Секция 1. ТЕОРЕТИЧЕСКИЕ ОСНОВЫ ИНФОРМАЦИОННЫХ ТЕХНОЛОГИЙ

УДК 004.7.056.5:519.17

МАТЕМАТИЧЕСКИЕ ПОДХОДЫ К АЛГОРИТМАМ АНАЛИЗА УЯЗВИМОСТЕЙ В КОМПЬЮТЕРНЫХ СЕТЯХ

Е.В. Бегляк
Научный руководитель В.Ф. Алексеев
Белорусский государственный университет информатики и радиоэлектроники, Минск, Беларусь, evbegliak@gmail.com

В современную эпоху цифровизации и глобальной сетевой интеграции безопасность компьютерных сетей стала критически важной. Количество кибератак и их сложность увеличиваются ежегодно, что обусловлено расширением сетевых структур, возрастанием сложности инфраструктуры и использованием новых технологий, таких как IoT (Интернет вещей) и облачные сервисы.

Анализ уязвимостей является основой для построения надежной системы защиты. Он позволяет определить слабые места в сети и разработать меры по их устранению. Однако сложность сетевых структур и количество возможных уязвимостей требуют применения современных математических алгоритмов и автоматизированных инструментов [1].

Существует ряд подходов к анализу уязвимостей в сетях. Одни из них основаны на сигнатурном анализе и поиске известных шаблонов уязвимостей, другие используют эвристические и машинные методы для обнаружения новых и меняющихся угроз. Важную роль играют математические модели, которые позволяют формализовать процессы анализа уязвимостей и прогнозирования атак [2].

Важно учитывать специфику сети, объем данных и доступные ресурсы при выборе подхода для анализа уязвимостей.

Уязвимость в компьютерных сетях определяется как слабое место в архитектуре, конфигурации или реализации системы, которое может быть использовано злоумышленниками для нарушения её нормального функционирования. Уязвимости могут возникать

на различных уровнях, включая аппаратное обеспечение, программное обеспечение и сетевую инфраструктуру [3].

Основные типы уязвимостей:

– сетевые уязвимости: недостатки в настройке сетевых устройств (маршрутизаторов, коммутаторов), протоколов передачи данных или шифрования;
– программные уязвимости: ошибки в коде приложений или операционных систем, которые могут быть использованы для выполнения вредоносного кода;
– конфигурационные уязвимости: слабые пароли, неправильно настроенные права доступа или открытые порты;
– человеческий фактор: ошибки пользователей, такие как открытие фишинговых писем или использование ненадежных паролей.

Для систематического анализа уязвимостей необходимо формализовать процесс их оценки [4]. Основные этапы включают:

1. Идентификация уязвимостей: сбор информации о системе, использование автоматизированных сканеров и ручных методов анализа.

2. Классификация уязвимостей: распределение уязвимостей по уровням риска с учетом их вероятности эксплуатации и возможных последствий.

3. Моделирование угроз: построение моделей, описывающих потенциальные атаки и их последствия.

4. Разработка мер защиты: определение и реализация способов устранения или минимизации рисков.

Математические методы играют ключевую роль в анализе уязвимостей. Среди них выделяются:

1. Теория графов: позволяет анализировать топологию сети, выявлять критические узлы и пути распространения атак. Например, с помощью алгоритмов поиска минимального разреза графа можно определить наименее защищенные участки сети.

2. Теория игр: используется для моделирования взаимодействия между атакующими и защитниками. Сценарии атак и защиты формализуются как игры с нулевой суммой, что позволяет находить оптимальные стратегии.

3. Вероятностные методы: помогают оценивать вероятность успешной атаки на основе текущего состояния системы и известной информации об угрозах. Например, байесовские сети используются для моделирования зависимостей между различными уязвимостями.

4. Машинное обучение: применяется для анализа больших объемов данных, выявления аномалий и предсказания новых типов угроз. Алгоритмы классификации и кластеризации позволяют автоматизировать процесс анализа.

Несмотря на успехи в разработке математических моделей и инструментов, существуют ограничения: сложность и масштаб сетевых структур усложняют моделирование, необходимость учета динамических изменений в сети, ограниченная точность существующих методов при анализе новых угроз, высокая стоимость вычислений для сложных моделей [2]. Решение этих проблем требует дальнейших исследований и разработки более эффективных алгоритмов.

На практике анализ уязвимостей часто проводится с использованием специализированных инструментов. Наиболее популярные из них:

• **Nessus**: мощный сканер уязвимостей, который позволяет обнаруживать широкий спектр проблем, от открытых портов до ошибок конфигурации;

• **OpenVAS**: бесплатное решение для анализа уязвимостей, поддерживающее множество плагинов для проверки безопасности;

• **Metasploit**: платформа для тестирования на проникновение, которая также может использоваться для проверки уязвимостей.

Эти инструменты сочетают в себе сигнатурный анализ, эвристические методы и базы данных известных уязвимостей.

Для анализа топологии сети используются алгоритмы теории графов. Основные из них:

– *алгоритм Дейкстры* для поиска кратчайших путей в сети, что позволяет определить критические маршруты;
– *алгоритм минимального разреза* для нахождения уязвимых мест, разрыв которых может изолировать часть сети;
– *кластеризация узлов* выявляет группы устройств, которые могут быть наиболее уязвимыми для атак.

Машинное обучение активно используется для анализа сетевых данных и обнаружения аномалий [5]. Примерами таких алгоритмов являются:

• **K-means**: для кластеризации сетевых данных и выявления нетипичных паттернов;

• **Random Forest**: используется для классификации трафика и обнаружения вредоносной активности;

• **Нейронные сети**: позволяют анализировать сложные зависимости в данных и предсказывать новые угрозы.

Эффективность анализа уязвимостей повышается при использовании комбинированных подходов. Например, интеграция инструментов сканирования с алгоритмами машинного обучения для автоматического анализа данных, использование теории графов для визуализации сети и моделирования атак.

Однако на практике использование алгоритмов анализа уязвимостей может сталкиваться с такими проблемами, как необходимость настройки инструментов под конкретную инфраструктуру, высокая стоимость лицензий на коммерческие продукты, сложность интерпретации результатов автоматизированного анализа. Для успешного применения алгоритмов требуется квалифицированный персонал и четко определенные процессы управления уязвимостями.

Для успешного противодействия угрозам в компьютерных сетях необходимо регулярно проводить анализ уязвимостей с учетом последних достижений в области математики и искусственного интеллекта, адаптировать существующие алгоритмы под специфику каждой сети, а также инвестировать в исследования и разработку новых методов, которые учитывают изменения в технологиях и угрозах [4].

Реализация предложенных мер и развитие указанных направлений позволит существенно повысить уровень безопасности компьютерных сетей и снизить риски кибератак.

Список источников

1. Xarper A., Makkirnan D. Gray hat hacking: the ethical hacker's handbook. New York : McGraw-Hill [et al.], 2005. P. 268–273.
2. Щеглов А. Ю., Щеглов К. А. Математические модели и методы формального проектирования систем защиты информационных систем. Санкт-Петербург : НИУ ИТМО, 2015. 93 с.

3. Бирюков А. А. Информационная безопасность: защита и нападение. Москва : ДМК Пресс, 2023. 440 с.
4. Хромова А. Р., Петросян Л. Э. Анализ уязвимостей в системах безопасности данных // Инженерный вестник Дона. 2023. № 6. С. 67–76.
5. Практические аспекты выявления уязвимостей при проведении сертификационных испытаний программных средств защиты информации / В.В. Варенница, А. С. Марков, В. В. Савченко, В. Л. Цирлов // Вопросы кибербезопасности. 2021. № 5. С. 36–42.