ДОДАТОК А

Графічний матеріал кваліфікаційної роботи

Харківський національний університет радіоелектроніки

Кваліфікаційна робота

«Методи виявлення мережних аномалій з використанням штучних нейронних мереж»

Виконав:
ст. гр. КСМм-21-1
Блохін О.О.

Керівник:
проф. Міхаль О.П.

Мета та завдання кваліфікаційної роботи

2

Мета кваліфікаційної роботи: аналіз методів виявлення мережних аномалій з використанням штучних нейронних мереж та імунних мереж.

Об’єкт дослідження: розподілені мережеві атаки, механізми їх виявлення та розподілені системи виявлення атак.

Завдання:

- аналіз сигнатурних та евристичних методів виявлення мережевих атак;
- розробка моделі штучної імунної системи;
- аналіз алгоритмів генетико-конкурентного навчання мережі Кохонена для виявлення аномальних мережевих з'єднань;
- розробка програмних інструментів для тестування мережевих систем виявлення атак та оцінка їх можливостей.

Класифікація методів виявлення мережних атак 3

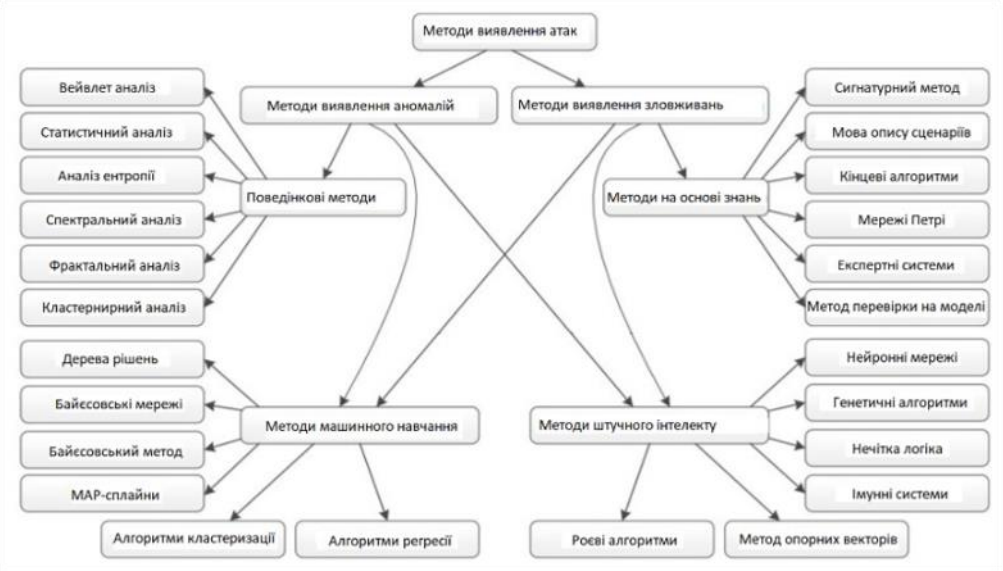
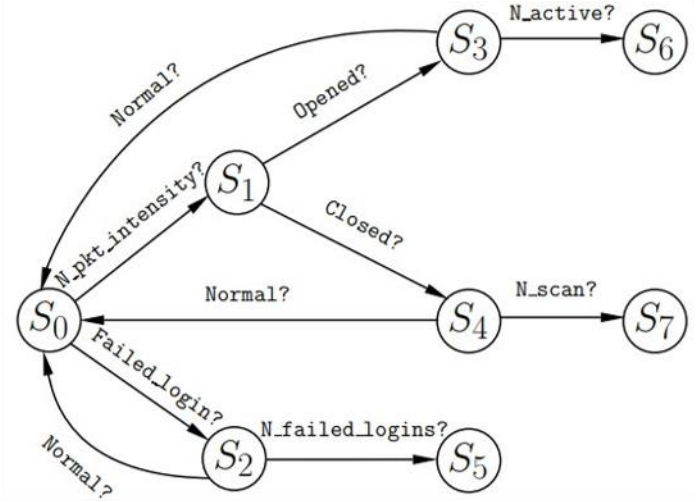
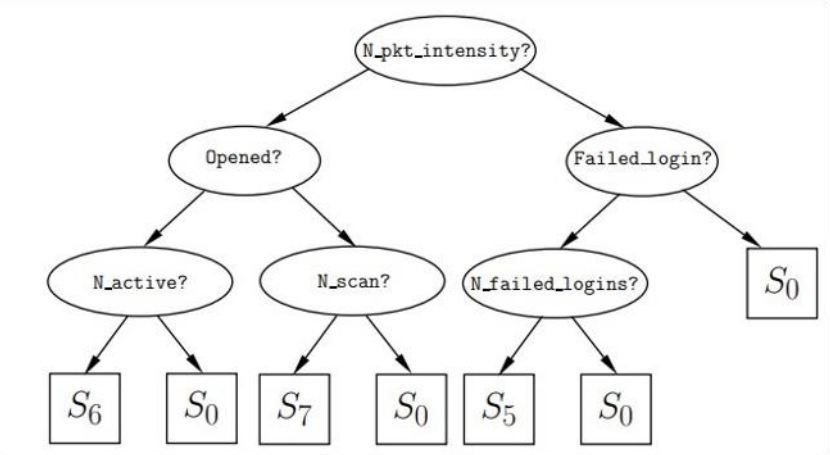


Схема класифікації мережних аномалій 4

Приклад КА для виявлення класу атак 5

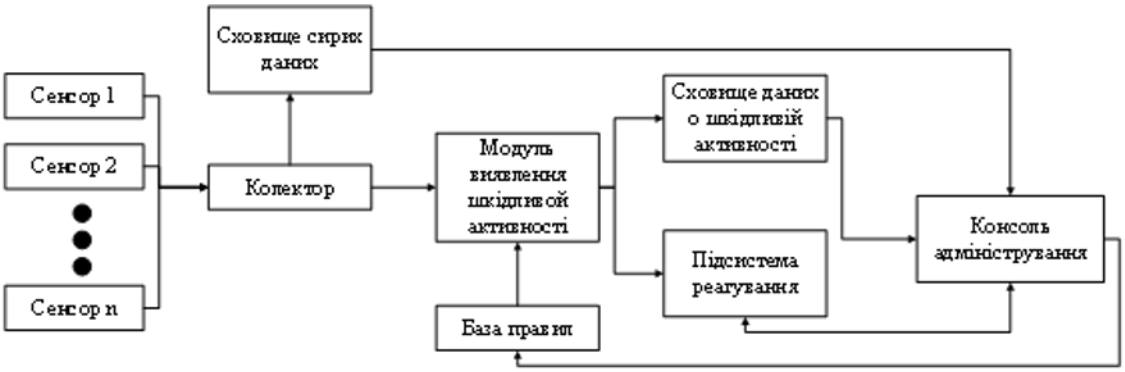


Представлення КА у вигляді дерева виразів 6



7

Архітектура розподіленої системи виявлення атак



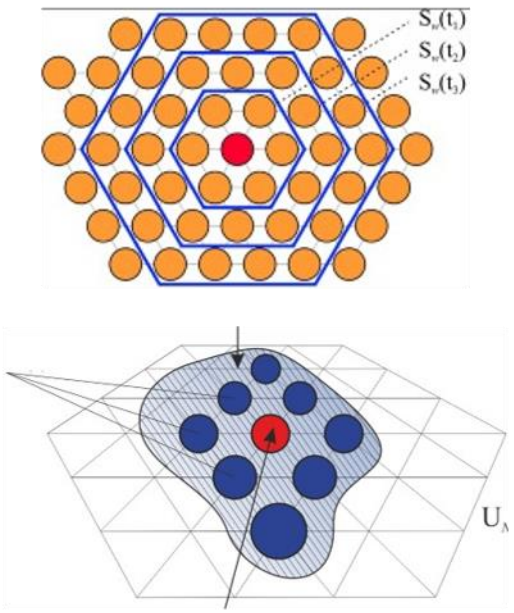
Вимоги до системи виявлення атак

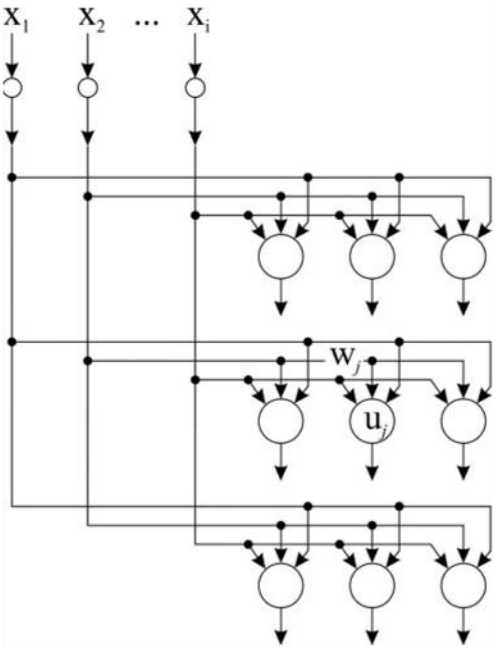
8

1. Можливість аналізу заголовків мережевих пакетів.
2. Можливість аналізу вмісту окремих мережевих пакетів, дефрагментованих послідовностей IP-пакетів та TCP-потоків.
3. Можливість збирання фрагментованого трафіку.
4. Можливість виявлення прихованих атак, атак зі вставкою.
5. Можливість обробки пакетів, що порушують стандартну поведінку сесії TCP.

Карти Кохонена

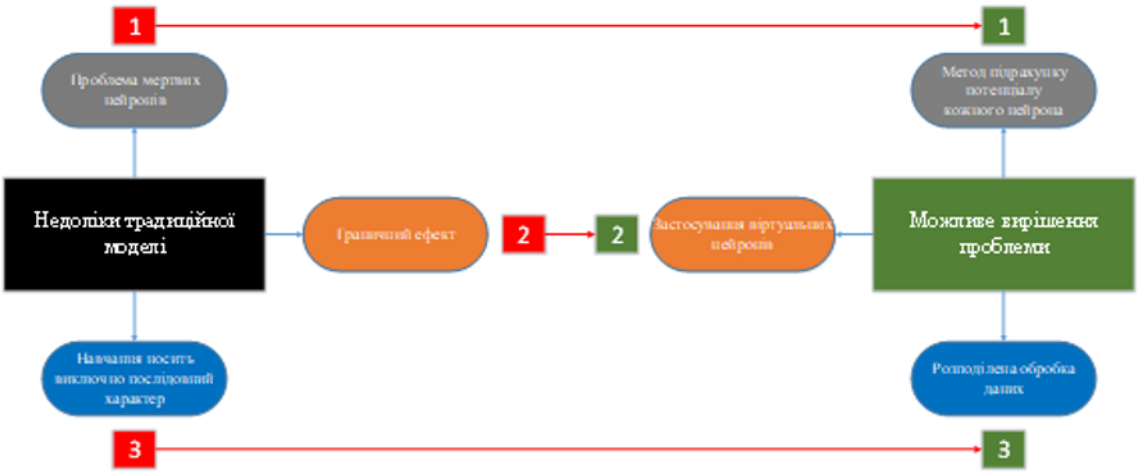
9





Недоліки класичної моделі

10



Модель штучної імунної системи на базі еволюційного підходу

11

$AISEA = \langle \mathcal{D}_T, \mathcal{D}_M, \mathcal{S}_A, \mathcal{S}_N, \mathcal{G}, R, \Psi \rangle,$

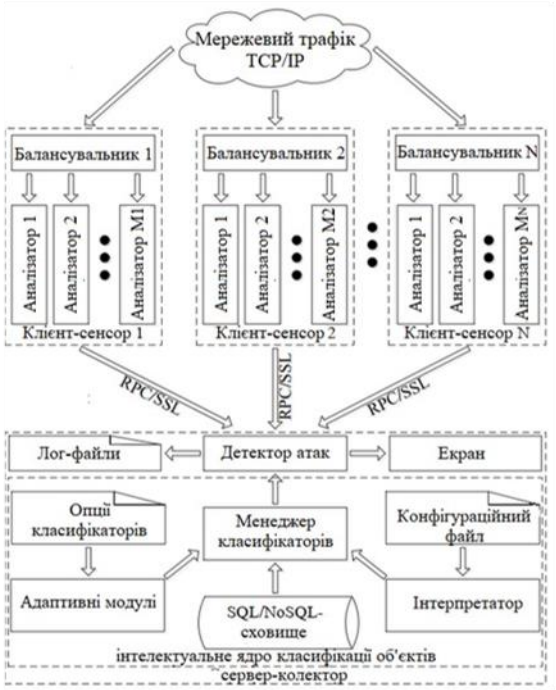
$d = \langle representation, threshold, life\_time, state \rangle,$

$representation \in \{BitString, RealV\ ector, NeuralNetwork, PetriNet, \dots\}$

- Вибір внутрішньої структури для кожного детектору $d \in \mathcal{D} : representation.$
- Формування навчального набору даних, що містить заздалегідь $\mathcal{S}_A$ відібрані „чужі“ об'єкти.
- Формування тестового набору даних, що містить заздалегідь відібрані „свої“ об'єкти.
- Вибір стратегії генетичної оптимізації імунних сенсорів.
- Вибір алгоритму навчання R імунних детекторів $\mathcal{D}$ залежно від їхнього внутрішнього уявлення.
- Вибір правила відповідності Ψ між імунним детектором та вхідним об'єктом

Архітектура розробленої СВА

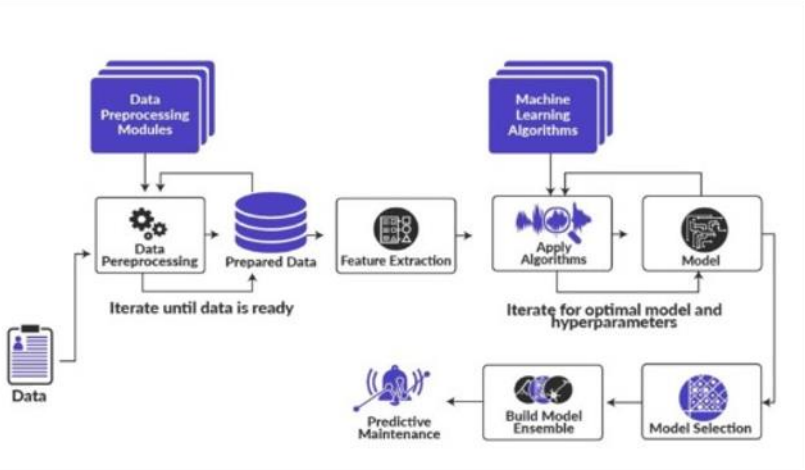
12



Узагальнена архітектура ПЗ блоку розробленої моделі.Структура для зберігання IP-потоку

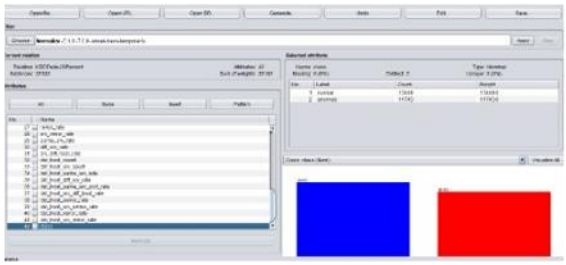
13

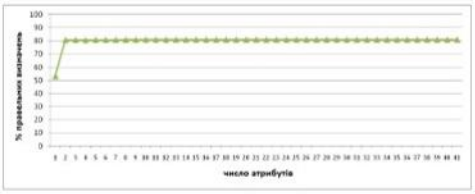
```
#pragma pack(push)
#pragma pack(1)
typedef struct {
uint32_t src_addr; // in network order
union {
uint16_t src_port; // in host order (TCP and UDP)
uint16_t icmp_echo_id; // in host order (ICMP
};
uint32_t dst_addr; // in network order
union {
uint16_t dst_port; // in host order (TCP and UI
uint16_t icmp_echo_seq; // in host order (ICM
};
uint8_t ip_proto; // TCP (6), UDP (17), ICMP (
} socket_pair;
typedef struct ip_connection {
socket_pair sock_pair;
struct timeval sndr_first_pkt_timestamp;
struct timeval sndr_last_pkt_timestamp;
struct timeval rcvr_first_pkt_timestamp;
struct timeval rcvr_last_pkt_timestamp;
uint32_t hash_value;
union {
tcp_connection tcp_conn;
udp_connection udp_conn;
icmp_connection icmp_conn;
};
u_char *user_data_l4; // user data (TCP, UDP, I
u_char *user_data_l3; // user data (IP)
uint8_t ttl; // time to live in the first packet
uint8_t tos; // type of service in the first packe
struct timeval first_pkt_timestamp;
struct timeval last_pkt_timestamp;
struct ip_connection *next_node;
struct ip_connection *prev_node;
struct ip_connection *next_free;
struct ip_connection *older_conn;
struct ip_connection *newer_conn;
scan_active_connection *s_active_conns; // scan
struct ip_connection *older_s_conn;
struct ip_connection *newer_s_conn;
dos_active_connection *d_active_conns; // DoS
struct ip_connection *older_d_conn;
struct ip_connection *newer_d_conn;
} ip_connection;
#pragma pack(pop)
```

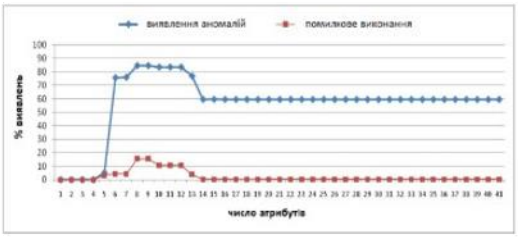


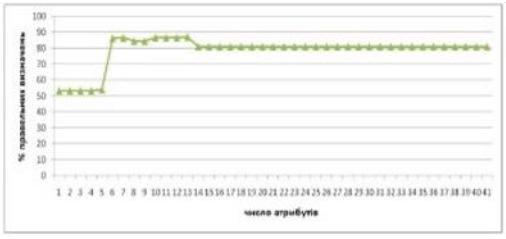
Результати

14









Висновки

Проведено аналіз методів виявлення мережних аномалій з використанням штучних нейронних мереж та штучних імунних мереж. Розроблено модель штучної імунної системи на основі еволюційного підходу. Модель характеризується наявністю дворівневої процедури навчання та тестування, а також дозволяє враховувати динамічну природу мережного трафіку за допомогою перенавчання імунних детекторів як з часом, так і у відповідь на виявлені в мережному трафіку аномалії. В якості детекторів запропоновано використання класичного апарату штучних нейронних мереж типу карт Кохонена. Розроблено архітектуру розподіленої СВА, побудованої на основі гібридизації методів ОІ та сигнатурного аналізу. СВА характеризується можливістю гарячої вставки коду, що виконується за рахунок завантаження плагінів, представлених у вигляді бінарних бібліотек і вбудованих динамічно в ядро СВА.