Д.А. Шибков, У.А. Савилова, Д.А. Яковлева, О.С. Машкова

ПРОГРАММНАЯ РЕАЛИЗАЦИЯ ПОДСИСТЕМЫ ОБНАРУЖЕНИЯ ВТОРЖЕНИЙ НА ОСНОВЕ СЕТЕЙ ПЕТРИ

(Тамбовский государственный технический университет)

Программная реализация подсистемы обнаружения вторжений Petri nets Emulator позволяет моделировать развитие атакующих действий злоумышленника с целью выявления ключевых моментов атак и выработки рекомендаций по ее парированию.

Пользовательский интерфейс Petri nets Emulator, продемонстрированный на рисунке 1, представляет собой одно окно с семью вкладками, предназначенными для выполнения различных задач.

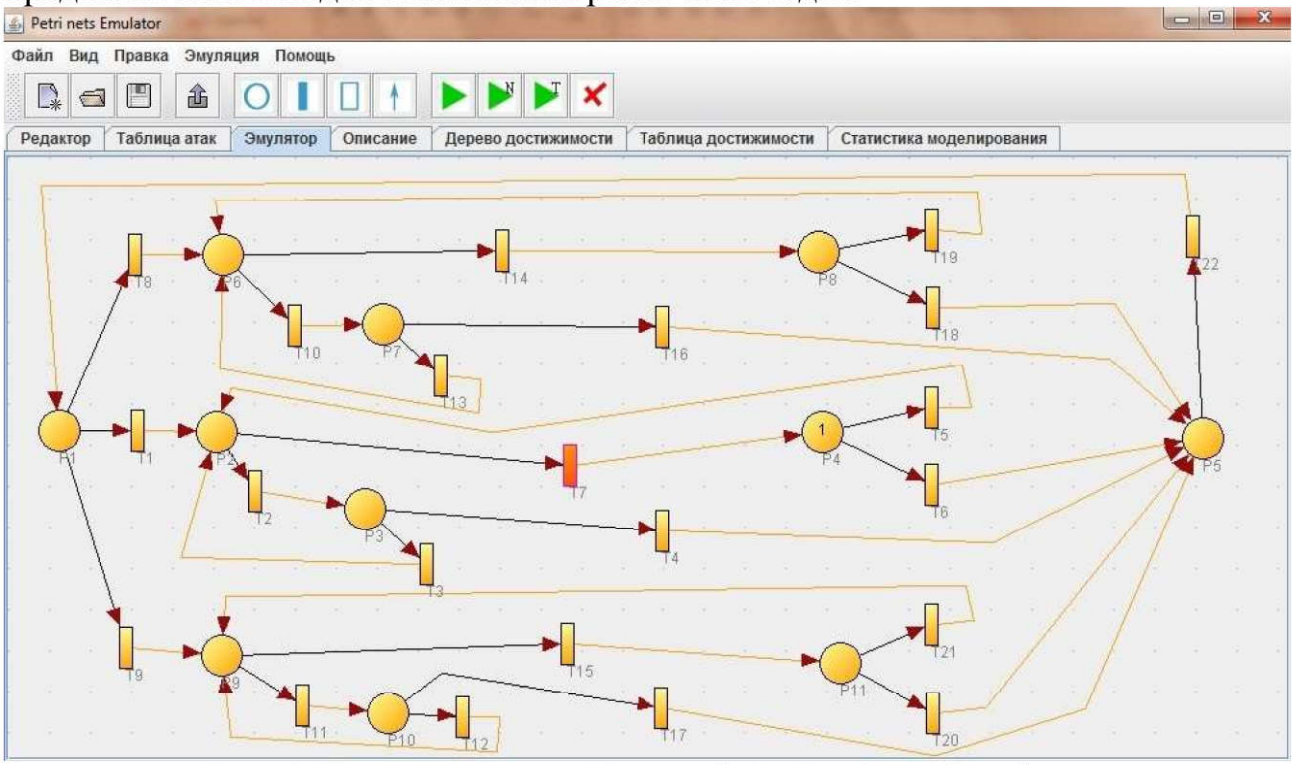

Рис. 1. Пользовательский интерфейс Petri nets Emulator

«Редактор» используется для создания новых сетевых моделей атак, а также для редактирования уже существующих.

«Таблица атак» позволяет установить связь с созданной базой данных атак, а затем выбрать атаки для эмуляции и квалификацию злоумышленника.

«Эмулятор» применяется для моделирования развития атак из базы данных с целью изучения статистических данных и расчета вероятности их успешной реализации.

«Описание» содержит таблицу связи позиций и переходов созданной сети.

«Дерево достижимости», представленное на рисунке 2, отображает связи между состояниями сети с выделением зеленым цветом нулевого состояния, оранжевым – состояния-повтора и красным – тупикового состояния при его наличии, что позволяет выполнить проверку логики построенной сети и выявить ошибки в связях.

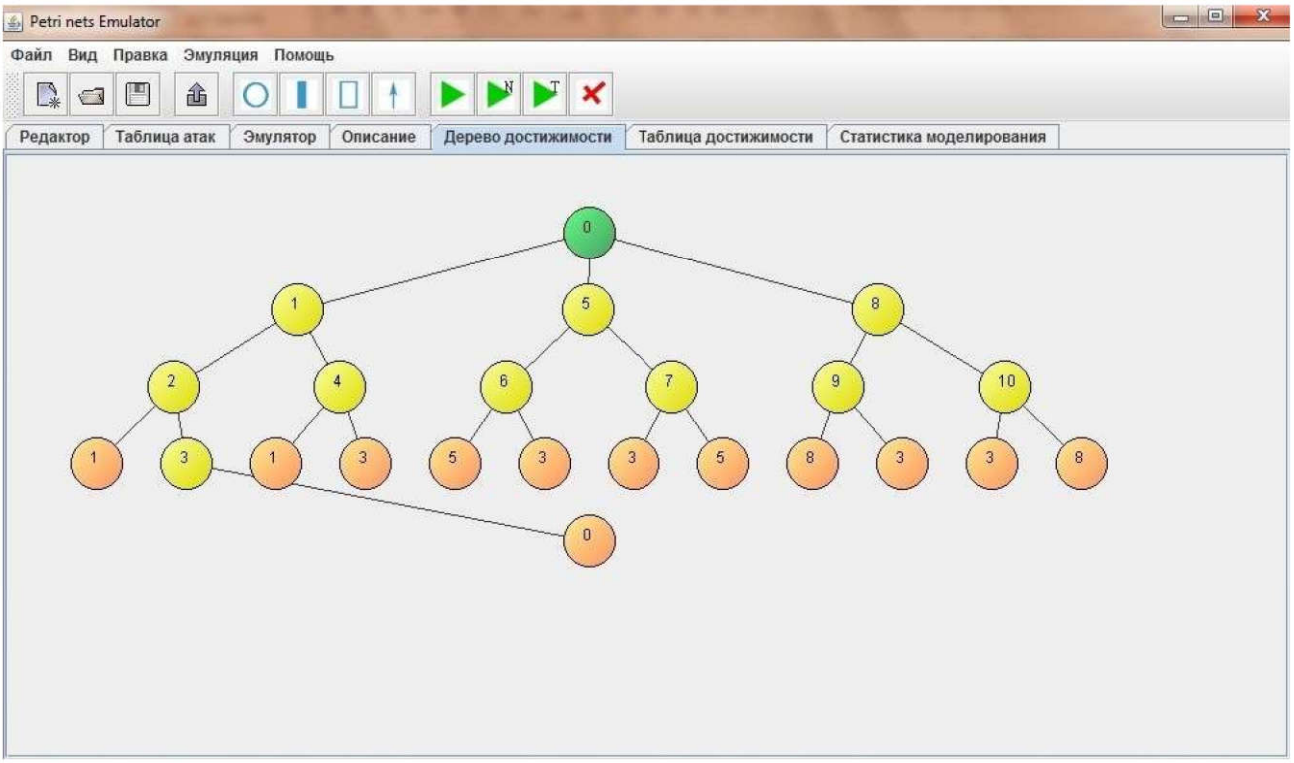

Рис. 2. Вкладка «Дерево достижимости»

«Таблица достижимости» используется для построения дерева достижимости, а также содержит информацию о связях между позициями, переходами и марковскими состояниями созданной сетевой модели атаки.

«Статистика моделирования», представленная на рисунке 3, содержит отчеты о результатах моделирования и диаграммы с частотами прохождения фишки через позиции, средним временем работы переходов, средним временем возврата сети в каждое состояние и статистической вероятностью перехода сети в каждое состояние.

Сеть Петри, формализующая общую стратегию развития атакующих действий злоумышленника, создана в качестве основы для использования в моделях конкретных атак различной сложности, но если при использовании составные переходы будут рассматриваться как обычные, то с ее помощью можно рассчитать статистические вероятности успешной реализации атак низкой, средней и высокой сложности в зависимости от выбранной квалификации злоумышленника. При этом модель может учитывать вероятность выбора злоумышленником атаки той или иной сложности [1-2].

По результатам моделирования составлена диаграмма, представленная на рисунке 4. Лингвистические переменные сложности атак и соответствующие

им квалификации злоумышленников взяты в неизменном виде из баз данных уязвимостей [3-5].

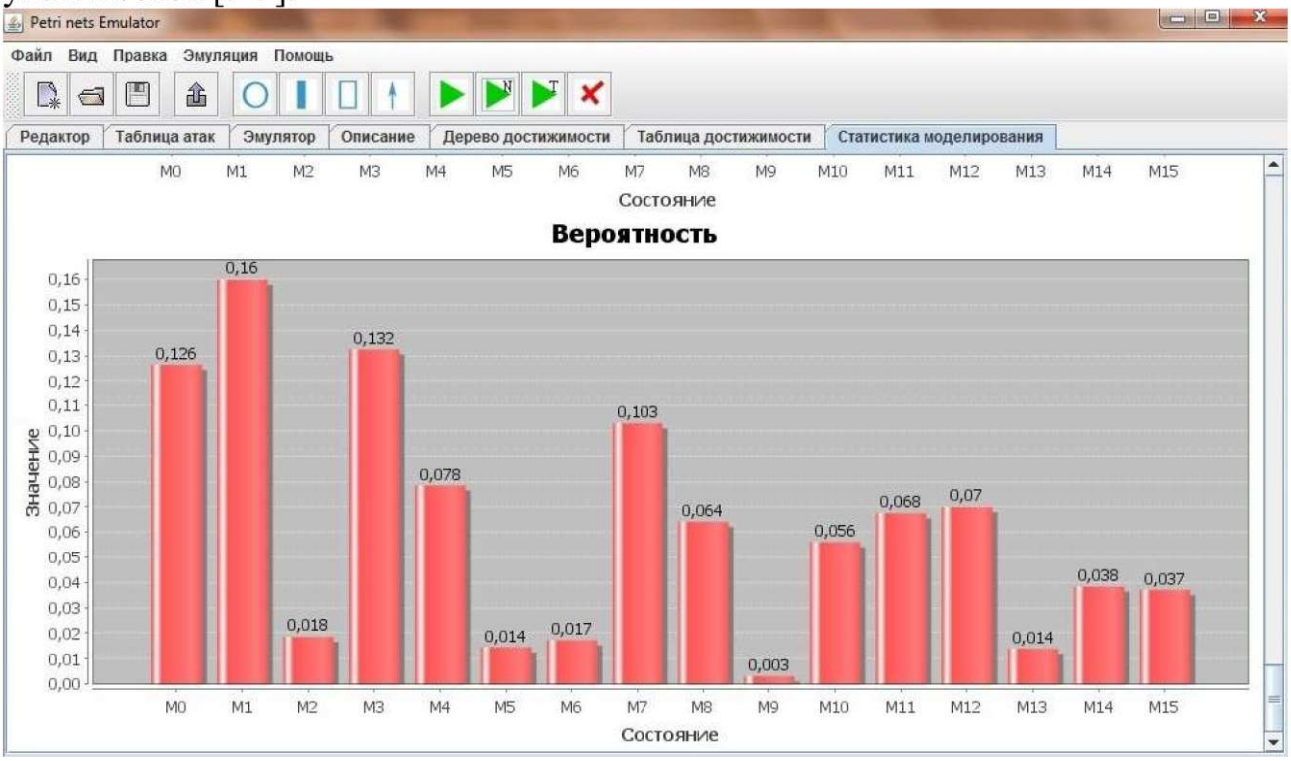

Рис. 3. Вкладка «Статистика моделирования»

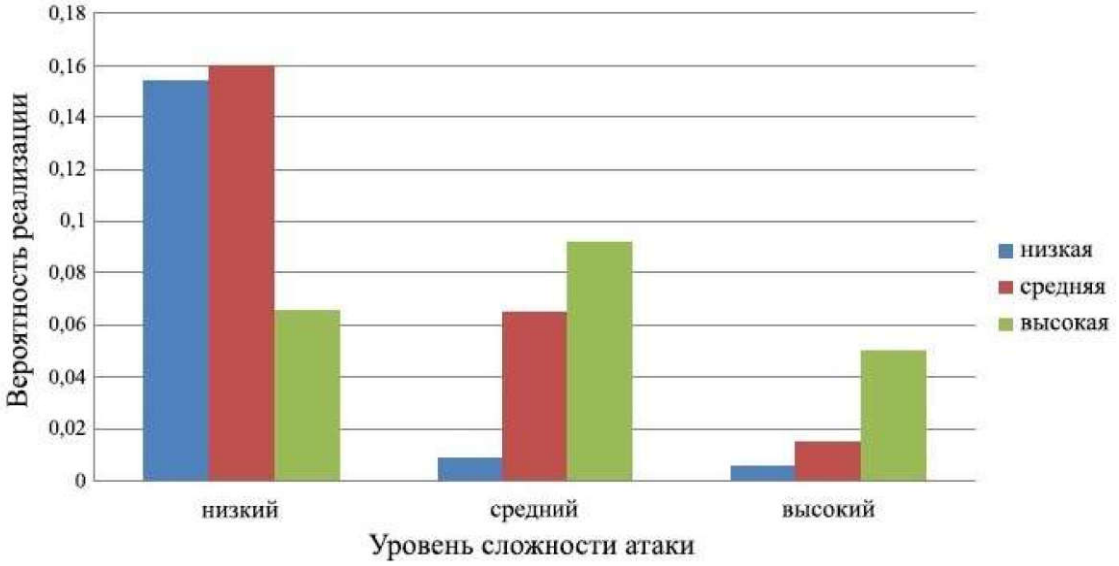

Рис. 4. Диаграмма вероятности реализации атаки в зависимости от квалификации злоумышленника

В следствии предусмотренной моделью возможности выбора злоумышленником атаки выходит так, что у злоумышленника высокой квалификации вероятность реализации атаки низкой сложности меньше, чем у менее квалифицированных злоумышленников. Это связано с тем, что деятельность профессиональных хакеров направлена в основном на получение прибыли, а атаки низкой сложности не позволяют им достичь этой цели,

поэтому проводятся намного реже и лишь в качестве вспомогательных или подготовительных действий.

Отсутствие в Petri nets Emulator сенсорной части приводит к невозможности ее проверки в качестве полноценной системы обнаружения вторжений на созданных моделях реальных атак. Поэтому развитие данных атак также было смоделировано с учетом указанных вероятностей и среднего времени работы переходов для каждой из трех возможных квалификаций злоумышленников.

Результаты моделирования с вероятностью успешной реализации представлены на рисунке 5. Диаграмма отражает вероятность успешной реализации каждой атаки, в случае если бы злоумышленник начал пробовать их реализовать в случайно выбранной целевой системе.

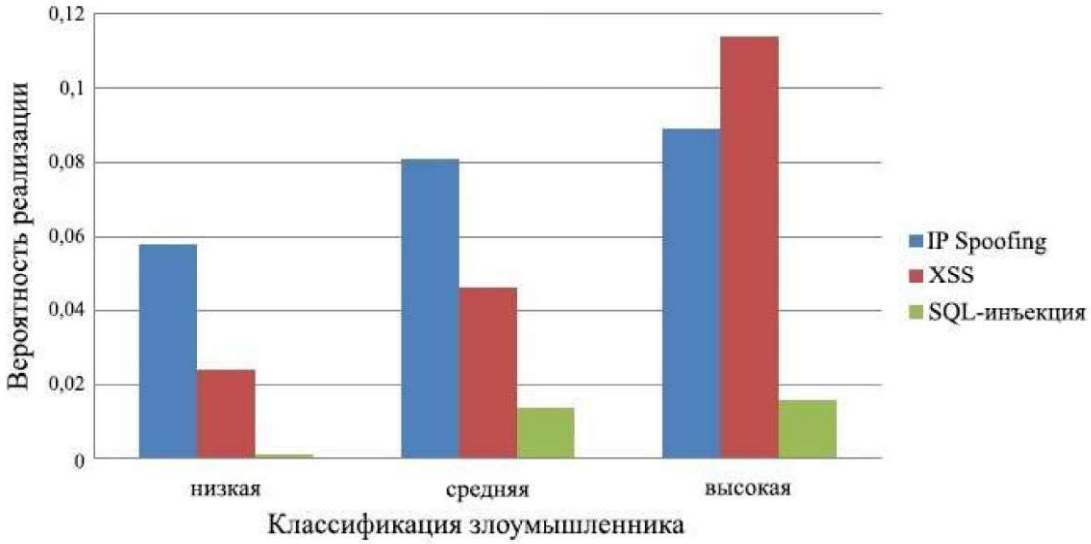

Рис. 5. Диаграмма вероятности реализации конкретных атак

Программное обеспечение Petri nets Emulator представляет собой часть системы обнаружения вторжений. В случае его дополнения сенсорами сбора информации и подсистемой преобразования до прикладного уровня, Petri nets Emulator сможет функционировать как полноценная система обнаружения вторжений.

Литература

1. Котов В.Е. Сети Петри / В.Е. Котов. – М.: Наука, 1984. – 160 с.

2. Питерсон Дж. Теория сетей Петри и моделирование систем / Дж. Питерсон. – М.: Мир, 1984. – 264 с.

3. Common Attack Pattern Enumeration and Classification (CAPEC) [Электронный ресурс]. URL: https://capec.mitre.org (дата обращения: 06.04.2020).

4. Common Vulnerabilities and Exposures (CVE) [Электронный ресурс]. URL: https://cve.mitre.org (дата обращения: 06.04.2020).

5. National Vulnerability Database [Электронный ресурс]. URL: https://nvd.nist.gov (дата обращения: 06.04.2020).