УДК 004.056

ПОДХОД К МОДЕЛИРОВАНИЮ РАСПРОСТРАНЕНИЯ СЕТЕВЫХ ЧЕРВЕЙ И АЛГОРИТМИЧЕСКОМУ ПОДБОРУ ЗАЩИТЫ НА ОСНОВЕ ГРАФОВЫХ МЕТРИК

Денисенко В.В.[1], Борисенко В.В.[1], Андрушкевич Д.В.[1]
Научный руководитель – кандидат технических наук, Андрушкевич Д.В.[1]
[1]Военно-космическая академия имени А.Ф.Можайского
vka@mil.ru

Введение

Рост автоматизации кибератак, в частности распространение сетевых червей, способных за считанные минуты охватить тысячи узлов, делает устойчивость вычислительных сетей все более зависимой от их топологической структуры. Графовые свойства сети напрямую определяют скорость распространения угроз и эффективность защитных мер. При этом существующие методы защиты, как правило, основаны на эвристических правилах или сигнатурном анализе и не учитывают топологию сети, что не позволяет обеспечивать ее структурную устойчивость. Анализ отечественной и зарубежной литературы подтверждает отсутствие универсальных количественных метрик для оценки влияния структуры сети на распространение угроз как на этапе проектирования, так и при ее эксплуатации [1]. Для преодоления этого ограничения разработан программный комплекс (ПК), реализующий графовые алгоритмы моделирования распространения атак и оценки структурной устойчивости. ПК использует метрики графа для выявления критических элементов топологии и алгоритмического подбора конфигурации защиты как при проектировании вычислительной сети, так и для повышения устойчивости действующей инфраструктуры [2].

Основная часть

Эффективность противодействия сетевым атакам повышается при алгоритмическом подборе метода защиты на основе структурных характеристик графа сети [3]. В отличие от традиционных эвристических решений, предлагаемый подход использует топологию связей для количественной оценки устойчивости и выбора оптимальной стратегии сегментации.

Цель исследования – разработать и протестировать инструмент для количественной оценки устойчивости сетевых топологий к кибератакам и автоматизированного подбора контрмер.

Программный комплекс моделирует распространение червя по принципу обхода графа в ширину (BFS): на каждом шаге заражаются все непосредственные соседи уже зараженных узлов, стартовый узел выбирается случайно. Реализованы четыре эталонные топологии (звезда, кольцо, mesh и гибридная) для размеров 20, 50, 100 и 500 узлов. Предложены два алгоритмических метода защиты:

1. сегментация сети с применением алгоритма Girvan-Newman для выявления и изоляции сообществ;
2. BFS-кластеризация, ограничивающая межуровневое заражение от критического узла.

Для каждой конфигурации выполнено по 10 независимых запусков, результаты сохранялись в SQLite-базу.

Эксперименты показали, что применение защиты замедляет полное заражение сети на 40–70%, причем эффективность методов сильно зависит от типа топологии сети:

– для mesh-топологии сегментация по алгоритму Girvan–Newman обеспечивает максимальное замедление распространения атаки;

– для звездообразных структур наиболее эффективна BFS-кластеризация при минимальном числе удаленных связей;
– гибридные топологии требуют комбинированного подхода, что подтверждает необходимость предварительного структурного анализа.

Подход позволяет формировать рекомендации с указанием ожидаемого заражения и оптимального метода защиты в зависимости от значений графовых метрик топологии.

Выводы

Исследование подтвердило, что графовые алгоритмы могут быть эффективно применены как для моделирования угроз, так и для построения адаптивной защиты. Алгоритмический подбор метода на основе структурных метрик сети обеспечивает существенно более высокие показатели замедления атаки по сравнению с универсальными эвристическими подходами [4].

Вклад работы заключается в переходе от универсальных или ручных методов сегментации к алгоритмическому выбору защиты, где тип метода и его параметры определяются объективными метриками топологии [2]. Такой подход обеспечивает структурную устойчивость сети и исключает субъективность подбора контрмер.

В дальнейшем планируется интеграция результатов моделирования с эмуляцией реальной сетевой инфраструктуры в среде EVE-NG для экспериментальной проверки предложенных методов защиты на уровне сетевого стека и оценки их влияния на производительность и задержки передачи данных.

Литература

1. Хорошко В., Хохлачова Ю., Вишневская Н. Декомпозиция технологии компьютерных сетей при их проектировании // Научный журнал по информационной безопасности – 2023.
2. Лаврова Д.С., Зегжда Д.П., Зайцева Е.А. Моделирование сетевой инфраструктуры сложных объектов для решения задачи противодействия кибератакам // Вопросы кибербезопасности. – 2019.
3. Елисеев Е.Э., Бурлаков М.Е. Применение адаптивных алгоритмов в графовых структурах при решении задач предотвращения компьютерных угроз: выпускная квалификационная работа по спец. 10.05.01 «Компьютерная безопасность». – Самара: Самарский университет, 2021. Самара: Самарский национальный исследовательский университет имени академика С. П. Королева, 2021. – URL: http://repo.ssau.ru/jspui/handle/123456789/52789 (дата обращения: 17. 01. 2026)
4. Al-Eiadeh M.R., Abdallah M. GeniGraph: A genetic-based novel security defense resource allocation method for interdependent systems modeled by attack graphs // Computers & Security. – 2024.