі, про яку відомо її

поточний стан. Опис тих чи іншим способом дозволених для кожного стану переходів дозволяє генерувати події при відхиленні поведінки системи від дозволеного. Однією з перших робіт в даному напрямку були дослідження P. Porras і K. Ilgun, реалізовані в системах STAT і USTAT відповідно. Згодом всередині виділився підклас методів, що використовує для контролю за послідовністю подій мережі Петрі. В даний час ведуться дослідження, спрямовані на підвищення гнучкості опису допустимого поведінки системи (наприклад, в дисертації Д. Ю. Гамаюнова) і на автоматизацію процесу побудови графа дозволених переходів.

Алгоритми контролю політики штатних впливів є повне або часткове опис дозволених дій на систему, тим самим формуючи політику «заборонено все, що не дозволено» (англ. «Default deny»), будь-яка спроба порушення якої формує інформує подія. Поряд з алгоритмами інспектування представляє підклас, який має найбільшу історію в області виявлення комп'ютерних атак. Різні варіанти реалізації даного підходу були впроваджені в безліч систем контролю доступу.

Контроль(пошук) позаштатних впливів. Алгоритми контролю політики позаштатних впливів представляють опис переліку свідомо заборонених дій на систему, формуючи політику «дозволено все, що не заборонено» (англ. «Default allow»). На відміну від контролю політики. штатних впливів, яка може бути виведена з протоколу або деякого формального опису бажаного поведінки системи, формування повного переліку заборонених дій важко, а в багатьох випадках і неможливо через складність і багаторівневість інформаційних систем. Вирішальні правила даного класу позбавлені помилок «помилкового спрацьовування», що дає їм значно перевага при впровадженні в системах без участі людини-оператора. Однак вони не в змозі виявляти нові, не враховані в їх базі знань типи злочинних дій на систему, а отже, якість їх роботи багато в чому залежить від швидкості актуалізації моделі зловмисника.

Сигнатурні алгоритми виконують пошук заздалегідь відомих шаблонів комп'ютерних вторгнень і відрізняються рівнем аналізу (відповідно до наведеної вище класифікації), а також різним ступенем деталізації / узагальнення

шаблонів. Алгоритми цього класу використовують антивірусні програмні продукти, а також системи фільтрації мережевого трафіку (в т. ч. поштового і веб-контенту). Совре менниє дослідження в цьому класі на рівні аналізу команд / подій присвячені в першу чергу універсалізації баз знань з метою уніфікованої актуалізації відомостей про атаки різної етимології, рівнів та інтенсивності, а також питань масштабованості систем на їх основі. У підкласі методів, що виконують пошук на байторієнтованому рівні, дослідження ведуться в області автоматичної генерації сигнатур вторгнень, а також в області пошуку ефективних методів протидії мімікрії і поліморфізму в атаках (наприклад, шляхом аналізу графа переходів в двійковому коді хробака[23].

Кореляційні методи вводять метрики відмінності спостережуваного вектора ознак або більш складної (наприклад, поведінкової) характеристики від свідомо коректного або свідомо злочинного стану. Характеризуються тим, що формують певні (позитивні або негативні) значення для всієї множини впливів - в тому числі це стосується і надзвичайно малоймовірних станів (хоча ступінь достовірності при ухваленні рішення в них невелика). Перевагою кореляційних методів є покриття всієї множини допустимих впливів, що гіпотетично дозволяє приймати коректні рішення і щодо невідомих раніше атак. Завдання сукупного зниження рівня помилок як I-го так і II-го роду є основною для даного класу алгоритмів. Стосовно всіх кореляційним методам можливі як реалізації в режимі «навчання з учителем» так і в режимі самонавчання (адаптивний режим).

Алгоритми «без пам'яті» розглядають кожну подію (вплив, перехід системи з одного стану в інший, або один відлік вимірювання будь-якої характеристики системи) як окремий елемент безлічі, щодо якої необхідно прийняти рішення. До даного класу також можна застосувати термін методи простору ознак.

З одновимірним вектором ознак. Порогові алгоритми генерують інформаційне події про факт виявлення аномалії по перевищенню спостережуваного значення деякої граничної величини. Порогові алгоритми були першими представниками класу кореляційних методів виявлення

вторгнень, зокрема, вони описані і в основоположною для всієї області IDS роботі D. Denning в 1987 р і в системі Haystack (1988). Найбільше застосування на практиці отримав контроль за обсягом запитуваних в системі ресурсів і за частотами тих чи інших подій в системі.

З багатовимірним вектором ознак. Алгоритми лінійної класифікації в багатовимірному просторі ознак в даний час поступилися позиції алгоритмам кластерного і нейросетевого аналізу, як більш гнучким.

Кластерний аналіз як зарекомендував себе метод класифікації набув широкого застосування і в області виявлення комп'ютерних атак. В даний час дослідження проводяться як в напрямку виявлення без вчителя (пошук значних відхилень), наприклад, в роботах L. Portnoy, так і кластеризації з попереднім навчанням на розмічених вхідних даних.Нейромережеві методи використовують для прийняття рішення про наявність чи відсутність злочинного впливу вирішальну схему на базі нейронної мережі. Перші роботи в цьому класі відносяться до кінця 1990-х рр. В даний час кількість різних методів в даному класі достатній точно велике, в т. ч. існують і незалежні вітчизняні дослідження. Зокрема в роботі В. В. Райха, І. Н. Синиці і С. М. шарашкіних пропонується використовувати нейронні мережі адаптивного резонансу, а в роботі С. В. Васютіна і С. С. Зав'ялова рішення приймається нейронною мережею на підставі вектора, що містить частоти системних запитів і ідентифікатор стану контрольованого обчислювального процесу.

Імунні методи роблять спробу поширити принципи виявлення і протидії імунної системи живих істот чужорідним вірусам. Система включає в себе централізовану «бібліотеку генів» формує обмежений набір векторів, що характеризують потенційно чужорідні події, і розподілену систему датчиків, що виконують власне детектування впливів, і що володіють зворотним зв'язком з «бібліотекою генів». Методи характеризуються невибагливістю до ресурсів, проте, в деяких умовах формують високий потік помилкових подій.

Алгоритми «з пам'яттю» аналізують події з урахуванням деякої передісторії, а також, можливо, істинного або передбачуваного стану системи.

Детерміновані алгоритми контролю поведінки генерують події з будь-якого факту відхилення поведінки системи від профілю, створеного на етапі навчання, і є деяким аналогом інспектуючих алгоритмів в класі структурних методів. У разі невдалого вибору об'єкта захисту або переліку контрольованих подій можуть генерувати високий потік помилкових спрацьовувань. В основному витіснені нечіткими алгоритмами як більш гнучкими. Нечіткі алгоритми контролю поведінки обчислюють в ході аналізу послідовності подій тим чи іншим чином вектор імовірнісних характеристик і генерують подія тільки по перевищенню ними деяких порогових значень. Аналіз можливий як на рівні байт, наприклад аналізуються параметри системних запитів, так і на рівні команд / подій.

До основних тенденцій розвитку сучасних методів виявлення вторгнень і аномалій кіберсистем відносяться[24]:

- ✓ підвищення достовірності та точності методів виявлення вторгнень і аномалій (зниження рівнів помилок I-го і II-го роду, особливо щодо раніше не спостерігалися інформаційно-технічних впливів);
- ✓ збільшення частки коригувальних процесів, які не потребують участі людини експерта, що знижує рівень евристичного прийняття рішення і дозволяє перевести час реакції на зловмисне вплив на якісно новий рівень (наприклад, при автоматичній генерації сигнатур для нового шкідливого коду через кілька хвилин після підтвердження факту його аномально швидкого поширення по мережі);
- ✓ протидія новим технологіям, що використовуються зловмисниками з метою: приховування факту шкідливого впливу, наприклад, за допомогою поліморфних кодувальників виконуваного коду і даних або техніки мімікрії ( «розчинення» або маскування в нормальному трафіку) атак; активного впливу на саму систему виявлення атак шляхом формування умов відмови в обслуговуванні або генерації надмірного потоку помилкових спрацьовувань, що робить її застосування неможливим.

## 2.2. Класифікація систем виявлення атак

Системи виявлення атак, які контролюють окремий комп'ютер, як правило, збирають і аналізують інформацію з журналів реєстрації операційної системи і різних додатків (Web-сервер, СУБД і т.д.). За таким принципом функціонує RealSecure OS Sensor. Однак останнім часом стали отримувати поширення системи, тісно інтегровані з ядром ОС, тим самим, надаючи більш ефективний спосіб виявлення порушень політики безпеки. Причому така інтеграція може бути реалізовано двояко. По-перше, можуть контролюватися всі системні виклики ОС (так працює Entercept) або весь вхідний / вихідний мережевий трафік (так працює RealSecure Server Sensor). В останньому випадку система виявлення атак захоплює весь мережевий трафік безпосередньо з мережевої карти, минаючи операційну систему, що дозволяє зменшити залежність від неї і тим самим підвищити захищеність системи виявлення атак[25].

Системи виявлення атак рівня мережі збирають інформацію з самої мережі, тобто з мережевого трафіку. Виконуватися ці системи можуть на звичайних комп'ютерах (наприклад, RealSecure Network Sensor), на спеціалізованих комп'ютерах (наприклад, RealSecure for Nokia або Cisco Secure IDS 4210 і 4230) або інтегровані в маршрутизатори або комутатори (наприклад, CiscoSecure IOS Integrated Software або Cisco Catalyst 6000 IDS Module). У перших двох випадках анализируемая інформація збирається за допомогою захоплення і аналізу пакетів, використовуючи мережеві інтерфейси в безладному (promiscuous) режимі. В останньому випадку захоплення трафіку здійснюється з шини мережевого обладнання.

Виявлення атак вимагає виконання одного з двох умов - або розуміння очікуваного поведінки контрольованого об'єкта системи або знання всіх можливих атак і їх модифікацій. У першому випадку використовується технологія виявлення аномального поведінки, а в другому випадку - технологія виявлення злочинного поведінки або зловживань. Друга технологія полягає в

описі атаки у вигляді шаблону або сигнатури і пошуку даного шаблону в контрольованому просторі (наприклад, мережевий трафік або журналі реєстрації). Ця технологія дуже схожа на виявлення вірусів (антивірусні системи є яскравим прикладом системи виявлення атак), тобто система може виявити всі відомі атаки, але вона мало пристосована для виявлення нових, ще невідомих, атак. Підхід, реалізований в таких системах, дуже простий і саме на ньому засновані практично всі пропоновані сьогодні на ринку системи виявлення атак.

### 2.2.1. Системи, що забезпечують виявлення атак на мережному рівні

Існують дві типові архітектури таких систем: автономна система і агент - менеджер. Перша занадто проста і в даний час в комерційних продуктах практично не зустрічається. Програми, створені на її основі, потрібно встановлювати на кожен контрольований комп'ютер. Зв'язок між автономними системами, встановленими на різних комп'ютерах, відсутня, і журнали реєстрації адміністратору доводиться завантажувати на свій комп'ютер за допомогою інших засобів або аналізувати ці журнали, здійснюючи віддалений вхід на кожен комп'ютер. Очевидно, що в великих, територіально розподілених мережах це нереально.

Для сучасних мереж більш ефективна архітектура агент - менеджер, оскільки інформація про події, що реєструються агентами на кожному контрольованому комп'ютері, передається на центральну консоль (менеджер). З цієї ж консолі здійснюється управління віддаленими агентами та їх налаштування.

До переваг систем виявлення атак, які аналізують журнали реєстрації, можна віднести:

- можливість виявлення атаки на конкретний вузол;

- можливість оцінити підсумки атаки. Оскільки IDS працює з подіями, вже зафіксованими в журналі реєстрації, можна з упевненістю стверджувати, була відображена атака чи ні;

- ефективність застосування в комутованих мережах і мережах з канальним шифруванням.

Однак у таких систем є і свої недоліки. Вони не можуть виявити атаки, спрямовані на ті вузли, де не ведуться журнали реєстрації, або на платформи, для яких не існує відповідного програмного забезпечення. Крім того, їх не можна використовувати для раннього виявлення атак.

Для вирішення цих проблем були розроблені системи виявлення атак на рівні мережі (Network-based IDS): вони аналізують мережевий трафік в реальному масштабі часу і порівнюють його із заздалегідь визначеними сигнатурами атак. У мережевих IDS є дві основні переваги. По-перше, один агент такої системи може переглядати цілий сегмент мережі з великим числом вузлів. Можуть бути виявлені атаки проти будь-яких елементів мережі підприємства, починаючи від маршрутизаторів і міжмережевих екранів і закінчуючи Web-серверами і серверами баз даних. По-друге, мережеві IDS здатні ідентифікувати атаки в реальному часі, завдяки чому можуть бути оперативно вжито заходів протидії[26].

Назвемо інші переваги таких систем.

Зловмисник не може приховати сліди своєї діяльності. При виявленні атак в реальному часі IDS мережевого рівня використовують поточний мережевий трафік, тому хакер не може видалити сліди своєї присутності. Аналізовані дані містять не тільки інформацію про метод атаки, але і відомості, які можуть допомогти при ідентифікації зловмисника і фігурувати як доказ в суді. Однак, оскільки багато хакерів добре знайомі з журналами реєстрації, вони знають, як маніпулювати цими файлами для приховування слідів своєї діяльності, щоб знизити ефективність систем рівня ОС, що користуються цією інформацією для виявлення атаки.

Системи можуть виявляти невдалі атаки або підозрілу діяльність. IDS мережевого рівня, встановлена з зовнішнього боку брандмауера (МСЕ), здатна фіксувати атаки, націлені на захищаються ресурси, навіть якщо екран відобразить ці спроби. Системи захисту, встановлені на вузлах всередині мережевого периметра, не бачать відображених атак, які не досягають вузлів, захищених МСЕ. Тим часом ця втрачена інформація може мати дуже важливе значення при оцінці і вдосконаленні політики безпеки.

Проте системи виявлення мережевих атак на рівні мережі мають і свої недоліки.

По-перше, їх застосування в високошвидкісних мережах пов'язано з певними проблемами. Сучасні комерційні системи захисту, незважаючи на декларовану можливість роботи з мережами Fast Ethernet (100 Мбіт / с), не можуть ефективно працювати в мережах із пропускною здатністю вище 80 Мбіт / с, отже, при швидкості передачі інформації понад 100 Мбіт / с (наприклад, для каналу ATM OC-3) вони непридатні.

По-друге, мережеві IDS неефективно працюють в комутованих мережах і мережах з канальним шифруванням[27].

Відзначимо, що IDS мережевого і системного рівнів зі своїми достоїнствами і перевагами ефективно доповнюють один одного і взаімоустраняют недоліки.

Завершуючи короткий опис наявних рішень в області виявлення атак, спробуємо відповісти на питання: чи підійдуть ці рішення в їх сучасному вигляді для захисту мереж в недалекому майбутньому?

На цей рахунок є серйозні сумніви. Мережі стали настільки складними, що їх важко контролювати існуючими методами. Число вузлів зростає з небувалою швидкістю. З появою гігабітних швидкостей і комутованих віртуальних приватних мереж обсяг переданого по мережах трафіку зріс на кілька порядків. Виникає необхідність в абсолютно нові підходи до виявлення атак, що дозволяють впоратися з цими проблемами.

Розглянемо такі підходи до створення ПО засобів захисту, які дозволять ефективно виявляти нові атаки, можливо, лише в наступному тисячолітті.

Мікроагенти. Як уже зазначалося, нинішні програми виявлення атак відносяться або до класу мережевих (network-based), або до класу системних (host-based) продуктів. Проте ідеальним рішенням було б створення системи, що поєднує в собі обидві технології, т. Е. На кожен контрольований вузол повинен бути встановлений агент системи виявлення атак, який контролював би атаки не тільки на прикладному рівні (ОС і додатків), але і мережеві атаки, спрямовані на даний вузол. У порівнянні з існуючими рішеннями такий підхід має кілька переваг.

По-перше, висока швидкість роботи мережі вже не викликає особливих проблем, оскільки зазначений агент не переглядає трафік всій мережі, зупиняючись лише на трафіку даного вузла. По-друге, розшифровка пакетів здійснюється перш, ніж вони досягнуть агента. І нарешті, завдяки тому, що агент розміщується безпосередньо на кожному контрольованому комп'ютері, комутовані мережі не накладають обмежень на їх використання.

Ці агенти об'єднують гідності мережевого модуля стеження, що працює в реальному масштабі часу, з тактичними перевагами агента системного рівня. До теперішнього часу про розробки в цій області оголосила тільки компанія Internet Security Systems (ISS), запланувала випуск продукту під назвою Micro Agent до кінця року. Ці мікроагенти будуть доповнювати мережеві і системні модулі стеження ПО виявлення атак RealSecure, створеного тією ж компанією[28].

Нейромережі. Майже всі сучасні підходи до процесу виявлення атак базуються на певній формі аналізу контрольованого простору на основі правил. Під контрольованим простором маються на увазі журнали реєстрації або мережевий трафік. Цей аналіз спирається на набір заздалегідь визначених правил, які створюються адміністратором або самою системою виявлення атак. Експертні системи являють найбільш поширену форму підходів до виявлення атак на основі правил. Експертна система складається з наборів правил, підготовлених фахівцем. На жаль, щоб відповідати постійно мінливих вимог,

такі системи повинні регулярно оновлюватися. Хоча експертні системи пропонують інтелектуальні засоби перегляду даних в журналах реєстрації, необхідні оновлення адміністратор повинен вводити вручну. Якщо оновлення не здійснюватимуться, це призведе до ослаблення можливостей експертної системи. У гіршому випадку знизиться ступінь захищеності всієї мережі, користувачі ж будуть введені в оману щодо її дійсного рівня.

Виявлення атаки, розподіленої в часі або між декількома зловмисниками, для експертної системи важко. Методи мережевих атак постійно вдосконалюються, хакери використовують індивідуальні підходи і стежать за регулярними змінами ПО і апаратних засобів обраних ними жертв. Через великого розмаїття видів атак навіть спеціальні постійні оновлення бази даних правил експертної системи ніколи не забезпечать їх стовідсоткової ідентифікації.

Одним із шляхів подолання цих проблем стало використання нейронних мереж. Нейросеть, проводячи аналіз інформації, дозволяє оцінити, чи узгоджуються отримані нею дані з розпізнаваними характеристиками. В цьому і полягає її відмінність від експертних систем, які визначають відповідність тих характеристик, які вона розглядає, і тих, які закладені в базі даних правил. У той час як ступінь відповідності нейросетевого уявлення може досягати 100%, достовірність вибору повністю залежить від здатності системи до аналізу прикладів (здатності до навчання).

Спочатку нейросеть навчається шляхом правильної ідентифікації попередньо обраних прикладів предметної області. Її реакція аналізується, і система налаштовується таким чином, щоб досягти задовільних результатів. На додаток до первісного періоду навчання нейромережа набирається досвіду в міру того, як вона проводить аналіз даних, пов'язаних з предметною областю. Найбільш важлива перевага нейромереж при виявленні зловживань полягає в їх здатності "вивчати" характеристики умисних атак і ідентифікувати елементи, відмінні від тих, що спостерігалися нею в мережі раніше.

Є два варіанти реалізації нейромереж в системах виявлення атак. Перший включає об'єднання нейромережі з існуючою або видозміненій експертної

системою. Другий підхід передбачає реалізацію нейромережі як окремо стоїть системи виявлення атак. На ринку поки немає комерційних реалізацій ні того ні іншого варіанту. Однак вже відомі науково-дослідні проекти з їх застосуванням - наприклад, використання даних, зібраних вже згаданої системою RealSecure, як вхідні для нейромережі.

### 2.2.2. Системи, що забезпечують виявлення атак на системному рівні

На початку 80-х років, ще до того, як мережі отримали свій розвиток, найбільш поширена практика виявлення атак полягала в перегляді журналів реєстрації на предмет наявності в них подій, які свідчать про підозрілу активність. Сучасні системи виявлення атак системного рівня залишаються потужним інструментом для розуміння вже здійснених атак і визначення відповідних методів для усунення можливостей їх майбутнього застосування. Сучасні IDS системного рівня, як і раніше використовують журнали реєстрації, але вони стали більш автоматизованими і включають складні методи виявлення, засновані на новітніх дослідженнях в області математики. Як правило, IDS системного рівня контролюють систему, події та журнали реєстрації подій безпеки (security log або syslog) в мережах, що працюють під управлінням Windows NT або Unix. Коли будь-якої з цих файлів змінюється, IDS порівнює нові записи з сигнатурами атак, щоб перевірити, чи є відповідність. Якщо така відповідність знайдено, то система посилає адміністратору сигнал тривоги або пускає в хід інші задані механізми реагування[29].

IDS системного рівня постійно розвиваються, поступово включаючи всі нові і нові методи виявлення. Один з таких популярних методів полягає в перевірці контрольних сум ключових системних і виконуваних файлів через регулярні інтервали часу на предмет несанкціонованих змін. Своєчасність реагування безпосередньо пов'язана з частотою опитування. Деякі продукти прослуховують активні порти і повідомляють адміністратора, коли хтось

намагається отримати до них доступ. Такий тип виявлення вносить в операційну середу елементарний рівень виявлення атак на мережевому рівні.

І хоча системи виявлення атак системного рівня не настільки швидкі, як їх аналоги мережевого рівня, вони пропонують переваги, яких не мають останні. До цих переваг можна віднести більш суворий аналіз, пильну увагу до даних про подію на конкретному хості і більш низька вартість впровадження.

Підтверджують успіх або відмова атаки. Оскільки IDS системного рівня використовують журнали реєстрації, які містять дані про події, які дійсно мали місце, то IDS цього класу можуть з високою точністю визначати - чи дійсно атака була успішною чи ні. В цьому відношенні IDS системного рівня забезпечують чудове доповнення до систем виявлення атак мережевого рівня. Таке об'єднання забезпечує раннє попередження за допомогою мережного компонента і "успішність" атаки за допомогою системного компонента.

Контролює діяльність конкретного вузла. IDS системного рівня контролює діяльність користувача, доступ до файлів, зміни прав доступу до файлів, спроби встановлення нових програм і / або спроби отримати доступ до привілейованих сервісів. Наприклад, IDS системного рівня може контролювати всю logon- і logoff-діяльність користувача, а також дії, що виконуються кожним користувачем при підключенні до мережі. Для системи мережевого рівня дуже важко забезпечити такий рівень деталізації подій.

Технологія виявлення атак на системному рівні може також контролювати діяльність, яка зазвичай ведеться тільки адміністратором. Операційні системи реєструють будь-яка подія, при якому додаються, видаляються чи змінюються облікові записи користувачів. IDS системного рівня можуть виявляти відповідну зміну відразу, як тільки воно відбувається. IDS системного рівня можуть також проводити аудит змін політики безпеки, які впливають на те, як системи здійснюють відстеження у своїх журналах реєстрації і т.д[30].

В кінцевому підсумку системи виявлення атак на системному рівні можуть контролювати зміни в ключових системних файлах або виконуваних файлах.

Спроби перезаписати такі файли або інсталювати "троянських коней" можуть бути виявлені і припинені. Системи мережевого рівня іноді упускають такий тип діяльності.

Виявлення атак, які втрачають системи мережевого рівня. IDS системного рівня можуть виявляти атаки, які не можуть бути виявлені засобами мережевого рівня. Наприклад, атаки, що здійснюються з самого атакується сервера, не можуть бути виявлені системами виявлення атак мережевого рівня.

Добре підходить для мереж з шифруванням і коммутацією.Поскольку IDS системного рівня встановлюється на різних хостах мережі підприємства, вона може подолати деякі з проблем, що виникають при експлуатації систем мережевого рівня в мережах з комутацією і шифруванням.

Комутація дозволяє управляти великомасштабними мережами, як кількома невеликими мережевими сегментами. В результаті буває важко визначити найкраще місце для установки IDS мережевого рівня. Іноді можуть допомогти адміністративні порти (managed ports) і порти відображення (mirror ports, span ports) трафіку на комутаторах, але ці методи не завжди застосовні. Виявлення атак на системному рівні забезпечує більш ефективну роботу в комутованих мережах, тому що дозволяє розмістити IDS тільки на тих вузлах, на яких це необхідно.

Певні типи шифрування також представляють проблеми для систем виявлення атак мережевого рівня. Залежно від того, де здійснюється шифрування (канальне або абонентське), IDS мережевого рівня може залишитися "сліпий" до певних атакам. IDS системного рівня не мають цього обмеження. До того ж ОС, і, отже, IDS системного рівня, аналізує розшифрований вхідний трафік.

Виявлення та реагування майже в реальному масштабі часу. Хоча виявлення атак на системному рівні не забезпечує реагування в дійсно реальному масштабі часу, воно, при правильній реалізації, може бути здійснено майже в реальному масштабі. На відміну від застарілих систем, які перевіряють статус і змісту журналів реєстрації через заздалегідь певні інтервали, багато сучасних

IDS системного рівня отримують переривання від ОС, як тільки з'являється новий запис в журналі реєстрації. Ця нова запис може бути оброблена відразу ж, значно зменшуючи час між розпізнаванням атаки і реагуванням на неї. Залишається затримка між моментом записи операційною системою події в журнал реєстрації і моментом розпізнавання її системою виявлення атак, але в багатьох випадках зловмисник може бути виявлений і зупинений перш, ніж завдасть будь-якої шкоди.

Не вимагають додаткових апаратних засобів. Системи виявлення атак на системному рівні встановлюються на існуючу мережеву інфраструктуру, включаючи файлові сервера, Web-сервера і інші використовувані ресурси. Така можливість може зробити IDS системного рівня дуже ефективними за вартістю, тому що вони не вимагають ще одного вузла в мережі, якому необхідно приділяти увагу, здійснювати технічне обслуговування та керувати ним.

Низька ціна. Незважаючи на те, що системи виявлення атак мережевого рівня забезпечують аналіз трафіку всієї мережі, дуже часто вони є досить дорогими. Вартість однієї системи виявлення атак може перевищувати $ 10000. З іншого боку, системи виявлення атак на системному рівні стоять сотні доларів за один агент і можуть купуватися покупцем у разі необхідності контролювати лише деякі вузли підприємства, без контролю мережевих атак.

### 2.2.3. Системи виявлення аномальної поведінки

Датчики-сенсори аномалій ідентифікують незвичайна поведінка, аномалії у функціонуванні окремого об'єкта - труднощі їх застосування на практиці пов'язані з нестабільністю самих об'єктів, що захищаються і взаємодіючих з ними зовнішніх об'єктів. Як об'єкт спостереження може виступати мережу в цілому, окремий комп'ютер, мережева служба (наприклад, FTP-сервер), користувач і т.д. Датчики спрацьовують за умови, що напади відрізняються від "звичайної"

(законної) діяльності. Тут з'являється ще одне слабке місце, яке характерне більшою мірою для конкретних реалізацій, що полягає в некоректності визначення "дистанції" відхилення спостережуваного поведінки від штатного, прийнятого в системі, і визначенні "порога спрацьовування" сенсора спостереження.

Заходи та методи, за допомогою яких традиційно у виявленні аномалії, включають в себе наступні:

✓ порогові значення: спостереження за об'єктом виражаються у вигляді числових інтервалів. Вихід за межі цих інтервалів вважається аномальним поведінкою. Як можна побачити параметрів можуть бути, наприклад, такі: кількість файлів, до яких звертається користувач в даний період часу, число невдалих спроб входу в систему, завантаження центрального процесора і т.п. Пороги можуть бути статичними і динамічними (тобто змінюватися, підлаштовуючись під конкретну систему);

✓ статистичні заходи: рішення про наявність атаки робиться по великій кількості зібраних даних шляхом їх статистичної предобработки; - параметричні: для виявлення атак будується спеціальний "профіль нормальної системи" на основі шаблонів (тобто деякої політики, якої зазвичай повинен дотримуватися даний об'єкт);

✓ непараметричні: тут вже профіль будується на основі спостереження за об'єктом в період навчання;

✓ заходи на основі правил (сигнатур): вони дуже схожі на непараметричні статистичні заходи. В період навчання складається уявлення про нормальному поведінці 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 сенсора-датчику ознак. В сучасних СОА 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 більш небезпечний, ніж помилкове зарахування аномального поведінки до класу атак.

Тому при інсталяції і експлуатації систем такої категорії звичайні користувачі та фахівці стикаються з двома досить нетривіальними завданнями:

✓ побудова профілю об'єкта - це важко формалізується і витратна за часом завдання, що вимагає від фахівця безпеки великої попередньої роботи, високої кваліфікації і досвіду;

✓ визначення граничних значень характеристик поведінки суб'єкта для зниження ймовірності появи одного з двох вищеназваних крайніх випадків.

Зазвичай системи виявлення аномальної активності використовують журнали реєстрації та поточну діяльність користувача в якості джерела даних для аналізу. Переваги систем виявлення атак на основі технології виявлення аномального поведінки можна оцінити таким чином:

✓ системи виявлення аномалій здатні виявляти нові типи атак, сигнатури для яких ще не розроблені;

✓ вони не потребують оновлення сигнатур і правил виявлення атак;

✓ виявлення аномалій генерують інформацію, яка може бути використана в системах виявлення злочинного поведінки.

Недоліками систем на основі технології виявлення аномального поведінки є такі:

✓ системи вимагають тривалого і якісного навчання;

✓ системи генерують багато помилок другого роду;

✓ системи зазвичай занадто повільні в роботі і вимагають великої кількості обчислювальних ресурсів.

Застосування методів статистичного аналізу є найбільш поширеним видом реалізації технології виявлення аномального поведінки. Статистичні датчики збирають різну інформацію про типову поведінку об'єкта і формують її у вигляді

профілю. Профіль в даному випадку - це набір параметрів що характеризують типова поведінка об'єкта. Існує період початкового формування профілю. Профіль формується на основі статистики об'єкта, і для цього можуть застосовуватися стандартні методи математичної статистики, наприклад метод ковзних вікон і метод зважених сум[31].

Після того як профіль сформований, дії об'єкта порівнюються з відповідними параметрами і при виявленні істотних відхилень подається сигнал про початок атаки. Параметри, які включаються в профіль системи, можуть бути віднесені до наступних поширеним групам: - числові параметри (кількість переданих даних по різних протоколах, завантаження центрального процесора, кількість файлів, до яких Ви отримували доступ і т.п.);

- ✓ категоріальні параметри (імена файлів, команди користувача, відкриті порти і т.д.);
- ✓ не вписується в класифікацію нарівні з попередніми типами параметрів.

Профілі також повинні мати механізми динамічного зміни, для того щоб більш повно описувати змінюється поведінка об'єкта. Системи, які застосовують статистичні методи, мають цілу низку переваг:

- ✓ не вимагають постійного оновлення бази сигнатур атак. Це значно полегшує завдання супроводу даних систем;
- ✓ можуть виявляти невідомі атаки, сигнатури для яких ще не написані. Можуть бути своєрідним стримуючим буфером, поки не буде розроблений відповідний шаблон для експертних систем;
- ✓ дозволяють виявляти більш складні атаки, ніж інші методи. Вони можуть виявляти атаки, розподілені в часі або по об'єктам нападу;
- ✓ можуть адаптуватися до зміни поведінки користувача і тому є більш чутливими до спроб вторгнення, ніж люди.

Серед недоліків систем виявлення вторгнень можна відзначити наступні:

- ✓ труднощі завдання порогового значення (вибір цих значень - дуже нетривіальне завдання, яке вимагає глибоких знань контрольованої системи);

- ✓ зловмисник може обдурити систему виявлення атак, і вона сприйме діяльність, відповідну атаку, в якості нормальної через поступової зміни режиму роботи з плином часу і "приручення" системи до нової поведінки;
- ✓ в статистичних методах ймовірність отримання хибних повідомлень про атаку є набагато вищою, ніж при інших методах;
- ✓ статистичні методи не дуже коректно обробляють зміни в діяльності користувача (наприклад, коли менеджер виконує обов'язки підлеглого в критичній ситуації). Цей недолік може становити велику проблему в організаціях, де зміни є частими. В результаті можуть з'явитися як помилкові повідомлення про небезпеку, так і негативні неправдиві повідомлення (пропущені атаки);
- ✓ статистичні методи не здатні виявити атаки з боку суб'єктів, для яких неможливо описати шаблон типової поведінки;
- ✓ системи, побудовані виключно на статистичних методах, не справляються з виявленням атак з боку суб'єктів, які з самого початку виконують несанкціоновані дії. Таким чином, шаблон звичайного поведінки для них буде включати тільки атаки;
- ✓ статистичні методи повинні бути попередньо налаштовані (задані порогові значення для кожного параметра, для кожного користувача); статистичні методи на основі профілю нечутливі до порядку проходження подій.

Проте, існують шляхи вирішення даних проблем, і їх практична реалізація є лише питанням часу. Очевидно, що статистичний метод є чистою реалізацією технології аномального поведінки. Статистичний метод успадковує у технології виявлення аномалій все так необхідні на практиці переваги.

З урахуванням сказаного вище, все системи виявлення вторгнень можна розділити на системи, орієнтовані на пошук:

- ✓ аномалій взаємодії контрольованих об'єктів;
- ✓ сигнатур всіх відомих атак;
- ✓ спотворення еталонної профільної інформації.

Необхідно відзначити, що в даний час практично відсутні системи гібридного типу, а також використовують інформацію розподіленого в часі і просторі характеру. В ході роботи переважної більшості сучасних систем використовується тільки сигнатурний метод розпізнавання атакуючих дій або тільки пошук аномалій в поведінці контрольованої мережі[32].

Ще одним недоліком майже всіх відомих систем є відсутність імітатора атак або будь-якого іншого засобу для перевірки коректності розгорнутої і експлуатованої СОА, який забезпечував би простий і надійний засіб тестування конфігураційних параметрів, використаних в кожній конкретній комп'ютерній мережі.

Даний засіб, за логічним міркувань, має дозволяти імітувати діяльність програмного забезпечення вірусного типу (наприклад, CodeRed, NetSky, Bagle, MSBlast і т.д.), атак на відмову в обслуговуванні (наприклад, SYN-шторм або атаку типу fraggle), атак з метою підвищення привілеїв облікового запису (як приклад, можна навести уразливості в мережевих службах MS SQL Server 2000, MS Internet Information Service 5.0), атаку з метою перенаправлення трафіку і нав'язування помилкових даних (підміна ARP і нав'язування DNS служби). При цьому бажано, щоб програмний засіб мало можливість генерувати атаки розподіленого характеру.

Наприклад, архітектура деяких типів імітаторів СОА складається з набору агентів різних типів, спеціалізованих для вирішення підзадач виявлення вторгнень. Агенти розміщуються на окремих комп'ютерах системи. У даній архітектурі в явному вигляді відсутня "центр управління" сімейством агентів - залежно від ситуації, що склалася провідним може ставати будь-який з агентів, який ініціює або реалізує функції кооперації та управління. У разі необхідності агенти можуть як клонувати (здійснювати своє копіювання в мережевий і локальному середовищі), так і припиняти своє функціонування, що дуже точно передає характер більшості комп'ютерних атак. Залежно від ситуації (виду і кількості атак на комп'ютерні мережі, наявності обчислювальних ресурсів для виконання функцій захисту), може знадобитися генерація кількох примірників

агентів кожного класу. Передбачається, що архітектура системи може адаптуватися до реконфігурації мережі, зміни трафіку і нових видів атак, використовуючи накопичений досвід.

Архітектура багатоагентній системи є цікавою і перспективною для подальшого розгляду. Однак, на жаль, у вітчизняних роботах немає вказівок на використовувані або розроблені алгоритми виявлення атак. Крім того, поточні версії відомих імітаторів не функціонують в реальному режимі часу (оскільки цього не дозволяє робити обраний базовий інструментарій).

Взагалі кажучи, відсутність імітаторів атак для оцінки ефективності СОА не є основною проблемою даного напрямку. Реальними недоліками існуючих систем виявлення комп'ютерних атак є примітивність простого сігнартурного пошуку, мала ефективність при виявленні розподілених за часом і місцем складних атак, недостатня інтеграція інформації на рівні хоста і мережі для виявлення комбінованих атак і несанкціонованих проникнень.

Серед експлуатаційних недоліків сучасних СОА можна відзначити велику кількість обчислювальних операцій для простого поділу приналежності події на "свій-чужий" і неможливість обробки всієї інформації, що надходить в реальному режимі часу на звичайних персональних комп'ютерах. Швидкість обробки мережевого чи іншого трафіку подій часто повільніше реального часу в 1.5-2 рази. А в деяких системах аналіз і зовсім відбувається у відкладеному режимі. Це означає, що реалізація атаки на захищаються інформаційні та обчислювальні ресурси не буде помічена вчасно і вже тим більше не буде відображена за допомогою наявних засобів захисту. В даному режимі СОА може бути використана в кращому випадку як засіб журналирования всіх етапів атаки і подальшої криміналістичної експертизи.

Більшість сучасних СОА спочатку не розробляються портіруемость, тобто їх код нестерпний на різні операційні системи і довільні апаратно-обчислювальні платформи. Робота на декількох операційних системах для більшості західних продуктів і майже всіх вітчизняних СОА (як експериментальних, так і комерційно адаптованих) є неможливою. З огляду на, що СОА не

використовують переваги розробки і оптимізації коду для обраних операційних систем і апаратних платформ, це є їх одним з найбільш істотних недоліків. Крім того, ні в одній програмній або апаратно-програмної системі не передбачений режим гарячої заміни, що дозволяє в разі виведення з ладу основного комплексу оперативно ввести в роботу комплекс гарячого резервування і відновити знищений рубіж оборони мережевого периметра. Незважаючи на це, є і позитивний момент у розвитку СОА, який полягає в прагненні розробників інтегрувати свої системи з існуючими засобами захисту (міжмережевими екранами, блокаторами каналів, QoS-диспетчерами) [33].

Системи пошуку аномалій ідентифікують незвичайна поведінка (аномалії) у функціонуванні контрольованого об'єкта. Як об'єкт спостереження може виступати мережу в цілому, окремий комп'ютер, мережева служба (наприклад, файловий сервер FTP), користувач і т.д. Сигналізація СОА спрацьовує за умови, що дії, вчинені під час нападу, відрізняються від звичайної (законної) діяльності користувачів і комп'ютерів. Заходи та методи, за допомогою яких традиційно у виявленні аномалії, включають використання:

- ✓ порогових значень (спостереження за об'єктом виражаються у вигляді числових інтервалів);
- ✓ статистичних заходів (рішення про наявність атаки робиться по великій кількості зібраних даних);
- ✓ профілів (для виявлення атак на основі заданої політики безпеки будується спеціальний список легітимних дій - профіль нормальної системи);
- ✓ нейронних мереж, генетичних алгоритмів.

Відмінною рисою даних систем є необхідність їх навчання на "стандартне" поведінку контрольованого об'єкта (наприклад, корпоративної локальної мережі). Це ж є і основним недоліком всіх подібних методів, оскільки час навчання становить досить великий проміжок часу і весь цей час на контрольовані об'єкти не повинно бути вироблено жодної атаки.

У разі, якщо захищається интрасеть на етапі навчання відключається від інших мереж, то на етапі експлуатації система захисту буде класифікувати всі спроби легального взаємодії з зовнішніми мережами як атаки.

У разі створення СОА, що використовує профільні системи слід враховувати, що за різними дослідженнями, як мінімум, 15% користувачів комп'ютерних мереж не підлягають профілізації взагалі, а ще стільки ж мають тенденцію до швидкого зміни поведінки протягом обмеженого часу. Статичність існуючих профільних систем дозволяє говорити про це як про один з основних недоліків, явно заважають експлуатації СОА на базі контролю профілів користувачів.

У разі динамічної підстроювання і модифікації профілів необхідно знайти компроміс між кількістю ознак профілювання (чим їх менше, тим грубіше оцінюється поведінка контрольованого об'єкта) і швидкістю обробки (швидкість оцінки аномальність поведінки за профілем є експоненціальною функцією від кількості досліджуваних ознак). Крім того, велике число конфігураційних параметрів в цьому випадку неминуче вимагатимуть від адміністратора системи захисту високої кваліфікації в досить спеціалізованої області виявлення атак.

Такий підхід реалізований в деяких вітчизняних СОА. Дані розробки відносяться до класу системних СОА, їх екземпляри повинні

експлуатуватися на кожному інформаційному ресурсі, який потребує захисту. Особливістю однієї з даних систем є використання процедур нечіткого пошуку. Для кожного з користувачів створюється свій індивідуальний профіль, при цьому поведінка, характерна для одного з користувачів, може вважатися незвичайним для іншого, і навпаки. Оскільки такі профілі важко формалізувати, вони створюються на основі прикладів нормальної роботи того чи іншого користувача.

Як показники активності користувачів обрані запуск і завершення додатків, а також перехід від одного активного застосування до іншого. Профілі створюються на основі прикладів нормальної роботи того чи іншого користувача. Для уявлення профілів розробниками були обрані нейронні мережі.

За даними розробників, тестування системи показало, що ймовірність помилки першого роду становить 5-15%, помилки другого роду - 10-20%. При цьому до половини тестової вибірки складали вектора користувачів, які не брали участі в побудові навчальної вибірки, що говорить про хорошу навчальної спроможності нейронної мережі.

Більшість розглянутих недоліків сучасних СОА є недоліками, з якими може зіткнутися користувач в реальних комп'ютерних мережах. Велика частина зауважень про недоліки і ступеня ефективності розроблюваних методів і засобів відбувається з практики використання СОА в реальних корпоративних інтрамережі.

Існуючі підходи до вирішення завдань виявлення вторгнень часто відрізняються не тільки реалізацією методів виявлення, а й своєю архітектурою, рівнем деталізації та типами виявлення вторгнень. Природно, що у кожної системи є свої переваги і недоліки. Незважаючи на постійний розвиток застосовуваних при розробці СОА технологій, про легкість розгортання, експлуатації та модифікації систем виявлення вторгнень доведеться забути, всі існуючі розробки мають тенденцію лише до ускладнення. Технології злому постійно вдосконалюються, атаки стають комбінованими і поширюються з дуже великою швидкістю, тому до сучасних СОА висуваються дедалі жорсткіші і сильні вимоги. Очевидно, що для відповідності своєму завданню СОА повинні реалізовувати дві основні розглянуті вище технології, в тій чи іншій мірі взаємодоповнюють одне одного[34].

Якщо розглядати СОА з точки зору методів виявлення атак, то, очевидно, це повинні бути системи, що включають в себе безліч модулів, що реалізують різні підходи - с урахуванням різних типових сегментів захищаються мереж. Перед більшістю СОА вже стоїть проблема підвищення швидкодії, так як сучасні комп'ютерні мережі стають все більш швидкими. У міру впровадження СОА в експлуатацію підвищуються вимоги до масштабованості і простоті управління системами виявлення. В майбутньому СОА, мабуть, розділяться на дві категорії, які будуть використовувати різні підходи для малих корпоративних мереж і для

великих, складних за своєю топології комп'ютерних интрасетей територіально розподілених корпорацій.

Таким чином, вимоги та особливості сучасних комп'ютерних мереж, такі як підвищення надійності мереж, підвищення мобільності, ієрархічна структура мереж, різні вимоги до безпеки - все це накладає відбиток на технології та підходи, які повинні бути вже сьогодні реалізовані в системах виявлення атак.

## 2.3. Огляд програмних продуктів, що відносяться до класу систем моніторингу та виявлення атак

Аналіз трафіку є процесом, важливість якого відома будь-якому IT-професіоналу, не залежно від того, чи працює він в невеликій компанії або у великій корпорації. Адже виявлення і виправлення проблем з мережею - це справжнє мистецтво, яке безпосередньо залежить як від інстинкту самого фахівця, так і від глибини і якості оперованих їм даних. І аналізатор трафіку є саме тим інструментом, який ці дані надає вам. Обраний з розумом рішення для аналізу мережевого трафіку може не тільки допомогти вам з'ясувати, як пакети відправляються, приймаються і наскільки сохранно передаються по вашій мережі, але і дозволить зробити набагато-набагато більше!

Зараз на ринку представлена велика кількість варіацій програмного забезпечення для аналізу мережевого трафіку. Причому деякі з них здатні викликати ностальгічні спогади у фахівців «старої школи»; вони використовують термінальний шрифт і інтерфейс командного рядка, і на перший погляд здаються складними у використанні. Інші рішення, навпаки, - виділяються простотою установки і орієнтовані на аудиторію з візуальним сприйняттям (вони буквально перенасичені різними графіками). Ціновий діапазон цих рішень також має велике значення відрізняється - від безкоштовних до рішень з вельми дорогий корпоративної ліцензією.

Для того, щоб ви в залежності від своїх задач і переваг змогли вибрати краще рішення для аналізу мережевого трафіку, представляємо вам список з найбільш цікавих з доступних зараз на ринку програмних продуктів для аналізу трафіку, а також короткий огляд вбудованої в них функціональності для вилучення, обробки і візуального надання різної мережевої інформації. Частина цих функцій у всіх наведених в цьому огляді рішень для аналізу мережевого трафіку схожа - вони дозволяють з тим чи іншим рівнем деталізації побачити відправлені і отримані мережеві пакети, - але практично всі з них мають деякі характерні особливості, які роблять їх унікальними при використанні в певних ситуаціях або мережевих середовищах. Зрештою, до аналізу мережевого трафіку ми вдаємося тоді, коли у нас з'явилася мережева проблема, але ми не можемо швидко звести її до певної машині, влаштуванню або протоколу, і нам доводиться проводити більш глибокий пошук. Ми допоможемо вам вибрати найбільш підходяще для цих цілей програмне рішення для аналізу трафіку[35].

SolarWinds Network Bandwidth Analyzer.

Дане рішення позиціонується виробником як програмний пакет з двох продуктів - Network Performance Monitor (базове рішення) і NetFlow Traffic Analyzer (модульне розширення). Як заявляється, вони мають схожі, але все ж відрізняються функціональні можливості для аналізу мережевого трафіку, що доповнюють один одного при спільному використанні відразу двох продуктів.

Network Performance Monitor, як випливає з назви, здійснює моніторинг продуктивності мережі і стане для вас привабливим вибором, якщо ви хочете отримати загальне уявлення про те, що відбувається у вашій мережі. Купуючи це рішення, ви платите за можливість контролювати загальну працездатність вашої мережі: спираючись на величезну кількість статистичних даних, таких як швидкість і надійність передачі даних і пакетів, в більшості випадків ви зможете швидко ідентифікувати несправність в роботі вашої мережі. А просунуті інтелектуальні можливості програми по виявленню потенційних проблем і широкі можливості по візуальному представленню результатів у вигляді таблиць

і графіків з чіткими попередженнями про можливі проблеми, ще більше полегшать цю роботу.

Модульне розширення NetFlow Traffic Analyzer більше сконцентровано на аналізі самого трафіку. У той час, як функціональність базового програмного рішення Network Performance Monitor більше призначена для отримання загального уявлення про продуктивність мережі, в NetFlow Traffic Analyzer фокус уваги спрямований на більш детальний аналіз процесів, що відбуваються в мережі. Зокрема, ця частина програмного пакета дозволить проаналізувати перевантаження або аномальні скачки смуги пропускання і надасть статистику, відсортовану по користувачах, протоколів або додатків. Зверніть увагу, що дана програма доступна тільки для середовища Windows.

Wireshark.

WireShark є відносно новим інструментом у великій родині рішень для мережевої діагностики, але за цей час він вже встиг завоювати собі визнання і повагу з боку IT-професіоналів. З аналізом трафіку WireShark справляється чудово, прекрасно виконуючи для вас свою роботу. Розробники змогли знайти золоту середину між вихідними даними і візуальним представленням цих даних, тому в WireShark ви не знайдете перекосів в ту чи іншу сторону, яким грішать більшість інших рішень для аналізу мережевого трафіку. WireShark простий, сумісний і портативний. Використовуючи WireShark, ви отримуєте саме те, що очікуєте, і отримуєте це швидко.

WireShark має прекрасний користувальницький інтерфейс, безліч опцій для фільтрації і сортування, і, що багато хто з нас зможуть оцінити по достоїнству, аналіз трафіку WireShark прекрасно працює з будь-яким з трьох найпопулярніших сімейств операційних систем - * NIX, Windows і macOS. Додайте до всього вищепереліченого той факт, що WireShark - програмний продукт з відкритим вихідним кодом і розповсюджується безкоштовно, і ви отримаєте прекрасний інструмент для проведення швидкої діагностики вашої мережі.

Tcpdump.

Аналізатор трафіку tcpdump виглядає як якийсь древній інструмент, і, якщо вже бути до кінця відвертими, з точки зору функціональності працює він також. Незважаючи на те, що зі своєю роботою він справляється і справляється добре, причому використовуючи для цього мінімум системних ресурсів, наскільки це взагалі можливо, багатьом сучасним фахівцям буде складно розібратися у величезній кількості «сухих» таблиць з даними. Але бувають в житті ситуації, коли використання настільки обрізаних і невибагливих до ресурсів рішень може бути корисно. У деяких середовищах або на ледве працюють ПК мінімалізм може виявитися єдиним прийнятним варіантом.

Спочатку програмне рішення tcpdump розроблено для середовища * NIX, але на даний момент він також працює з декількома портами Windows. Він має всю базовою функціональністю, яку ви очікуєте побачити в будь-якому аналізаторі трафіку - захоплення, запис і т.д., - але вимагати чогось більшого від нього не варто.

EtherApe.

За своїми функціональними можливостями EtherApe багато в чому наближається до WireShark, і він також є програмним забезпеченням з відкритим вихідним кодом і розповсюджується безкоштовно. Однак те, чим він дійсно виділяється на тлі інших рішень - це орієнтація на графіку. І якщо ви, наприклад, результати аналізу трафіку WireShark переглядаєте в класичному цифровому вигляді, то мережевий трафік EtherApe відображається за допомогою просунутого графічного інтерфейсу, де кожна вершина графа являє собою окремий хост, розміри вершин і ребер вказують на розмір мережевого трафіку, а кольором відзначаються різні протоколи. Для тих людей, хто віддає перевагу візуальному сприйняттю статистичної інформації, аналізатор EtherApe може стати найкращим вибором. Доступний для середовищ * NIX і macOS

Cain and Abe.

У даного програмного забезпечення з вельми цікавим назвою можливість аналізу трафіку є скоріше допоміжною функцією, ніж основний. Якщо ваші

завдання виходять далеко за межі простого аналізу трафіку, то вам варто звернути увагу на цей інструмент. З його допомогою ви можете відновлювати паролі для ОС Windows, виробляти атаки для отримання втрачених облікових даних, вивчати дані VoIP в мережі, аналізувати маршрутизацію пакетів і багато іншого. Це дійсно потужний інструментарій для системного адміністратора з широкими повноваженнями. Працює тільки в середовищі Windows.

NetworkMiner.

Рішення NetworkMiner - ще одне програмне рішення, чия функціональність виходить за рамки звичайного аналізу трафіку. У той час як інші аналізатори трафіку зосереджують свою увагу на відправку та отримання пакетів, NetworkMiner стежить за тими, хто безпосередньо здійснює цю відправку та отримання. Цей інструмент більше підходить для виявлення проблемних комп'ютерів або користувачів, ніж для проведення загальної діагностики або моніторингу мережі як такої. NetworkMiner розроблений для ОС Windows.

Таблиця 2.1.

Порівняльна характеристика розглянутих програмних засобів

| Назва П/З | Модульність | Фільтрація т сортування | Підтримка системи *NIX | Підтримка системи Windows | Підтримка системи MacOS |
|---|---|---|---|---|---|
| Solarwinds | Так | Так | Так | Так | Ні |
| Wireshark | Так | Так | Так | Так | Ні |
| Tcpdump | Ні | Ні | Ні | Так | Ні |
| Etherape | Так | Ні | Так | Так | Ні |
| Kain and ab | Ні | Так | Так | Так | Так |
| NetworkMi er | Ні | Так | Ні | Так | Так |

В таблиці 2.1. наведено порівняльну характеристику описаних вище програмних засобів за на ступними параметрами:

- ✓ модульність програми;

- ✓ фільтрація та сортування;
- ✓ підтримка різних операційних систем.

Програмні засоби Solarwinds та Wireshark є найоптимальнішими рішеннями для користувачів систем *NIX та Windows, вони мають модульну структуру та підтримують можливість фільтрації та сортування отриманих в ході роботи даних, в той же час, для користувачів системи MacOS програмний засіб Kain and Abe буде у пріоритеті у порівнянні з NetworkMiner, оскільки модульність програми надає більшу кількість можливостей з точки зору гнучкості та цілеспрямованого використання окремих функцій засобу.

Таблиця 2.2.

Порівняльна характеристика розглянутих програмних засобів

| Назва П/З | Підтримувані стандарти | Моніторинг бездротових мереж | Виявлення прихованих мереж | Виявлення загроз |
|---|---|---|---|---|
| Solarwinds | 802.11b, 802.11 802.11n | Так | Так | Так |
| Wireshark | 802.11b, 802.11ac, 802.11a, 802.11g | Так | Так | Так |
| Tcpdump | 802.11b | Так | Ні | Ні |
| Etherape | 802.11a, 802.11ac, 802.11 | Так | Так | Так |
| Kain and abe | 802.11n, 802.11g | Так | Так | Так |
| NetworkMiner | 802.11x | Так | Ні | Так |

В таблиці наведено порівняльну характеристику на основі наступних критеріїв:

- ✓ підтримувані стандарти безротових мереж;
- ✓ поніторинг бездротових мереж;
- ✓ виявлення прихованих мереж;
- ✓ виявлення загроз.

З цієї порівняльної характеристики можна зробити висновок, що програмні засоби Solarwinds, Wireshark та Ethertape надають користувачам найбільший спектр можливостей у кількості підтримуваних стандартів. Усі програми можуть

використовуватись як системи моніторингу мережевого трафіку, зокрема трафіку бездротових мереж, проте не всі мають змогу виявляти приховані мережі та загрози інформаційній безпеці.

**Висновки до розділу**

У другому розділі дипломної роботи було досліджено та описано існуючі методи моніторингу та виявлення атак, проведено класифікацію існуючих систем виявлення атак, зокрема систем виявлення на мережному та системному рівнях та систем, що виявляють аномальну поведінку.

Системи моніторингу мережі можна розділити на ті, що відстежують продуктивність мережі і сигналізують при перевантаженні каналів, а також на ті, що виробляють моніторинг мережі з метою пошуку збоїв і інших проблем, пов'язаних з працездатністю серверного обладнання та інших систем.

до функцій систем моніторингу мережі можна віднести:

- ✓ Можливість складання топології мережі в автоматичному режимі.
- ✓ Постійний моніторинг мережі.
- ✓ Можливість своєчасного оповіщення осіб, відповідальних за адміністрування інфраструктури.
- ✓ Побудова ретроспективи працездатності мережевої інфраструктури.
- ✓ Складання різних звітів.

Для здійснення моніторингу складної корпоративної мережі або розподіленої інфраструктури необхідне застосування комплексної платформи, яка дозволила б переглядати як фізичний, так і віртуальні сервери, WAN-з'єднання, програмну і мережеву інфраструктуру, хмарні сервіси, мережеві додатки, а також мобільні пристрої, які підключаються до мережі .

Проведений огляд та порівняльна характеристика існуючих програмних продуктів, що відносятся до класу систем моніторингу та виявлення атак, дали

змогу встановити необхідні вимоги до розроблюваного програмного засобу, який матиме переваги існючих і не матиме їх недоліків.

# РОЗДІЛ 3. РОЗРОБКА СИСТЕМИ МОНІТОРИНГУ МЕРЕЖЕВОГО ТРАФІКУ ДЛЯ ВИЯВЛЕННЯ АТАК

## 3.1. Розробка алгоритму роботи програмного забезпечення

Фільтрації і маршрутизація пакетів на основі політик, має ряд недоліків, причому вони стають більш відчутними при посиленні вимог до безпеки мережі, що захищається. Відзначимо основні з них:

складність сприйняття правил (в деяких випадках сукупність правил може стати некерованою);

неможливість повного тестування правил (призводить до незахищеності мережі від б не протестували атак, в результаті адміністратору важко визначити, скомпрометований чи маршрутизатор чи ні).

Насправді причин виникнення помилок маршрутизації і фільтрації набагато ширше і підлягає окремому розгляду, проте спосіб їх виявлення часто однаковий: адміністратор порівнює фактичний стан мережі з очікуваним, шукає відмінності і з'ясовує, за яких обставин вони могли виникнути. У більшості випадків це здійснюється вручну. Спеціаліст по маршрутизації самостійно реєструється на окремих пристроях маршрутизації і перевіряє інформацію про маршрути і конфігурацію самих пристроїв, намагаючись виявити причини помилок і невідповідності.

Тим часом набагато ефективніше для пошуку причини використовувати засоби моніторингу та аудиту, які регулярно і паралельно на всіх обстежуваних пристроях можуть робити моментальні знімки за допомогою інструменту для аналізу маршрутів, а також збирати всю необхідну інформацію, на всіх пристроях маршрутизації. Крім цього інструменти перевіряють дані про маршрутизації на предмет можливих помилок, автоматично виконуючи ті ж самі кроки, які зробив би фахівець. Після аналізу, що займає всього кілька секунд, програмне забезпечення відображає можливі джерела помилок при

маршрутизації, адміністратору в свою чергу досить лише вивчити їх, щоб швидко локалізувати проблему. Крім того, використовуючи порівнянні двох знімків, можна визначити, які шляхи були зради, ким і чому в результаті виникла помилка.

система моніторингу та аудиту повинна розпізнавати навіть проміжні зміни в налаштування окремих пристроїв і відразу ж повідомляти про це адміністратора. Наприклад, можливо, що застосування асиметричних маршрутних шляхів необхідно в даний момент часу при конкретних умовах, але якщо їх число постійно змінюється, отже в мережі є аномалія, і це необхідно перевірити.

Наведені вимоги можна формалізувати наступним чином. При реалізації функцій моніторингу та аудиту параметрів роботи систем фільтрації і маршрутизації трафіку засіб, що відповідає за виконання цих функцій, має забезпечувати:

1) формування, перегляд, редагування, активацію (деактивацію) і видалення завдань на збір значень параметрів роботи (виконання \ невиконання правил) систем фільтрації і маршрутизації пакетів інформації;

2) система повинна здійснювати ідентифікацію будь-які зміни (видалення, зміна або додавання нових правил) ключових елементів в конфігурації політик мережевих пристроїв, а так само виявляти такі типи аномалій систем фільтрації і маршрутизації пакетів інформації: перетин, узагальнення, затінення і надмірність. Конфігурація кожної системи повинна перевірятися за затвердженою базі даних еталонних образів для перевірки будь-яких змін в настройках безпеки, які могли б вплинути на безпеку;

3) створення звітів (у вигляді журналів) за параметрами роботи систем фільтрації і маршрутизації пакетів інформації. Звіт повинен містити час і дату виявлення аномалії, найменування об'єкта моніторингу, тип виявленої аномалії, джерело виявленої аномалії, короткий опис її розташування;

4) видачу аварійних повідомлень за параметрами роботи і конфігурацій систем фільтрації і маршрутизації пакетів інформації, якщо отримані значення відрізняються від встановлених.

Таким чином для повноцінного контролю за процесами фільтрації і маршрутизації, засіб забезпечує ці функції має надавати такі можливості:

- ✓ моніторинг зміни конфігурації правил фільтрації і маршрутизації;
- ✓ моніторинг протиріч (валідація) правил фільтрації і маршрутизації;
- ✓ видача аварійних повідомлень з короткою інформацією про виявлені аномалії;
- ✓ ведення журналу звітів;

Застосування методу функціональної декомпозиції дозволило виділити в таблицю складові частини, характерні для описаної системи моніторингу та аудиту.

Таблиця 3.1.

Складові частини системи моніторингу

| | |
|---|---|
| Підсистема збору даних | Здійснює із заданою регулярністю опитування об'єктів, що підлягають моніторингу, для отримання досліджуваних значень Може також включати в себе первинний аналіз отриманих даних з метою, кваліфікації отриманих значень як нормальних, які потребують втручання оператора або критичних. |
| Підсистема зберігання | Відповідає за накопичення, зберігання, архівацію даних про результати перевірок. Включає компоненти для роботи з базами даних (БД) або іншими репозиторіями, програмні засоби зменшення об'єму інформації |
| Підсистема аналізу дани | Включає компоненти, що виробляють дослідження даних, накопичених системою, збір статистики, вироблення еталонних значень і порівняння з ними різних станів спостерігається системи, верифікацію правил маршрутизації і фільтрації |

| | |
|---|---|
| Підсистема оповіщення | Відповідає за повідомлення осіб, відповідальних за функціонування об'єктів, що перевіряються про нештатні ситуації і інших значимі події, що виникають в системі. |
| Підсистема виведення | Відповідає за надання інформації про роботу системи і результатів перевірок у вигляді, зручному для сприйняття користувачем. Для взаємодії з кінцевим користувачем, безумовно, необхідний розвинений інтерфейс, що надає зручну навігацію між різними типами звітів і зведень про стан об'єктів моніторингу. |

Эти подсистемы ориентированы на оперативный мониторинг, направленный на оценку текущей работоспособности и немедленную реакцию на разнообразные внештатные ситуации работы систем маршрутизации и фильтрации.

Можна стверджувати, що математичного моделювання, для наведеного набору модулів, вимагає тільки та частина, функції якої зводяться до аналізу і перевірки формальних специфікацій. Відомі різні загальні підходи, але їх застосовність до верифікації правил фільтрації і маршрутизації обмежена, в наслідок чого існуючих засобів мережевого моніторингу та управління маршрутизацією або фільтрацією, які відповідають всім поставленим в даному дослідженні вимогам не виявлено.

Слід зазначити, що аномалії виникають в правилах фільтрації і маршрутизації легко піддаються математичної формалізації, що стало одним з вирішальних факторів, що вплинули на результат ретельного аналізу, в ході якого був зроблений наступний висновок: для даної роботи найбільш підходящим представляється сигнатурний метод верифікації правил. Цей підхід передбачає структурування і подальший аналіз зібраної про конфігураціях політик інформації. Т.ч. основною перевагою даного підходу є поєднання простоти програмної реалізації з максимальною точністю виявлення аномалій.

Для реалізації обраного методу було прийнято рішення покласти в основу аудиту правил фільтрації і маршрутизації спосіб виявлення аномалій заснований на складанні і наступному порівнянні поточних значень об'єктів моніторингу з контрольними. Формалізуємо даний прийом наступним чином.

Нехай існує така безліч, елементи якого описують стан об'єкта моніторингу. Назвемо його профілем об'єкта і позначимо як П. При цьому виділяють два види профілю:

1) контрольний профіль: даний профіль формується при тестовому проведенні моніторингу системою моніторингу та аудиту або задається вручну, уповноваженим на те фахівцем, і характеризує стан контрольованого об'єкта.

2) поточний профіль: даний профіль створюється кожен раз при проведенні моніторингу стану КС.

Програмний комплекс моніторингу та аудиту правил фільтрації і маршрутизації відповідно до що висуваються до нього вимогам повинен передбачає два типи аудиту: цілісності конфігурацій і протиріч правил конфігурацій, які легко формалізувати у вигляді блок-схем:

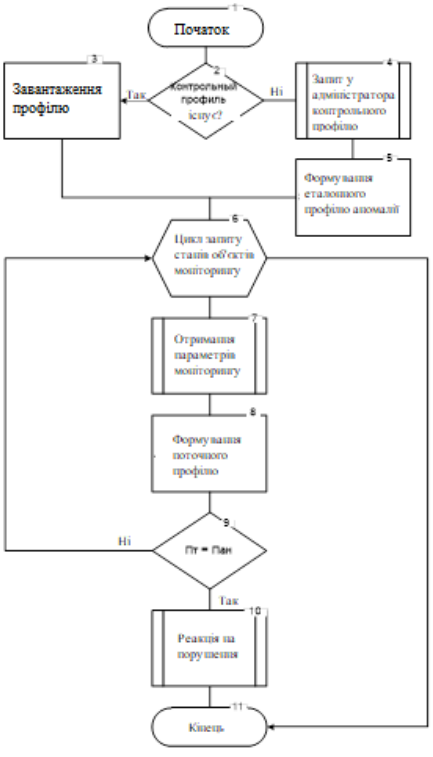


Рис. 3.1.Блок-схема роботи програми-виявлювача загроз

### 3.2. Розробка інтерфейсної частини програми

Сучасне підприємство - це безліч взаємодіючих процесів і виробництв, цехи, адміністративні будівлі, а часто і віддалені ділянки. Питанням першорядної важливості є управління і контроль безлічі параметрів. Для оперативного управління виробничими процесами необхідна автоматизація. А для роботи систем управління необхідна надійна інфраструктура.

Підприємство здійснює збір інформації з механізмів спеціальними датчиками. Далі всю цю інформацію потрібно відправити в заводоуправління для обробки, аналізу і прийняття рішень. Як і на будь-якому промисловому підприємстві, кабельні лінії зв'язку можуть бути пошкоджені або вийти з ладу через несприятливі умов, а в окремих випадках їх прокладка взагалі неможлива. Бездротові технології вільні від цих недоліків і можуть бути застосовані для вирішення завдань організації каналів зв'язку, попутно вирішуючи й інші завдання.

Бездротова передача даних в даний час переживає своєрідний бум. А на тлі активного розвитку мереж супермаркетів, великих медичних центрів, виробничих об'єднань, де на частини підприємств відсутні розгалужені кабельні інфраструктури, організації різних часових інсталяцій - на кшталт мереж на промислових виставках і семінарах, використання бездротової передачі даних стає найбільш актуальним.

У Україні бездротові мережі часто виявляються єдиним засобом організації корпоративних мереж або забезпечення доступу в Internet. Досить велику область бездротової передачі даних можна розділити на три підобласті: мобільний зв'язок, передача даних усередині будівель і між будівлями. Ця класифікація досить умовна, проте, вона відображає основні види завдань, що вирішуються засобами бездротового зв'язку. Технічні рішення, що застосовуються в цих областях, значно відрізняються один від одного.

Мобільні системи передачі даних поширені на Заході дуже широко, і, в першу чергу, до них відносяться стільникові мережі з комутацією пакетів і комутацією каналів. Всі вони забезпечують передачу даних на досить низьких швидкостях (як правило, не вище 19,2 кбіт / с) і розраховані в основному на індивідуальних користувачів.

У Україні ж, навпаки, бездротові технології передачі даних використовуються переважно поза будівлями. І головним чином, вони потрібні для організації інформаційного обміну на порівняно великій відстані. Пояснюється це, по-перше, відсутністю розгалуженої кабельної інфраструктури; а по-друге, низькою щільністю населення і частим відсутністю взагалі будь-якої інфраструктури.

У ряді великих міст Україні вже розгорнуті опорні мережі з бездротовим доступом. Вони, по-перше, розширюють можливості використання великих інформаційних ресурсів і Internet, а по-друге, дозволяють організовувати корпоративні мережі приблизно так само, як це робиться за допомогою кабельних мереж. У тих містах (а таких поки більшість), де немає міських опорних мереж, організація може створити свою власну бездротову мережу, об'єднавши радіоміст два віддалені один від одного локальні мережі.

Для безперешкодного функціонування підприємства, його мережі мають бути захищеними від загроз, вторгнень та має бути присутня можливість моніторингу мережевого трафіку. Для вирішення цієї проблеми, працівники служби безпеки підприємства мають впровадити систему моніторингу мережевого трафіку, яка матиме можливість аналізувати трафік на мережевому рівні, «прослуховувати» трафік за допомогою майже будь-яких бездротових мережевих адапторів, що використовують драйвери Airo, HostAP, Wlan-NG и Orinoco.

Така система також повинна мати простий інтерфейс.

Проектування - це набагато більше, ніж просто компонування, організація і навіть редагування; проектувати - значить надавати цінність і сенс, вносити

ясність, спрощувати і пояснювати, реформувати, надавати лиск, привертати увагу, переконувати і навіть, можливо, розважати.

Головне завдання - ясність. Ясність - це перша і найголовніша задача будь-якого інтерфейсу. Щоб інтерфейс ефективно допомагав людям домагатися своїх цілей, він повинен мати наступні характеристики.

По-перше, він повинен бути впізнаваним, а його призначення - очевидним для користувача.

По-друге, люди повинні розуміти, з чим вони взаємодіють через інтерфейс.

Нарешті, процес взаємодії з інтерфейсом повинен бути передбачуваним. В інтерфейс можна внести якусь загадковість або елементи гри, але ось плутанини бути не повинно.

Ясність народжує в користувачів впевненість і готовність продовжувати роботу з інтерфейсом. Сто зрозумілих екранів краще, ніж один безладний.

Ключове призначення інтерфейсів - взаємодія

Інтерфейси існують, щоб люди могли взаємодіяти з нашим світом. Через інтерфейс ми можемо прояснити, проілюструвати, дати можливість, показати взаємозв'язок, об'єднати людей або розділити, управляти очікуваннями та давати доступ до послуг.

Інтерфейс розробленої програми моніторингу мережевого трафіку був розроблений на основі інтерфейсу системної консолі. Він є простим та зрозумілим навіть для починаючих мережевих адміністраторів. Увесь функціонал, який має програмний засіб і з яким користувач може взаємодіяти має відображувальну частину, мовою програми було обрано англійську.

Після запуску програми, відкривається початкове вікно, яке зображено на рисунку.

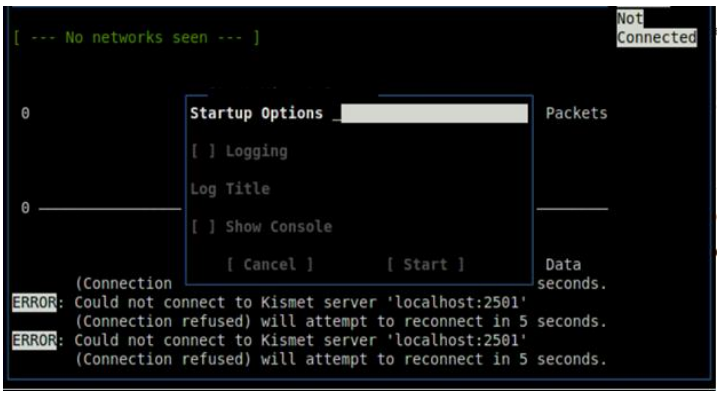


Рис. 3.2. Стартове вікно програми

### 3.3. Опис та тестування розробленого програмного забезпечення

Розробка програмного продукту суттєво залежить від операційної системи, встановленої на апаратному забезпеченні. В даному випадку було обрано операційну систему Windows 10 Professional. Windows 10 — операційна система від компанії Microsoft для персональних комп'ютерів, включаючи домашні та офісні системи, ноутбуків, планшетів [41]. Windows 10 Pro призначена для використання у більш професійних цілях. Вона підтримує всі можливості базової версії Windows 10 і додатково забезпечує підтримку шифрування, віртуалізації, розширені можливості управління комп'ютером та роботи з доменами.

Для розробки програмного модуля було використано Visual Studio Code – редактор вихідного коду, розроблений Microsoft для Windows, Linux і macOS. Він підтримує ряд мов програмування, підсвічування синтаксису, технологію автодоповнення Microsoft, рефакторинг, налагодження, навігацію по коду, підтримку розподіленої системи управління версіями та інші можливості. Багато можливостей Visual Studio Code не доступні через графічний інтерфейс, найчастіше вони використовуються через палітру команд або JSON файли (наприклад, призначені для користувача налаштування). Палітра команд представляє собою вигляд командного рядка, який викликається поєднанням клавіш.

Java є об'єктно-орієнтованою мовою, відноситься до мов програмування з сильною типізацією. Творці реалізували принцип WORA: write once, run anywhere або «пиши один раз, запускай скрізь». Це означає, що написане на Java додаток можна запустити на будь-якій платформі, якщо на ній встановлена середовище виконання Java (JRE, Java Runtime Environment).

Це завдання вирішується завдяки компіляції написаного на Java коду в байт-код. Цей формат виконує JVM або віртуальна машина Java. JVM - частина середовища виконання Java (JRE). Віртуальна машина не залежить від платформи.

В Java реалізований механізм управління пам'яттю, який називається складальником сміття або garbage collector. Розробник створює об'єкти, а JRE за допомогою збирача сміття очищає пам'ять, коли об'єкти перестають використовуватися. Програма побудована за технологією клієнт-сервер, тому при запуску клієнта буде запропоновано запустити сервер або вказати його адресу. У цій статті передбачається, що програма використовується на одній машині, тому слід запустити локальний.

Залежно від завдання можна передати сервера параметри запуску, включити або вимкнути протоколювання, а також поспостерігати за консоллю сервера прямо в інтерфейсі клієнта.

Для реалізації було використано наступні бібліотеки:

- ✓ fmtlib: Форматування рядків C ++ для швидшого формування повідомлень із меншою кількістю тимчасових змінних.
- ✓ jsoncpp: синтаксичний аналізатор JSON
- ✓ kaitai: Бінарний генератор синтаксичного аналізатора та бібліотека потоків
- ✓ microhttpd: Веб-сервер
- ✓ nlohmann json: санітарна обробка JSON
- ✓ sha1: Проста реалізація алгоритму шифрування SHA1

Розроблений програмний модуль моніторингу мережевого трафіку має доволі зручний та простий у використанні користувацький інтерфейс. Найбільш

розповсюдженою операційною системою є Windows. За останніми даними її використовують 36 відсотків користувачів персональних комп'ютерів. Тому зручно використовувати саме цю операційну систему для взаємодії з модулем.

Після з'єднання з сервером і запуску почнеться сканування. Програма виведе на екран інформацію про знайдені мережах. За замовчуванням червоним кольором виділяються мережі з небезпечним шифруванням WEP, зеленим - мережі без шифрування, а жовтим з шифруванням WPA.

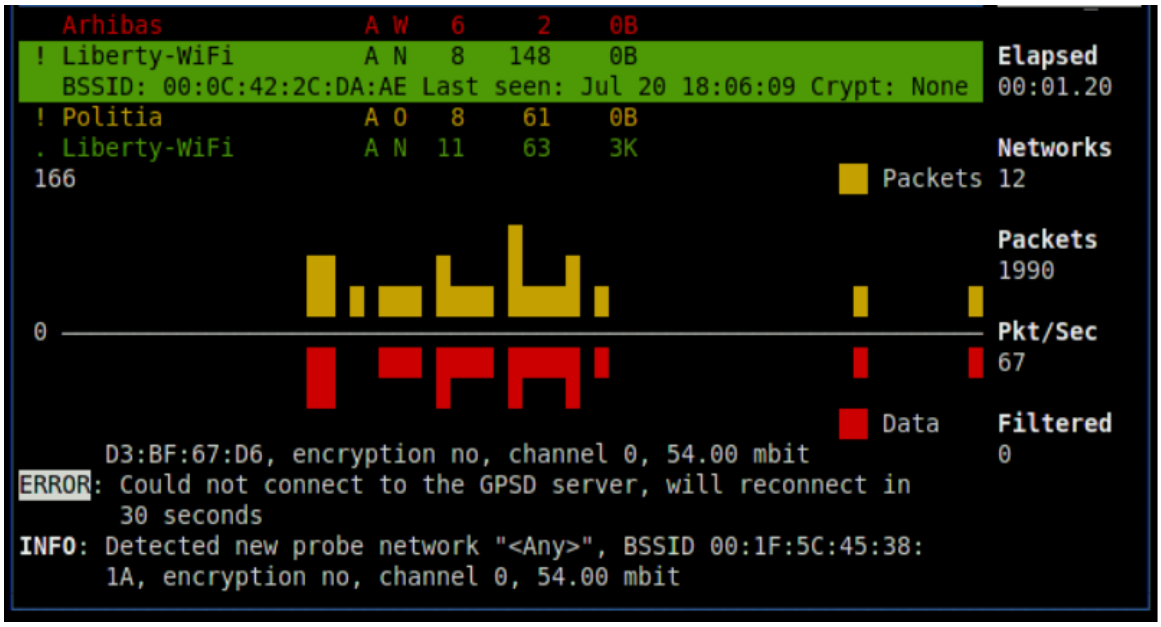


Рис 3.3.Вікно сканування наявних мереж

Фігури під списком - візуальне уявлення пакетів і даних, що проходять в ефірі, подібні графіки зустрінуться і в інших вікнах програми. При виділенні будь-якої мережі в рядку з'явиться додаткова інформація: ідентифікатор (BSSID), час виявлення, метод шифрування, кількість пакетів і обсяг даних, переданих після виявлення. Знак оклику, точка або пробіл перед назвою мережі позначають три рівня активності, колонка T - тип мережі (A = Access point), C - тип шифрування (W = WEP, N = none і т.д). Поля даних можна прибирати, рівно як і додавати нові через меню настройки. Справа відображається загальна статистика спостереження, а значення Filtered показує кількість пакетів, які потрапили під створені фільтри. У нижній частині ведеться лог, уважний читач міг помітити там помилку з'єднання з GPSD сервером. Програма може працювати з GPS-пристроєм і забезпечувати захоплювані дані географічними координатами.

При виборі мережі відкриється вікно, що відображає більш детальну інформацію:

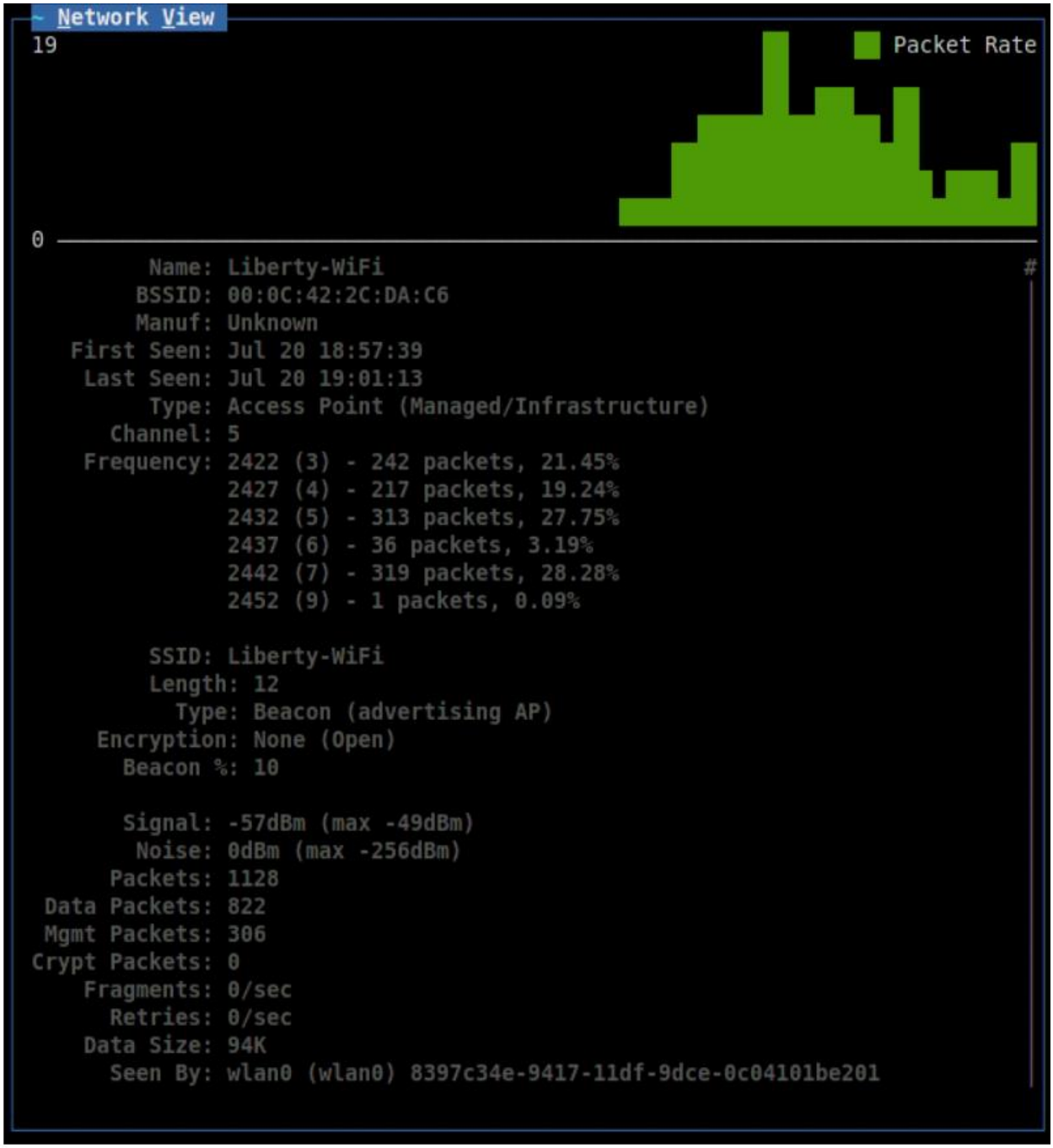


Рис. 3.4. Вікно виведення інформації про мережу

Тут, крім основної інформації, додається важливий параметр: IP-адреса клієнта.

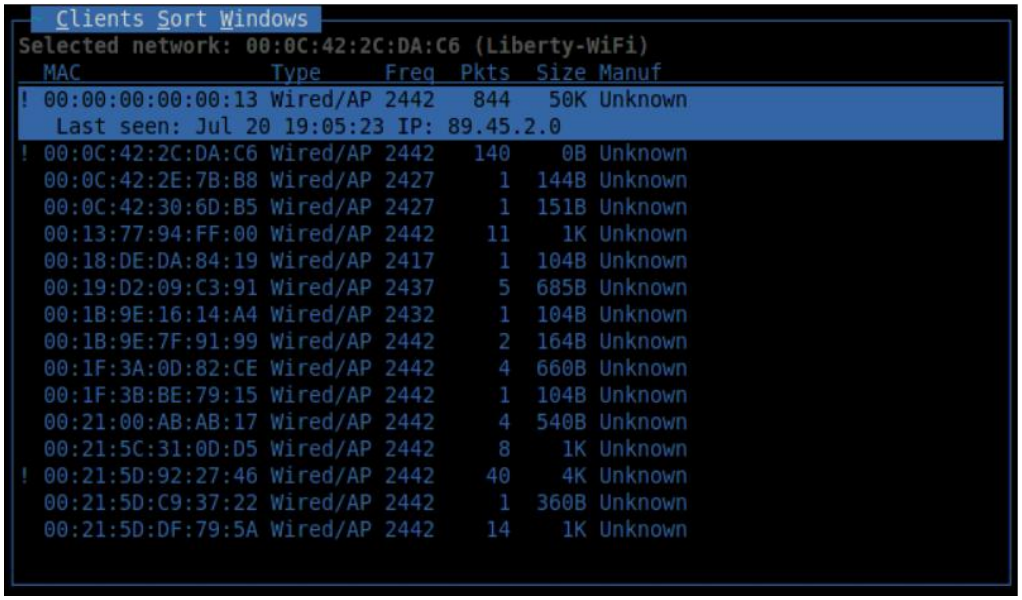


Рис. 3.5. Інформація про мережі з IP-адресами

Останнє вікно програми відображає інформацію про клієнта:

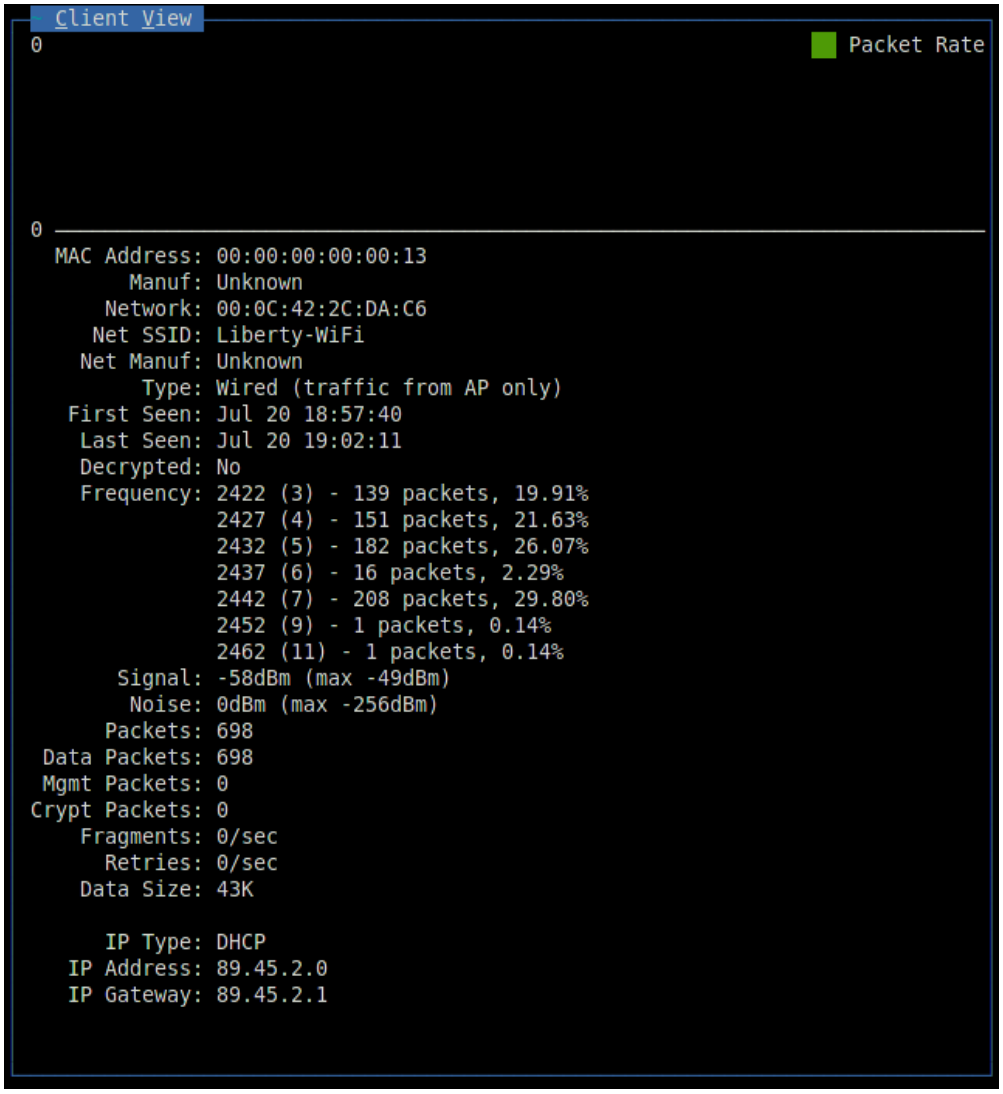


Рис.3.6.Вікно інформації про клієнта

Розглянемо роботу системи виявлення вторгнень, що дозволяє розпізнати атаку, в ході якої зловмисник виступає в ролі підробленої точки доступу.

Validmacs - допустимі значення MAC адреси для точки доступу з ім'ям «Politia», яку необхідно захистити. Спровоковану за допомогою Karma Tools атаку, програма виявляє миттєво про що і повідомляє в вікні Alerts і балці.

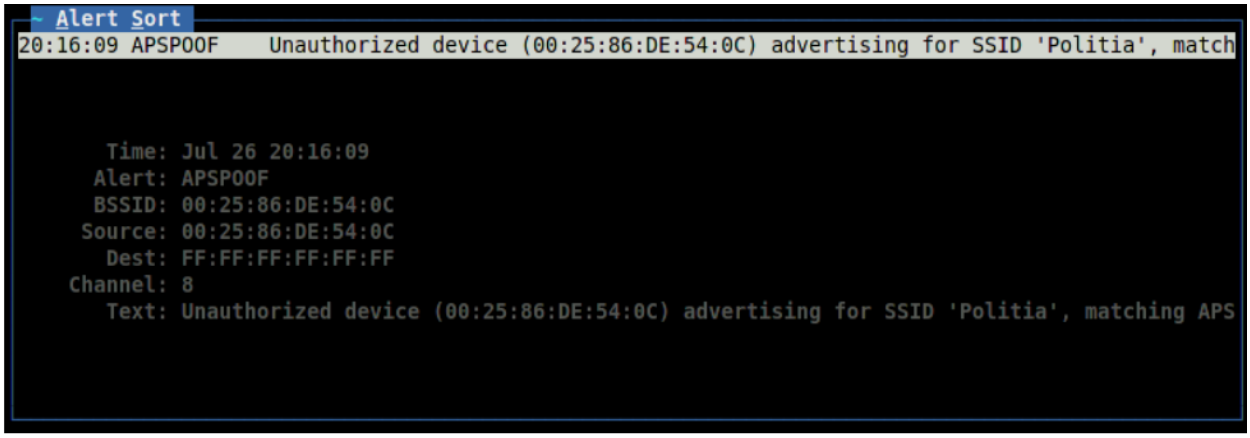


Рис. 3.7.Вікно виведення інформації про атаку

### 3.4. Порівняльний аналіз розглянутих програмних продуктів та розробленої системи виявлення атак

Так, під час дослідження розробленого програмного модуля, було виявлено ряд переваг у порівнянні з існуючими програмними засобами моніторингу мережевого трафіку. Серед плюсів можна виділити модульність програми, фільтрацію, сортування та можливість підтримки різними операційними системами.

Більш детально порівняльна характеристика наведена у таблиці 3.2.

Таблиця 3.2.

Порівняльна характеристика існуючих та розробленого ПЗ

| Назва П/З | Модульність | Фільтрація т сортування | Моніторин бездротови мереж | Виявлення прихованих мереж | Виявлення загроз |
|---|---|---|---|---|---|
| Solarwinds | Так | Так | Так | Так | Ні |
| Wireshark | Так | Так | Так | Так | Ні |

| | | | | | |
|---|---|---|---|---|---|
| Tcpdump | Ні | Ні | Ні | Так | Ні |
| Etherape | Так | Ні | Так | Так | Ні |
| Kain and ab | Ні | Так | Так | Так | Так |
| NetworkMi er | Ні | Так | Ні | Так | Так |
| Розроблени й ПЗ | Так | Так | Так | Так | Так |

Як видно з таблиці, при порівнянні програмних засобів моніторингу мережевого трафіку розроблений програмний засіб має ряд переваг над іншими порівнюваними програмними засобами. Розроблений програмний метод має модульну структуру, підтримує функції фільтрації та сортування отриманих в процесі роботи даних, що дає змогу більш детально аналізувати отримані в результаті моніторингу даних. Функції моніторингу бездротових мереж є основним завданням таких систем для використання у сучасному світі, а можливість виявлення бездротових мереж та загроз на платформах різних операційних систем у поєднанні з вище перерахованими можливостями, роблять розробленій програмний засіб більш ефективним, ніж розглянуті та описані існуючі засоби моніторингу.

**Висновки до розділу**

У третьому розділі дипломної роботи, було реалізовано та описано програмний модуль моніторингу мережевого трафіку. Після проведення досліджень та тестування програмного модуля, можна зробити висновок: Розроблений програмний модуль цілком відповідає поставленому завданню до нього, має всі необхідні функції для аналізу вихідних пакетів та виявлення

вторгнень до системи, підтримує роботу з бездротовими мережами та розпізнає атаки на систему.

Розроблений програмний модуль має зручний інтерфейс користувача, що створює сприйнятливі умови для повсякденного використання. Інтерфейс був розроблений з метою мінімізації дій користувача. При цьому, розроблений програмний модуль надає користувачу можливість власноруч керувати процесом моніторингу трафіку, що в поєднанні з інтуїтивним інтерфейсом є значно зручніше та надійніше в порівнянні з іншими існуючими програмними засобами.

Впровадження розробленого модуля в програмні засоби інформаційної безпеки значно вплине на надійність захищеності даних, оскільки він надає можливість в режимі реального часу слідкувати за інформацією та виявляти вторгення.

## СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ


1. Методи захисту інформації [Електронний ресурс]: https://works.doklad.ru/view/ZlS6TrF551o.html
2. PKI [Електронний ресурс]: https://ru.bmstu.wiki/PKI_(Public_Key_Infrastructure)#.D0.9E.D1.81.D0.BD.D0.BE.D0.B2.D0.BD.D0.B0.D1.8F_.D0.B8.D0.B4.D0.B5.D1.8F
3. A. J. Menezes, P. C. van Oorschot, S. A. Vanstone. Handbook of Applied Cryptography. — 1997.
4. Шнайер Б. Прикладная криптография. Протоколы, алгоритмы, исходные тексты на языке Си = Applied Cryptography. Protocols, Algorithms and Source Code in C. — М.: Триумф, 2002. — 816 с.
5. Нильс Фергюсон, Брюс Шнайер. Практическая криптография = Practical Cryptography: Designing and Implementing Secure Cryptographic Systems. — М. : Диалектика, 2004. — 432 с.
6. Boneh D. Twenty Years of attacks on the RSA Cryptosystem // Notices Amer. Math. Soc. / F. Morgan — AMS, 1999.
7. Gardner M. A New Kind of Cipher that Would Take Millions of Years to Break // Sci. Amer. — New York City: Nature Publishing Group, 1977.
8. NIST Special Publication 800-90A Recommendation for Random Number Generation Using Deterministic Random Bit Generators. [Електронний ресурс]: https://www.nist.gov/
9. Phong Q. Nguyen, Igor E. Shparlinski. The Insecurity of the Digital Signature Algorithm with Partially Known Nonces. [Електронний ресурс]: https://www.semanticscholar.org/paper/The-Insecurity-of-the-Digital-Signature-Algorithm-Nguyen-Shparlinski/b2ba95d5155df3a56e32fbb8320df8a197bfe1e0
10. David Pointcheval, Jacques Stern. Security Arguments for Digital Signatures and Blind Signatures. [Електронний ресурс]: https://dl.acm.org/citation.cfm?id=2816009

11. Алферов А. П., Зубов А. Ю., Кузьмин А. С., Черемушкин А. В. Основы криптографии. — «Гелиос АРВ», 2002. — 480 с.

12. Security Multiparts for MIME [Електронний ресурс]: http://tools.ietf.org/html/rfc1847.

13. Security of CBC Ciphersuites in SSL/TLS: Problems and Countermeasures
[Електронний ресурс]: https://www.openssl.org/~bodo/tls-cbc.txt

14. Simon Josefsson. GnuTLS
[Електронний ресурс] :https://lists.gnu.org/archive/html/info-gnu/2010-06/msg00015.html

15. “К вопросу о социальной инженерии.”
[Електронний ресурс]: https://cyberleninka.ru/article/n/k-voprosu-o-sotsialnoy-inzhenerii

16. “Рассказывать ли сотрудникам о социальной инженерии?.” [Електронний ресурс]: https://habr.com/ru/post/357412/

17. “Защита информации с помощью пароля.”
[Електронний ресурс]: https://studopedia.su/16_4323_ataki-na-parol.html

18. “Недостатки парольной аутентификации.”
[Електронний ресурс]: http://www.azone-it.ru/polzovateli-hotyat-otkazatsya-ot-paroley

19.“Парольная защита.”
[Електронний ресурс]: http://mf.grsu.by/UchProc/livak/b_protect/zd_3.htm

20. Корченко А. Г. Несанкционированный доступ к компьютерным системам и методы защиты: Учеб. пособие. – К.: КМУГА, 1998. – 116.

21. “Социальная инженерия и защита от неё в корпоративной среде.” [Електронний ресурс]: http://nauka-rastudent.ru/34/3683/

22. Корченко О.Г. Построение систем защиты информации на нечетких множествах. Теория и практические решения. – К.: «МК – Пресс», 2006. – 320с.

23. Процессор Intel Core i5-450M [Електронний ресурс] // Главная страница службы поддержки. – 2018. – Режим доступу до ресурсу: https://ark.intel.com/content/www/ru/ru/ark/products/49022/intel-core-i5-450m-processor-3m-cache-2-40-ghz.html.

24. Ёще раз о шифровании ГОСТ 28147 [Електронний ресурс] // Информационная безопасность. – 2018. – Режим доступу до ресурсу: https://m.habr.com/ru/post/256843.

25. Windows 8 [Електронний ресурс] // Стаття. – 2017. – Режим доступу до ресурсу: https://uk.wikipedia.org/wiki/Windows_8.

26. Підручник мови JAVA [Електронний ресурс] // Вікіпідручник. – 2018. – Режим доступу до ресурсу: https://uk.m.wikibooks.org/wiki/Підручник_мови_Python/Вступ.

27. Кнут Д.В. Получисленные алгоритмы / Д.В. Кнут. – Москва: Мир, 2008. – 724 с.

28. Брассар Ж.М. Современная криптология. / Ж.М. Брассар – Москва: ПОЛИМЕД, 2004. – 231 с.

29. Ященко В.В. Введение в криптографию. / В.В. Ященко — Москва: Гелиос АРВ, 2007. – 56 с.

30. Иванов М.А. Криптографические методы защиты информации в компьютерных системах и сетях: Учебное пособие / М.А. Иванова, И.В. Чугунков – Москва: НИЯУ МИФИ, 2012. – 220 с.

31. Дронь М.М. Основи теорії захисту інформації: Навч. посібник. / М.М. Дронь, В.П. Малайчук, О.М. Петренко – Дніпропетровськ: Вид-во Дніпропетр. ун-ту, 2011. – 312 с.

32. Кавун С.В. Інформаційна безпека. Навчальний посібник. Ч.1/ С.В. Кавун, В.В. Носов, О.В. Мажай. – Харків: Вид. ХНЕУ, 2008. – 352 с.

33. Аникин И.В. Теория информационной безопасности и методология защиты информации: учебное пособие. / И.В. Аникин, В.И. Глова, Л.И. Нейман, А.Н. Нигматуллина - Казань: Изд-во Казан. гос. техн. ун-та, 2008. – с. 358.

34. Бакут П.А. Информационные ресурсы – вопросы теории и практики / П.А.Бакут //Научно-техническая информация. Серия "Организация и методика информационной работы. – 2007. – №11. – С.16-23.

35. Гордієнко С.Б. Методи та рекомендації забезпечення інформаційної безпеки консалтингової компанії / С.Б. Гордієнко, О.С. Микитенко, В. Г. Данильчук // Вісник ДУІКТ. — 2013. — № 1. — С. 106.