# Розробка підсистеми виявлення атак у системах безпеки

*Науковий керівник*

*д.т.н., проф. Роїк О. М.*

*Волкотруб Ол. П.*

# Актуальність

- Обсяг інформації, що передається в електронному вигляді постійно зростає;
- Розширюється спектр послуг, які надаються через мережу Інтернет;
- Ускладнюється структура систем, які захищаються, з’являються нові протоколи рівня додатків;
- Збільшується кількість чинників, що впливають на працездатність мережі.

Таким чином вимоги до систем захисту та контролю стану мережі збільшуються

# Мета роботи

Метою дипломної кваліфікаційної роботи є вдосконалення методу прийняття рішень в задачах захисту комп'ютерної мережі (КМ) та контролю її поточного стану.

## Завдання роботи

- Проаналізувати існуючі системи виявлення вторгнень (СВВ);
- Запропонувати шляхи підвищення точності СВВ;
- Вибрати критичні параметри, що характеризують стан мережі;
- Визначити закон розподілу вхідних даних;
- Обґрунтувати вибір порогового значення з використанням теорії прийняття рішень.

# Наукова новизна одержаних результатів

Вперше застосовано статистичні методи для визначення критичного стану комп’ютерної мережі, що дозволяє підвищити точність систем виявлення вторгнень.

# Технології захисту мережі:

- організаційний захист;
- управління доступом;
- міжмережеві екрани;
- віртуальна приватна мережа;
- системи виявлення вторгнень.

# Системи виявлення вторгнень

| + | – |
| --- | --- |
| виявляють вразливості системи безпеки;<br>можуть спрогнозувати майбутні атаки;<br>зберігають дані про минулі та поточні загрози;<br>виявляють факт вторгнення або мережеву атаку;<br>визначають розташування джерела атаки відносно локальної мережі. | неточність роботи;<br>висока ймовірність помилкових спрацювань;<br>необхідність експертних оцінок для налаштування. |

# Збір даних

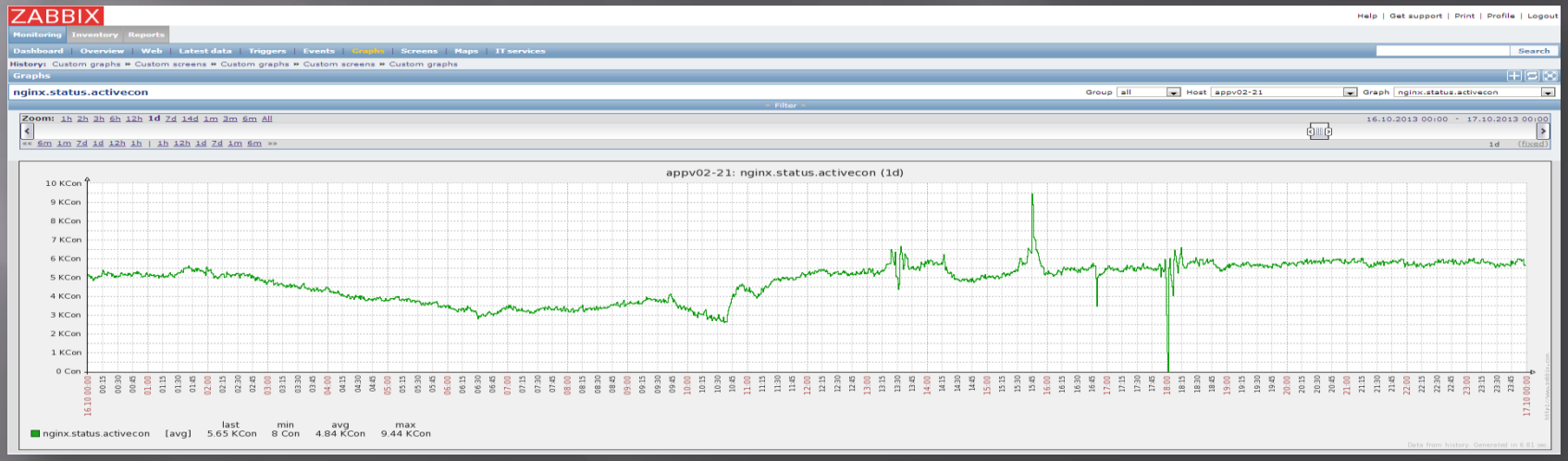
Для практичної перевірки методу використано дані, зібрані системою моніторингу Zabbix2 з реального сервера. Параметром контролю мережі обрано кількість встановлених сесій на сервері.

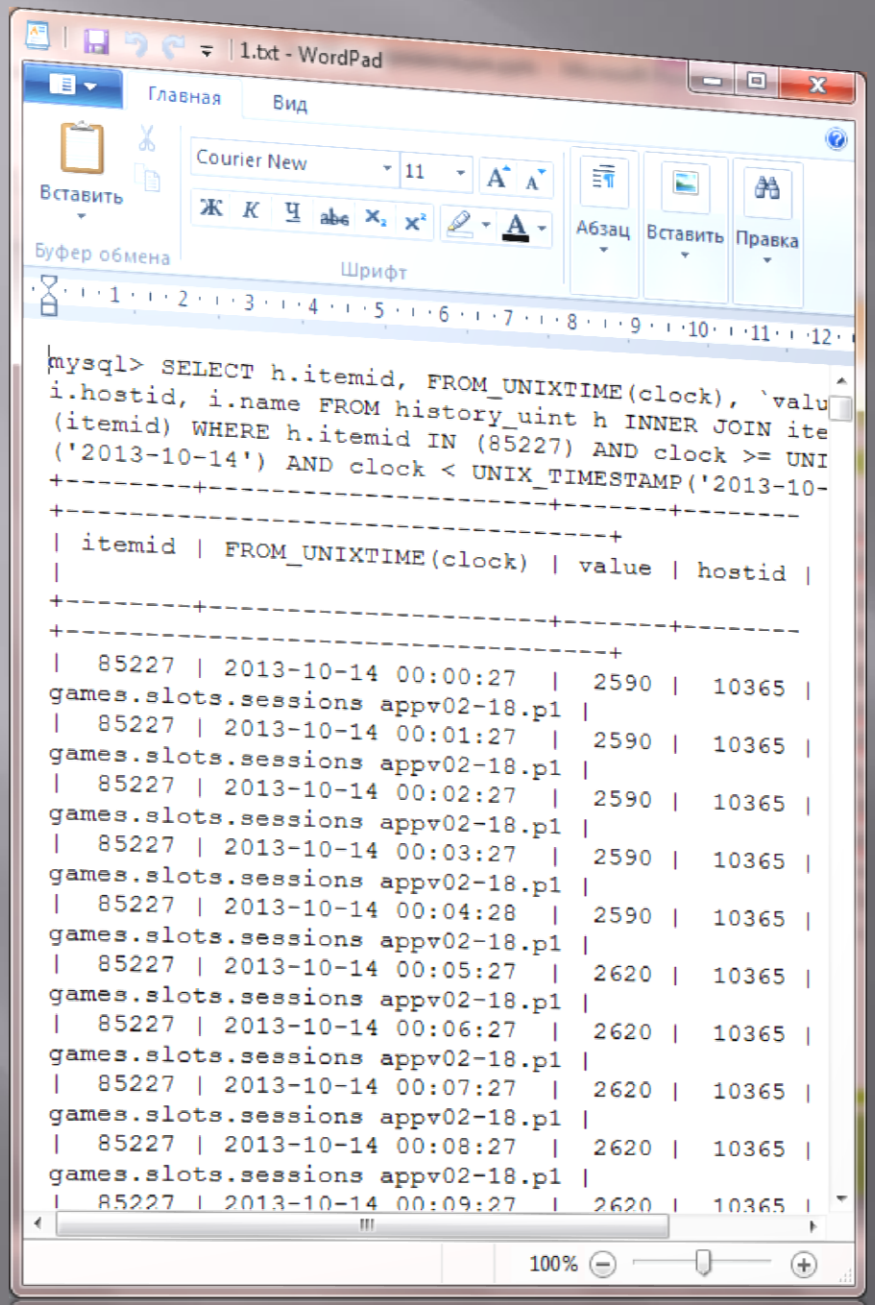
Для проведення дослідження необхідні дві вибірки:

- контрольна вибірка, що характеризує стан нормально працюючої мережі;
- вибірка з наявною аномалією;

У даному випадку визначається нижнє порогове значення контрольного параметру (кількість сесій).

# Графіки системи моніторингу Zabbix2




# Формування вибірки

Сервер Zabbix2 зберігає дані у таблиці Mysql.

Запиту для формування вибірки:

***SELECT h.itemid, FROM_UNIXTIME(o), `value`, i.hostid, i.name***

***FROM history_uint h***

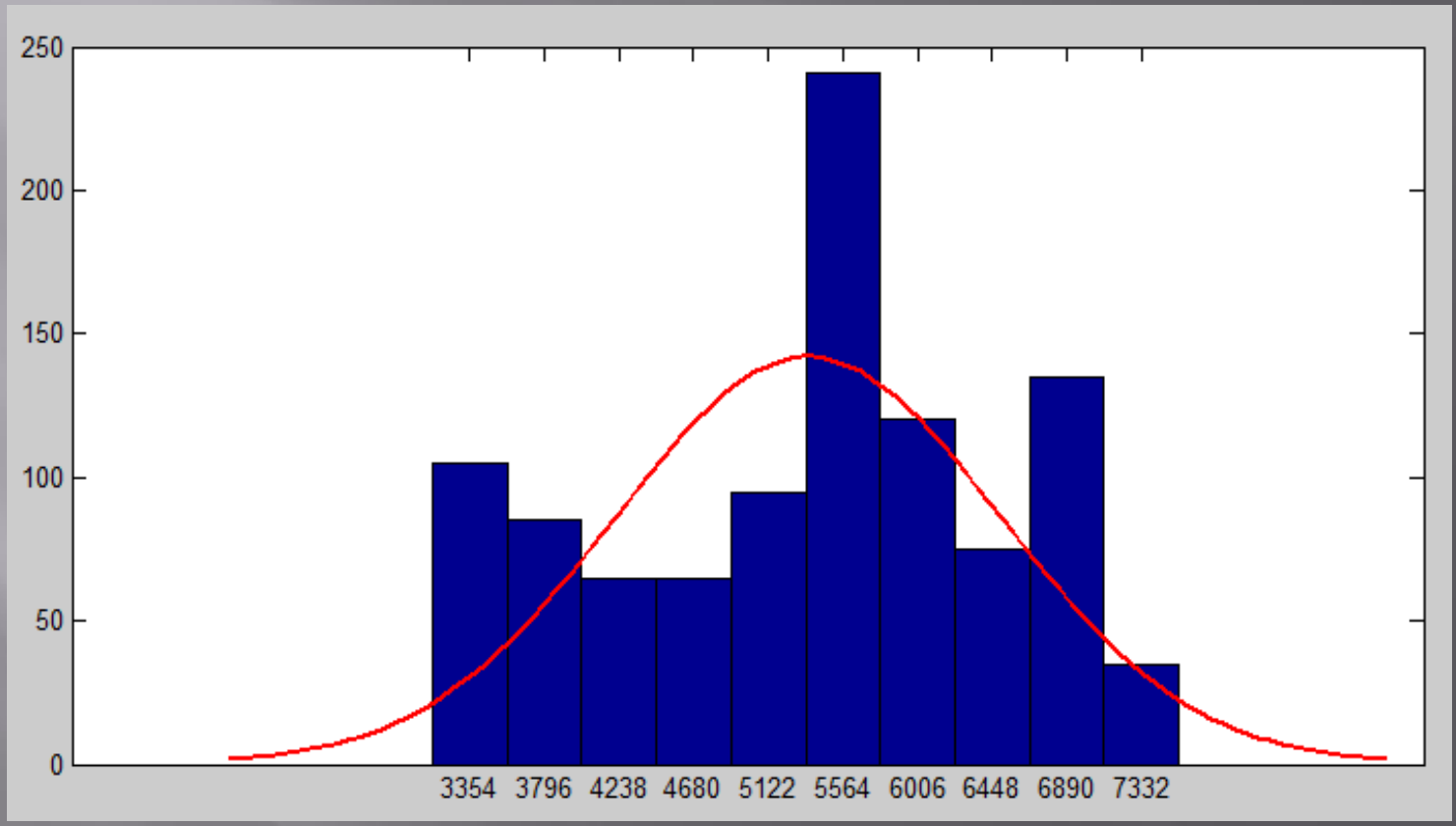
***INNER JOIN items i USING(itemid)***

***WHERE h.itemid IN (85162)***

***AND clock >= UNIX_TIMESTAMP('2013-10-13')***

***AND clock < UNIX_TIMESTAMP('2013-10-16');***

# Визначення закону розподілу




histfit(a,10),
де a – масив даних, 10 – кількість колонок гістограми.

# Розрахунок порогових значень

Порогові значення розраховані методами статистичних рішень, які направлені на зменшення середнього ризику.

Формула для розрахунку середнього ризику:

$$R = C_{21}P_1 \int_{-\infty}^{x_0} f(x/D_1)\,dx + C_{12}P_2 \int_{x_0}^{\infty} f(x/D_2)\,dx$$

$P_1$ та $P_2$ – апріорні ймовірності діагнозів $D_1$ та $D_2$ відповідно, приймемо $P_1 = 0{,}9$ та $P_2 = 0{,}1$.

$C_{12}$ та $C_{21}$ – вартості пропуску дефекту та помилкової тривоги, $C_{12} = 0{,}7$ і $C_{21} = 0{,}3$.

# Порогові значення та відповідні їм значення ризиків

| Метод | $X_0$ | $P(H_{21})$ | $P(H_{12})$ | R |
|---|---|---|---|---|
| **Мінімального ризику** | **4774** | **0,012** | **0,141** | **0,099** |
| **Мінімального числа помилкових рішень** | 5172 | $6*10^{-6}$ | 0,141 | 0,099 |
| **Максимальної правдоподібності** | 3758 | 0,031 | 0,138 | 0,106 |
| **Мінімаксу** | 2898 | 0,402 | 0,102 | 0,192 |
| **Неймана-Пірсона** | 2700 | 0,567 | 0,087 | 0,231 |

$X_0$ - розраховане значення середнього ризику

$P(H_{21})$ – ймовірність помилкової тривоги

$P(H_{12})$ – ймовірність пропуску дефекту.

# Висновки

- Проведено аналіз існуючих технологій захисту комп’ютерних мереж, який показав, що їх точність є недостатньою для багатьох потреб сучасних комп’ютерних мереж;
- Вперше запропоновано використовувати статистичні методи для визначення критичного стану комп’ютерної мережі, що дозволяє підвищити точність систем виявлення вторгнень;
- Розроблений метод використано в системі моніторингу Zabbix2, що дозволило визначити критичні значення контрольних параметрів з мінімальним ризиком;
- Цей метод рекомендовано застосовувати для систем діагностики комп’ютерних мереж, систем виявлення вторгнень, систем моніторингу.

# Дякую за увагу!