**Шафрай Ілля Юрійович**

здобувач вищої освіти освітнього ступеня «Магістр», 2 курс

Національний авіаційний університет

м. Київ, Україна

IlliaShafray@gmail.com

**Метод протидії кібератакам в корпоративних мережах**

**Вступ.** У наші часи обмін даними між учасниками є важливим аспектом процесів обробки та зберігання інформації. Локальні та глобальні мережі розвиваються з впровадженням нових протоколів передачі даних, вдосконаленням апаратних можливостей мережевого обладнання, зростанням кількості підключених користувачів і збільшенням загального обсягу трафіку. Інтенсивний розвиток цієї галузі супроводжується низкою проблем. Такими як: зростання кількості користувачів інформаційних послуг та проблема захисту інформації, яка передається через мережу.

**Класифікація систем виявлення вторгнень.** Системи виявлення вторгнень можна класифікувати за різними ознаками. Одним із ключових факторів є розташування системного агента.

* Системи виявлення вторгнень на основі хостів (HIDS);
* Мережеві системи виявлення вторгнень (NIDS);
* Гібридні системи виявлення вторгнень.

HIDS -це система виявлення вторгнень, яка працює на окремому хості і моніторить його внутрішні події для виявлення загроз.

NIDS -це система виявлення вторгнень, яка аналізує мережевий трафік у реальному часі для виявлення підозрілих або шкідливих дій. Вона розташовується в ключових точках мережі, перехоплює пакети і перевіряє їх на наявність відомих атак або аномалій.

Гібридні - поєднують в собі можливості як HIDS, так і NIDS для забезпечення комплексного захисту на рівні хостів і мережі.

**Аналіз методів раннього виявлення вторгнень.** Методології, що застосовуються сучасними системами виявлення вторгнень, можна поділити на три основні категорії:

* Сигнатурні - метод виявлення на основі сигнатур функціонує через аналіз шаблонів раніше виявлених загроз. Він дозволяє швидко та точно ідентифікувати відомі атаки. Проте цей метод залежить від постійного оновлення бази даних сигнатур і не здатний розпізнавати невідомі загрози, відсутні в базі даних, або нові види атак.
* Орієнтовані на аномалії - ґрунтується на припущенні, що всі атаки відрізняються від типової поведінки системи. Цей метод базується на розділенні мережевої активності на нормальні та ненормальні стани, що здійснюється за допомогою правил або евристик, а не шаблонів або сигнатур.
* Гібридні - поєднують у собі як сигнатурні методи, так і методи виявлення аномалій, забезпечуючи таким чином більш комплексний підхід до виявлення вторгнень.

**Класифікація основних загроз у вигляді аномальної поведінки.** Атака на інформаційну систему визначається як цілеспрямована дія зловмисника, яка використовує вразливості системи, що призводить до порушення доступності, цілісності та конфіденційності оброблюваної інформації. Усунення цих вразливостей може запобігти здійсненню атаки.

Якщо атаки розглядати як аномалії в комп'ютерних мережах, то:

1. **Розвідка** класифікується як **контекстна аномалія**, оскільки ця атака спрямована на отримання специфічної інформації та розвідувальних даних.
2. **Експлойти** типу R2U і U2R є **точковими аномаліями** через їхню специфічну та складну природу, яка залежить від контексту.
3. **DoS** і **DDoS**-атаки характеризуються як **колективні аномалії**, оскільки велика кількість запитів надходить одночасно, намагаючись підключитися до сервера, хоча жоден окремий запит не є дійсним.

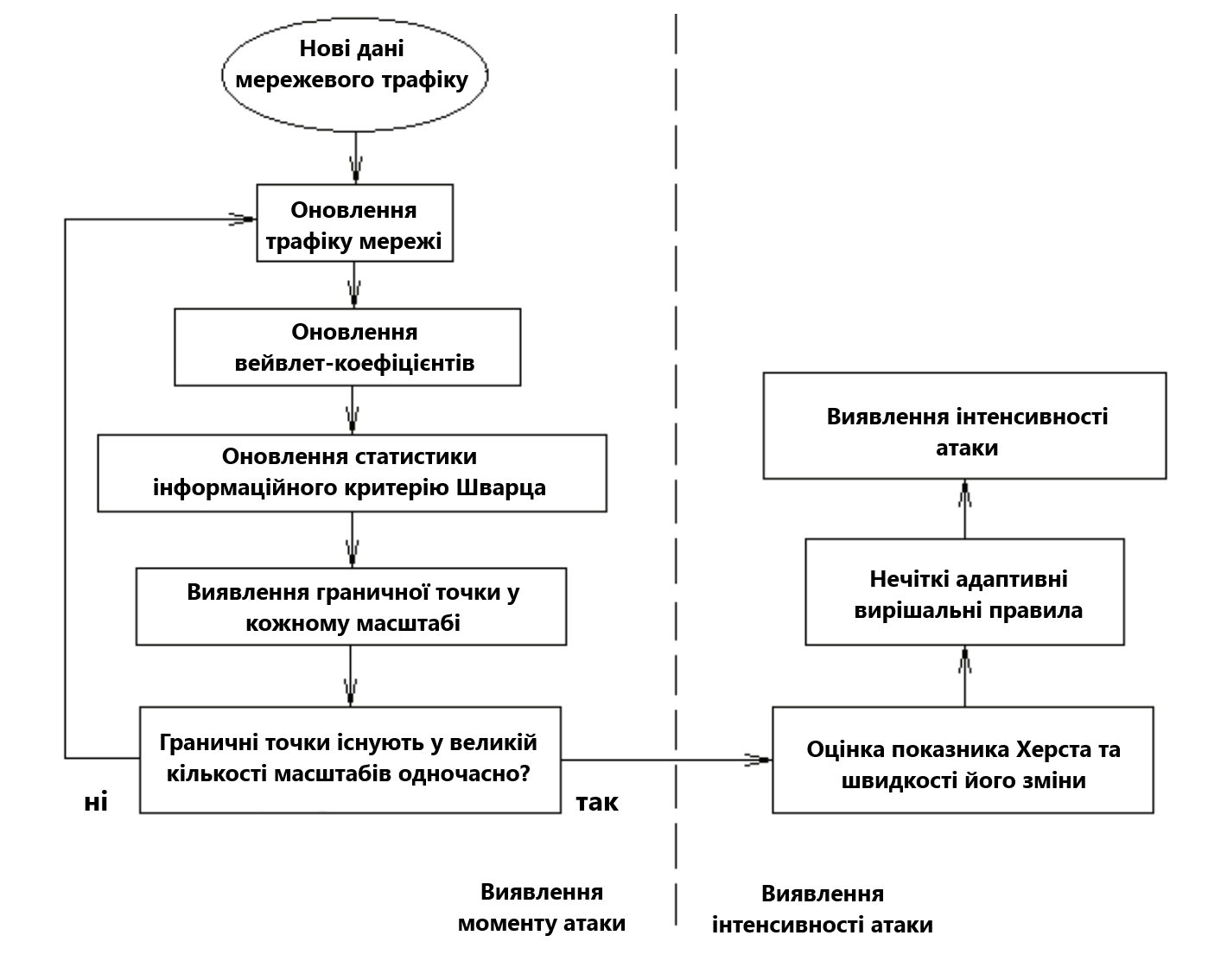


Рис. 1.1. Загальна схема виявлення атаки

**Основні етапи виконання атаки.** Процес здійснення атаки можна поділити на кілька основних етапів:

1. Збір інформації перед атакою;
2. Безпосереднє виконання атаки;
3. Завершення атаки.

Часто, коли йдеться про атаку, акцент робиться лише на другій фазі, нехтуючи початковою та завершальною стадіями. Проте збір інформації та дії з приховування слідів також є невід'ємними частинами атаки й можуть бути поділені на кілька підетапів.

**Виявлення аномально-шкідливої поведінки.** Методи виявлення зловживань базуються на припущенні, що характеристики, які визначають поведінку зловмисника, є заздалегідь встановленими. Технології виявлення зловживань здебільшого реалізуються за допомогою експертних систем, таких як Snort, RealSecure IDS та Enterasys Advanced Dragon IDS.

Нижче розглянемо технології, що використовуються в цих системах (рис. 1.2).

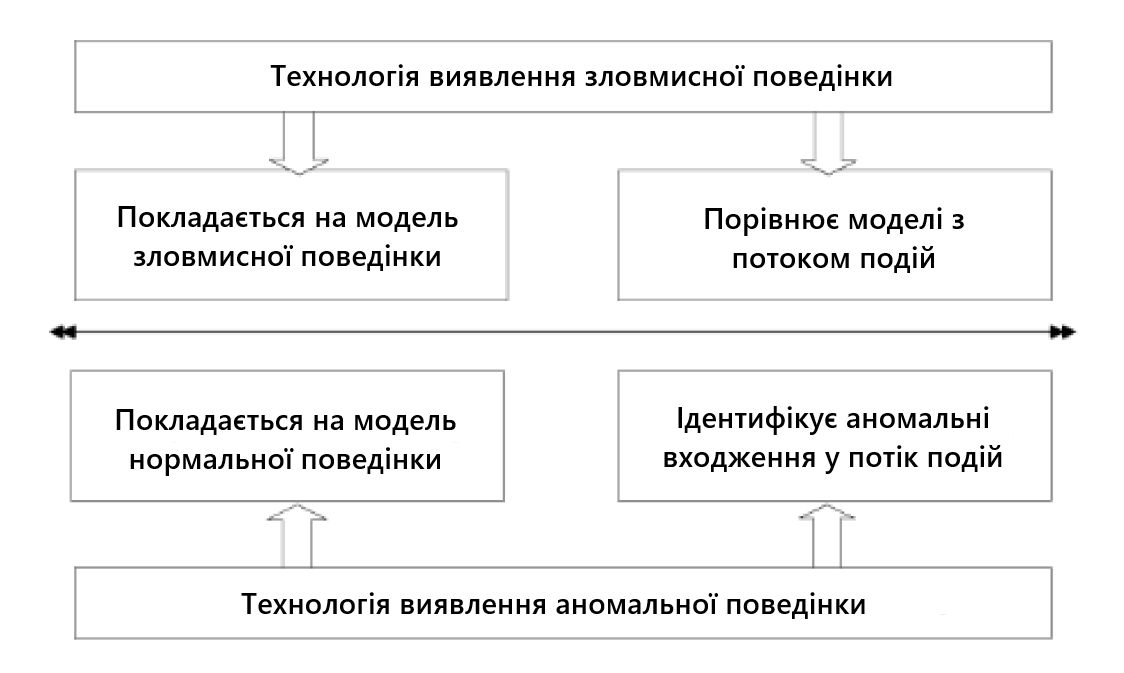


Рис. 1.2. Сучасні технології СВВ

Датчики аномалій виявляють нетипову поведінку, або аномалії, в роботі окремого об'єкта. Основною проблемою їх практичного застосування є нестабільність як захищених об'єктів, так і зовнішніх елементів, які з ними взаємодіють. Об'єктом спостереження може бути як уся мережа, так і окремий комп'ютер або мережевий сервіс.

**Головні недолікі у сучасних СВВ.** У сучасних системах домінує підхід, заснований або виключно на ідентифікації зловмисників за сигнатурами, або на виявленні аномалій у роботі мережі, що моніториться. До експлуатаційних недоліків належить високий обсяг обчислювальних завдань, необхідних для базової категоризації подій як "свої" або "чужі". Крім того, більшість існуючих систем не здатні обробляти весь обсяг вхідних даних у режимі реального часу на звичайних персональних комп'ютерах. Швидкість обробки мережевого або іншого трафіку подій часто відстає від реального часу в 1,5-2 рази. Це призводить до того, що в деяких системах аналіз проводиться із затримкою, що означає, що атака на інформаційно-обчислювальні ресурси може не бути вчасно виявлена і не буде нейтралізована існуючими засобами захисту.

Більшість сучасних сервіс-орієнтованих архітектур спочатку не призначені для роботи з різними операційними системами та апаратними обчислювальними платформами. Як наслідок, більшість продуктів, як західних, так і вітчизняних, не можуть функціонувати на кількох операційних системах одночасно.

Крім того, жоден програмний або апаратний комплекс не підтримує функцію "гарячої заміни", яка дозволила б негайно активувати резервну систему у разі відмови основної, тим самим відновлюючи скомпрометовану лінію захисту мережевого периметра.

**Висновки**

У роботі було здійснено огляд, аналіз і класифікацію сучасних систем виявлення вторгнень (СВВ). Розглянуто різні підходи до виявлення загроз, зокрема сигнатурний та поведінковий аналіз, також класифікували основні типи загроз, що проявляються у вигляді аномальної поведінки в мережах. Важливим аспектом стало виявлення недоліків сучасних СВВ, таких як обмеженість у виявленні нових загроз та кросс-платформеність. Задача підвищення ефективності СВВ в умовах зростаючих обсягів трафіку й кількості користувачів залишається актуальною, що потребує вдосконалення як методів, так і інструментів захисту.

**Список використаних джерел:**

1. Цмоць І.Г., Теслюк С.В. Моделі та засоби автоматизованої системи дослідження трафіку комп’ютерних мереж з використанням фільтра пакетів Берклі. Інтелектуальна система моніторингу та аналізу трафіку для виявлення атак в програмно-конфігурованих мережах // Наукові журнали та конференції Львівської політехніки. — 2022. — №2(1). — С. 1–11.

2. Наталенко М.М., Корецька В.О. Ефективність класифікації додатків аналізу мережевого трафіку комп’ютерних мереж методами машинного навчання // Телекомунікаційні та інформаційні технології. — 2022. — №4(72). — С. 46–53.