УДК 004.056.5

СРАВНИТЕЛЬНЫЙ АНАЛИЗ МЕТОДОВ ОБНАРУЖЕНИЯ УЯЗВИМОСТЕЙ В КОМПЬЮТЕРНЫХ СЕТЯХ

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

С развитием информационных технологий и ростом количества подключенных к сети устройств компьютерные сети становятся все более сложными и уязвимыми к атакам. Угрозы безопасности, такие как несанкционированный доступ, кража данных и внедрение вредоносного кода, могут привести к серьезным потерям финансов и репутации. В условиях увеличивающейся сложности атак традиционные методы защиты становятся менее эффективными, что подчеркивает необходимость разработки и применения новых подходов к обнаружению уязвимостей.

Уязвимость в компьютерной сети – это слабое место в системе, которое может быть использовано злоумышленниками для получения несанкционированного доступа, нарушения работы системы или кражи данных [1]. Уязвимости могут возникать из-за ошибок в программном обеспечении, неправильной настройки оборудования или недостатков в политике безопасности.

Существующие методы обнаружения уязвимостей можно разделить на несколько категорий [2]:

Сканирование уязвимостей – автоматизированные инструменты, такие как Nessus и OpenVAS, которые проверяют системы на наличие известных уязвимостей.

Анализ сетевого трафика – мониторинг и анализ данных, передаваемых по сети, для выявления подозрительной активности.

Использование баз данных известных уязвимостей – сопоставление текущей конфигурации системы с информацией из таких баз, как CVE (Common Vulnerabilities and Exposures).

Методы на основе машинного обучения – применение алгоритмов ИИ для выявления аномалий и предсказания возможных угроз.

Каждая из этих категорий имеет свои плюсы и минусы, что делает их применение зависимым от конкретного сценария и требований безопасности.

Рассмотрим основные методы обнаружения уязвимостей компьютерных сетей:

– ручная проверка уязвимостей включает анализ системы специалистами по безопасности. Этот метод предполагает детальное изучение конфигураций, кодов и архитектуры сетевых приложений. Хотя он требует значительных временных затрат и высококвалифицированных специалистов, ручная проверка позволяет выявить сложные уязвимости, которые могут быть пропущены автоматизированными инструментами. Однако этот метод не может обеспечить полное покрытие всех возможных уязвимостей из-за человеческого фактора и ограниченного времени;

– сканеры безопасности – это автоматизированные инструменты, которые позволяют быстро и эффективно обнаруживать уязвимости в системах и приложениях. Они работают путем отправки запросов к целевой системе и анализа ответов для выявления слабых мест [3]. Сканеры могут быть как активными, так и пассивными. Активные сканеры взаимодействуют с системой, а пассивные анализируют трафик без вмешательства. Несмотря на свою эффективность, сканеры могут не всегда обнаруживать сложные уязвимости и требуют регулярного обновления баз данных угроз;

– анализ сетевого трафика включает мониторинг и анализ данных, передаваемых по сети. Этот метод позволяет выявлять аномалии и подозрительное поведение, которые могут указывать на наличие уязвимостей или атак [1]. Использование технологий глубокого анализа пакетов (DPI) помогает детально исследовать содержимое передаваемых данных. Однако данный метод требует значительных ресурсов и может быть затруднен шифрованием трафика;

– машинное обучение (ML) становится все более популярным в области обнаружения уязвимостей благодаря своей способности выявлять паттерны и аномалии в больших объемах данных. Алгоритмы ML могут обучаться на исторических данных о атаках и уязвимостях, что позволяет им предсказывать возможные угрозы в реальном времени [4]. Однако эффективность машинного обучения зависит от качества обучающих данных и может быть подвержена ошибкам;

– системы анализа больших данных (Big Data) позволяют обрабатывать огромные объемы информации из различных источников, включая журналы событий, сетевой трафик и данные о пользователях. Эти системы помогают выявлять сложные взаимосвязи между данными и потенциальными угрозами. Использование технологий Hadoop и Spark позволяет быстро обрабатывать данные и извлекать из них полезную информацию для обнаружения уязвимостей;

– искусственный интеллект (AI) используется для автоматизации процессов обнаружения уязвимостей и повышения их точности. AI может анализировать данные из различных источников, обучаться на примерах атак и предлагать рекомендации по устранению уязвимостей [4]. Однако внедрение AI требует значительных ресурсов и может столкнуться с проблемами интерпретируемости результатов.

Для проведения сравнительного анализа методов обнаружения уязвимостей были выбраны ключевые критерии, такие как: способность метода корректно выявлять уязвимости без ложных срабатываний (точность); время, необходимое для анализа сети (сложность реализации); способность метода адаптироваться к новым угрозам (обновляемость); возможность применения метода в больших сетях (масштабируемость).

Сравнительный анализ показывает (табл. 1), что традиционные методы, такие как ручная проверка и использование сканеров без-

опасности, остаются важными инструментами, особенно для детального анализа или быстрого выявления известных уязвимостей. Однако они уступают современным подходам, таким как машинное обучение и анализ больших данных, в аспектах точности, адаптивности и масштабируемости.

Сравнение методов обнаружения уязвимостей

Критерий	Ручная проверка	Сканеры безопасности	Анализ сетевого трафика	Машинное обучение	Анализ больших данных
Точность	Высокая	Средняя	Средняя	Высокая	Высокая
Скорость	Низкая	Высокая	Средняя	Высокая	Средняя
Сложность реализации	Высокая	Низкая	Средняя	Высокая	Высокая
Обновляемость	Низкая	Средняя	Средняя	Высокая	Высокая
Масштабируемость	Низкая	Средняя	Средняя	Высокая	Высокая

Машинное обучение демонстрирует наилучшие результаты в обнаружении новых угроз благодаря своей способности обучаться и адаптироваться к меняющимся условиям. Анализ больших данных обеспечивает возможность обработки огромных объемов информации [4], что делает его незаменимым для крупных организаций. При этом выбор метода зависит от конкретных задач и ресурсов организации.

Современный подход, такой как интеграция аналитики больших данных, обеспечивает дополнительные уровни безопасности в компьютерных сетях, позволяя минимизировать человеческий фактор и повышать надежность систем. Но внедрение связано с высокими затратами и техническими вызовами, что требует взвешенного подхода к выбору методов в зависимости от задач и возможностей организации.

Методы обнаружения уязвимостей активно применяются в различных отраслях и сценариях, например, таких, как корпоративные сети, облачные сети, электронная коммерция и т. д. Однако, несмотря на широкое применение, эти методы сталкиваются с рядом ограничений в виде ложных срабатываний, высокой стоимости внедрения, эволюции угроз, нарушении конфиденциальных данных, сложности интеграции.

В условиях стремительного роста сложности и масштабов компьютерных сетей вопросы обеспечения их безопасности становятся приоритетными. Уязвимости в сетях представляют собой значительные риски для организаций и пользователей, что требует постоянного совершенствования методов их обнаружения [1].

Таким образом, для обеспечения надежной защиты компьютерных сетей необходим комплексный подход, сочетающий несколько методов. Внедрение инновационных технологий в практику безопасности позволит не только оперативно выявлять уязвимости, но и предвидеть появление новых угроз, создавая условия для устойчивого развития цифровой инфраструктуры.

Список источников

1. Олифер В., Олифер Н. Компьютерные сети. Принципы, технологии, протоколы. Санкт-Петербург : Питер, 2024. 1008 с.
2. Kali Linux : тестирование на проникновение и безопасность / Ш. Парасрам, А. Замм, Т. Хериянто [и др.] ; пер. с англ. А. Гераськенко. 4-е изд. Санкт-Петербург [и др.] : Питер, 2020. 446 с.
3. Синадский Н. И., Хорьков Д. А. Защита информации в компьютерных сетях : учеб. пособие. Екатеринбург : УрГУ, 2008. 225 с.
4. Чио К., Фримен Д. Машинное обучение и безопасность. Москва : ДМК-Пресс, 2020. 388 с.