УДК 004.056:519.17

АНАЛІЗ МОДЕЛЕЙ СИСТЕМ ЗАХИСТУ ІНФОРМАЦІЇ, ПОБУДОВАНИХ З ВИКОРИСТАННЯМ ТЕОРІЇ ГРАФІВ

Румянцева О.В
Науковий керівник – к.т.н., с.н.с. Пшеничних С.В.
Харківській національний університет радіоелектроніки,
каф. Інфокомунікаційної інженерії ім. В.В. Поповського,
м. Харків, Україна
тел+38(099) 029-93-20

The report reviews the analysis of information security models that utilize graph theory. Graph theory is an essential tool for visualizing and analyzing complex systems, and its application to information security has resulted in models such as Attack Graphs, Defense Graphs, and Threats and Countermeasures. The strengths and limitations of each model are explored, and it is emphasized that the choice of an appropriate model depends on the specific security goals and the size of the system. The analysis highlights the potential for graph theory to contribute to the development of robust information security systems.

Моделі систем захисту інформації, що побудовані на основі теорії графів, дозволяють візуалізувати структуру інформаційної системи та виявляти вразливі місця, що дозволяє оптимізувати процеси керування доступом та керування вразливостями. У доповіді розглядається декілька таких моделей.

1. Модель управління доступом на основі графа. Дана модель використовується для визначення того, які суб'єкти мають доступ до об'єктів в інформаційній системі. Граф у цій моделі є набір вузлів (суб'єктів та об'єктів) та ребер (прав доступу). Вузли можуть бути пов'язані один з одним кількома ребрами, що представляють різні види доступу (читання, запис, видалення тощо) [1].

Ця модель полегшує процес управління доступом, дозволяючи визначати та змінювати права доступу для кожного суб'єкта окремо. Однак, необхідно враховувати, що ця модель може бути неефективною, якщо інформаційна система має великий розмір та складну структуру.

2. Модель оцінки ризиків на основі графів. Ця модель використовується для визначення ризиків, пов'язаних із компонентами інформаційної системи, та для вжиття заходів для зниження рівня цих ризиків. У цій моделі інформаційна система представлена у вигляді графа, де вершини відповідають компонентам, а ребра позначають зв'язок між ними.

Ця модель дозволяє виявити критичні компоненти системи та зосередити зусилля на їхньому захисті. Крім того, вона може бути використана для оцінки ефективності різних заходів щодо зменшення рівня

ризику. Однак, ця модель може бути неповною, якщо не враховувати всі можливі загрози.

3. Модель управління вразливістю на основі графів. Ця модель використовується для виявлення вразливостей в інформаційній системі та визначення заходів щодо їх усунення. У цій моделі інформаційна система представлена у вигляді графа, де вершини являють собою уразливості, а ребра - зв'язки між вразливостями та компонентами системи, які можуть на них вплинути [2]. Наприклад, вразливість в одному компоненті може призвести до розкриття інформації в іншому компоненті, з яким вона пов'язана.

Ця модель дозволяє виявляти вразливості та оцінювати їхню критичність для інформаційної системи. Крім того, вона може використовуватися для визначення оптимальної стратегії управління вразливістю. Однак, дана модель може бути складною для аналізу у випадку, якщо інформаційна система має велику кількість компонентів та вразливостей, що може призвести до складнощів при прийнятті рішень щодо управління вразливостями.

4. Модель загроз і контрзаходів (Threats and Countermeasures - TAM). Ця модель заснована на поданні інформаційної системи у вигляді графа, в якому вузли являють собою загрози, а ребра - контрзаходи, що спрямовані на запобігання цим загрозам.

Ця модель дозволяє визначити найбільш ймовірні загрози для інформаційної системи та вибрати найбільш ефективні контрзаходи для їх запобігання [2]. Крім того, вона може використовуватися для оцінки ефективності наявних контрзаходів та визначення того, які покращення слід внести до системи захисту. Однак, ця модель також може бути складною для аналізу у випадку, якщо є велика кількість загроз та контрзаходів, що може призвести до складнощів при ухваленні рішень щодо управління інформаційною безпекою.

Загалом моделі систем захисту інформації, що побудовані з використанням теорії графів, є ефективними інструментами для аналізу та управління інформаційною безпекою. Однак, для досягнення найкращих результатів необхідно враховувати особливості конкретної інформаційної системи та обирати ту модель, що найбільше підходить для даної системи та її цілей.

Список використаних джерел:

1. Кіровоградський, М. І., & Куренков, О. С. (2016). Теорія графів: Навчальний посібник. Логос.

2. Коваленко, В. О., & Куренков, О. С. (2018). Аналіз інформаційних систем з використанням методів теорії графів. Виддавництво «Видавництво Полтавського університету економіки і торгівлі».