МОДЕЛІ ТА ЗАСОБИ АНАЛІЗУ ІНЦИДЕНТІВ БЕЗПЕКИ В ЦЕНТРАХ ЗАХИСТУ ІНФОРМАЦІЇ

Купцов Іван Іванович
Шапорін Володимир Олегович, к.т.н., доцент

Забезпечення інформаційної безпеки в корпоративних мережах все частіше покладають на спеціальні підрозділи, які називають центри кібероперацій (Cyber operations Center, SOC). Це дозволяє організувати захист ресурсів підготовленим персоналом, та перенести значну частину ризиків інформаційної безпеки третім особам.

Робота таких центрів пов’язана з великою кількістю задач, головною з яких є збір і аналіз інформації про події в мережі та на її вузлах, а також прийняття рішень про наявність реальних інцидентів безпеки.

Головним джерелом журналів подіє є системи виявлення вторгнень. Модель системи виявлення вторгнень базується спеціальних алгоритмах і моделях та формує три підсистеми виявлення:

– підсистема формування сигнатур;
– підсистема аналізу трафіку;
– підсистема реалізації реакцій на виявлення вторгнень.

Підсистема формування сигнатур використовується для аналізу відомих атак та сигнатур з ціллю виявлення загальних при знаків атак та віднесення їх до існуючих сімейств, або формування нового сімейства.

Підсистема аналізу реалізує моделі аналізу трафіку на різних рівнях мережевої моделі TCP.

Підсистема реакцій реалізує автоматизовані процеси, які направлені на активні дії системи виявлення вторгнень в разі детектування шкідливої діяльності в мережі.

Модель формування родових сигнатур можна представити множиною параметрів, композиція яких надає можливість, в подальшому, створювати

сигнатури атак. Параметри моделі відокремлюють причину атаки, етапи атаки та вразливості, які використовуються для атаки, а також методи класифікації, які використовуються для створення родових сигнатур.

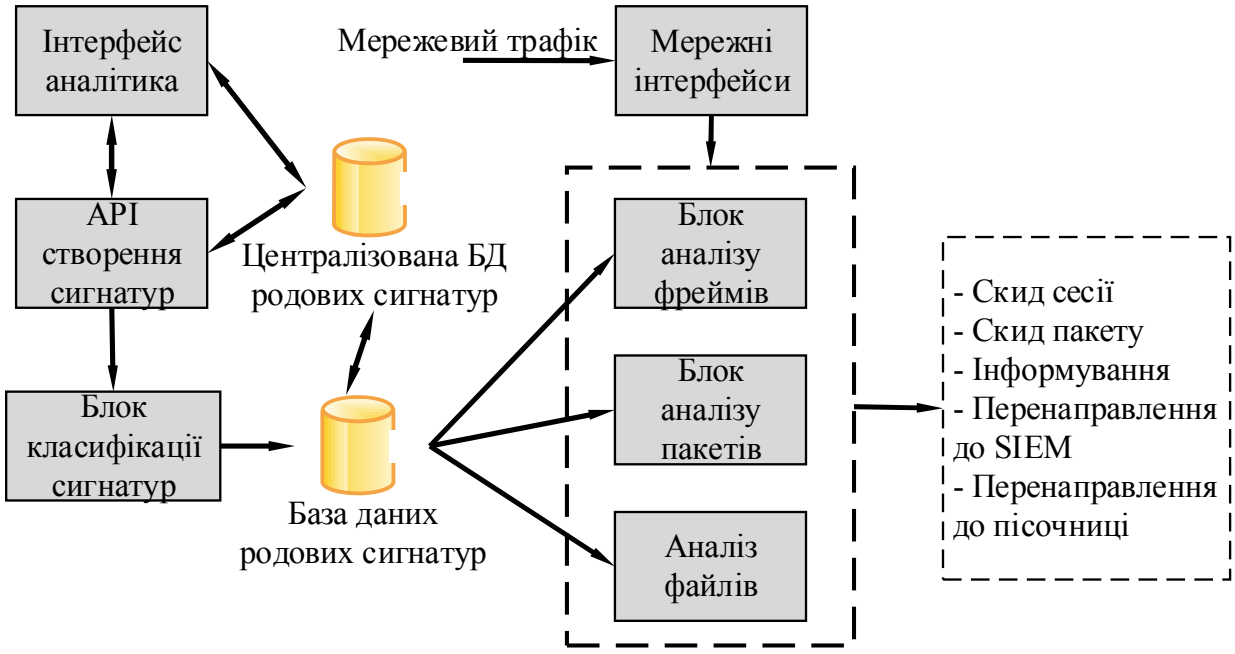

Рисунок 1 – Модель системи виявлення вторгнень

$$B_{SS} = \{\{PT(T_i)\}, \{S_a\}, \{A_C\}\},$$

$$PT(T_i) = \{\{Tf_1\}, \{Tf_2\}, \dots, \{Tf_n\}\},$$

$$S_a = \{S_{i1}, S_{i2}, \dots, S_{in}\},$$

$$A_C = \{a_1, a_2, \dots, a_k,\}$$

В даній моделі $PT(T_i)$ є множиною загроз, які призводять до атак, а Tf_n – множина факторів, які впливають на загрозу. Множина S_a – опис атаки на мережу, де S_{i1} є множиною етапів атаки, яка формує сигнатуру атаки і в подальшому родову сигнатуру.

Множина A_C являє собою набір алгоритмів класифікації, який використовується для створення родових сигнатур.

Аналіз мережевого трафіку базується на моделях виникнення загроз та проведення атак. Враховуючі різноманітність мережевих атак, підсистема ділиться на три блоки:

– блок аналізу фреймів;

– блок аналізу пакетів;

– блок аналізу файлів.

У відповідності з даним підходом ймовірність виникнення небажаного інциденту залежить від п'яти параметрів:

– ймовірність загрози;

– ймовірність здійснення сценарію загрози;

– вплив відносини спадщини між сценаріями загроз і небажаними інцидентами;

– оцінка набору вразливостей системи;

– ймовірності здійснення сценарію небажаного інциденту.

Аналізуючи побудовані раніше дерева впливу, можна побачити, що кожен небажаний інцидент схильний до впливу різних варіантів композиції сценаріїв загроз і небажаних інцидентів. Узагальнюючи дані варіанти, можна побудувати 6 ієрархічних моделей небажаних інцидентів.

Одиночна модель. Дана модель описує вплив одного сценарію загрози на небажаний інцидент.

Послідовна модель. Дана модель описує вплив на небажаний інцидент послідовно відбуваються сценаріїв загрози.

Паралельна модель. Дана ієрархічна модель описує вплив на небажаний інцидент незалежних один від одного сценаріїв загрози.

Паралельно-послідовна модель. Дана модель описує випадок коли на небажаний інцидент паралельно впливають залежні сценарії.

Модель небажаний інцидент - небажаний інцидент. Дана модель описує випадки, коли на один небажаний інцидент впливає інший небажаний інцидент.

Змішана модель. Дана модель описує випадки, коли на небажаний інцидент впливають і сценарії загроз і інші небажані інциденти.

$$P(VBD) = FUI_{VBD}\left(YUI(VBD), PX, C_{L\xi}(VIS, VBD), PUI(VBD)\right),$$

$$PX = FTS_{VIS}\left(PT(V), Cinit(V), YTS(VIS), PTS(VIS)\right).$$

$$P(HAG) = FUI_{HAG}\left(PX2, C_{Lt}(HPA, HAG), PUI(HAG), YUI(HAG)\right),$$

$$PX1 = FTS_{HSP}(PT(H), PTS(HSP), Cinit(H), YTS(HSP)),$$

$$PX2 = FTS_{HPA}(PT(H), PTS(HPA), PX1, C_{Lt}(HSP, HPA)\}, Cinit(H), YTS(HPA)).$$

На першому етапі визначаються всі фактори, які можуть вплинути на виникнення інциденту. Будується відповідна структура і безліч, де фактори групуються і представляються своїми оцінками. Кожна термінальна структура являє оцінку фактора, нетермінальних вершина є функцією згортки приватних чинників.

На другому етапі кожен фактор отримує експертну оцінку. Оцінку необхідно унормувати, тому вона задається з використанням коефіцієнта задоволеності:

$$f_i = 1 - e^{-\alpha t}$$

де - α - коефіцієнт задоволеності,

t- час функціонування даного об'єкту

Коефіцієнт визначає ступінь задоволеності станом системи, роботою і навичками персоналу тощо. Час характеризує тривалість роботи об'єкта (пристрій, система, актуальність інформації і т. д.), Який схильний до ризику від розглянутої загрози.

В рамках даного етапу виконується ранжування виявлених чинників. Це дозволяє, на основі переваг експертів, встановити важливість одних чинників перед іншими, або визначити найбільший вплив сукупності факторів де використовується відношення переваги між факторами та відношення взаємодії пар факторів. На основі даних переваг будується навчальна множина.

На третьому етапі визначаються нечіткі міри для кожної нетермінальних вершини. Для цього використовуються отримані раніше оцінки і значення переваг і взаємодії. В результаті виходить безліч нечіткої міри.

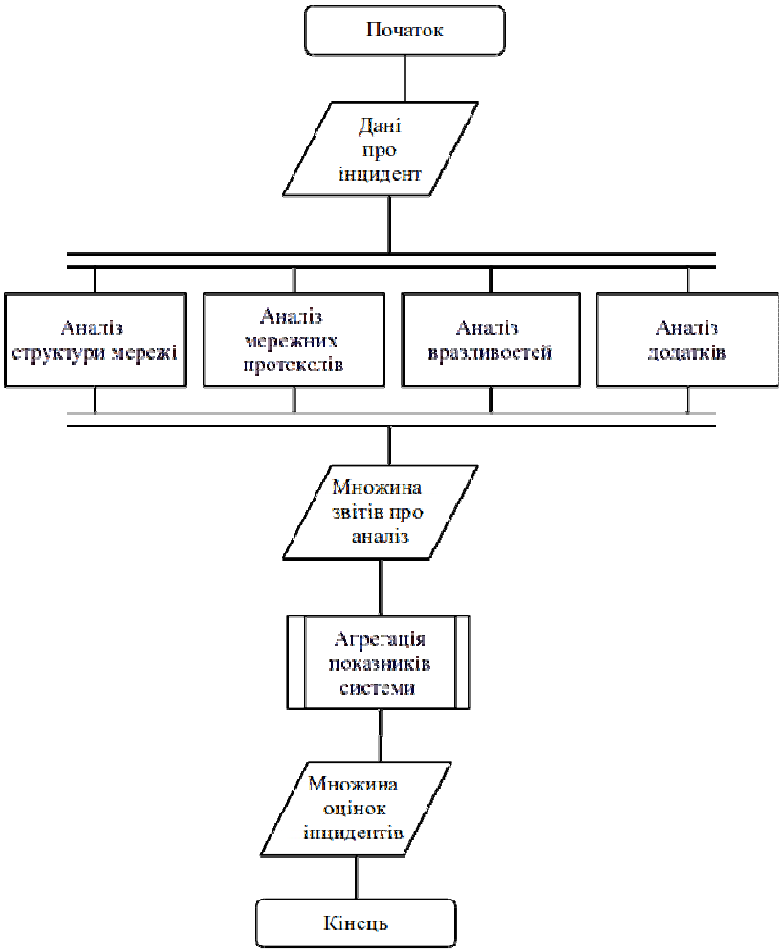

Рисунок 2 — Загальний алгоритм оцінки інцидентів

Узагальнюючи дані моделі, можна сказати, що використання інтелектуальних засобів збору, класифікації, аналізу та візуалізації даних про інциденти, дозволяє скоротити час реакції на виникнення подій безпеки в комп'ютерних мережах, а також зменшити кількість ложнопозитивних тривог (витрачають час аналітиків) та ложнонегативних (не виявляються реальні інциденти).