В. Л. Шарова
(ГГУ имени Ф. Скорины, Гомель)
Науч. рук. **О. В. Дегтярева**, ст. преподаватель

ОБЗОР МЕТОДОВ АНАЛИЗА СЕТЕВОГО ТРАФИКА

Большие объёмы конфиденциальной информации хранятся на компьютерах и серверах, подключённых к локальной и внешней сети, что потенциально создаёт угрозу компрометации. Каждая организация принимает меры по обеспечению защиты своих данных, однако с каждым днём количество разновидностей атак и угроз увеличивается, и разработчики не успевают создавать обновления и программы, которые бы в полной мере защищали системы информации. Поэтому важной ступенью в обеспечении защиты информации является проведение мониторинга и анализа сетевого трафика с целью своевременного обнаружения угроз и уязвимостей и последующего устранения их во избежание попадания в систему злоумышленников, кражи и модификации данных.

Анализ сетевого трафика – это метод мониторинга сети, осуществляющийся посредством перехвата трафика и последующего его изучения с целью выявления в нём аномалий. Аномалиями можно считать подозрительную сетевую активность, к которой относятся сканирование локальной сети, попытки подбора пароля, сокрытие сетевого трафика, попытки удалённого запуска программ и приложений, передача нетипично больших объёмов данных. Такая активность может указывать как на сбой в работе системы, так и на неправомерное использование ресурсов или проведение кибератаки. Поэтому крайне важно отслеживать сетевой трафик для раннего выявления угроз и своевременного реагирования на них.

Традиционным способом анализа считается использование статистических методов. Статистический метод подразумевает собой сбор данных, их изучение, установление закономерностей и связей, выявление отклонений от «нормы». В основе этих методов зачастую лежат математические модели, такие как марковская модель, временные ряды, фрактальное броуновское движение. Несмотря на подтверждённую эффективность в других отраслях, в информационной безопасности данный способ анализа имеет свои недостатки: свойственные шумы в данных могут неправильно интерпретироваться, что негативно сказывается на точности обработки трафика; изменения в динамичном трафике не всегда учитываются используемой моделью, поэтому необходима предобработка данных, что влечёт за собой увеличение ресурсо- и трудозатрат. Для оптимизации анализа можно использовать специальные интеллектуальные системы – обучаемые математические модели для обработки информации, которые автоматически смогут распознавать атаки и угрозы [1].

В настоящее время уже существуют более узконаправленные способы исследования сетевого трафика. Они разделяются на использование аппаратных и программных анализаторов, систем обнаружения вторжений, DPI-решения. Аппаратный анализатор представляет собой отдельное физическое устройство, в которое зашит сложный программно-аппаратный комплекс, предназначенный для захвата и анализа сетевого трафика. С помощью такого прибора специалист мониторинга может исследовать проводные и беспроводные сети, отслеживать какие устройства и типы программ больше остальных нагружают полосу пропускания, проверять наличие запрещённого трафика в сети. В зависимости от конфигураций аппаратные анализаторы могут подключаться как напрямую к маршрутизатору, так и к любой точке сети [2].

Программные анализаторы – это программы и программное обеспечение, разработанные для анализа сетевого трафика. Такие программы пользуются большой популярностью за счёт своей практичности, эффективности и наличия понятного интерфейса. В большинстве своём подобные программы находятся в открытом доступе

для бесплатного скачивания и имеют графический интерфейс для удобной работы. Программные анализаторы позволяют захватывать сетевой трафик для ретроспективного анализа, а также могут работать в режиме реального времени. С их помощью специалисты могут фильтровать трафик, просматривать сетевую активность, статистику производительности сети и контролировать подключения к ней. Примерами таких программ являются Wireshark, Tcpdump, Kismet, EtherApe.

Для детального анализа сетевого трафика можно применять технологию DPI (Deep Packet Inspection). Эта технология глубокой проверки пакетов данных по заголовкам и полезной нагрузке помогает фильтровать трафик, регулировать нагрузку на сеть, выявлять несанкционированный доступ к сети и останавливать распространение вредоносного программного обеспечения. DPI-решения можно интегрировать в аппаратные анализаторы.

Наиболее автоматизированной программой анализа сетевого трафика является система обнаружения вторжений (IDS). IDS представляет собой совокупность программных средств для анализа трафика, обнаружения несанкционированных действий и реагирования на них. Такая система собирает логи с журналов событий операционной системы и анализирует их. У неё есть два метода обнаружения угроз: поведенческий и интеллектуальный. Поведенческий метод подразумевает работу с информацией о нормальном поведении системы, а интеллектуальный анализ использует информацию об известных атаках. IDS не устраняют угрозы безопасности самостоятельно, а лишь отправляют уведомление о них пользователю программы.

Развитие информационных технологий способствует появлению и усовершенствованию систем и методов анализа сетевого трафика, что позволяет на ранних этапах выявить несанкционированные действия в сети, предотвратить компрометацию данных и распространение вредоносного программного обеспечения.

Литература

1. Гладких, А. М. Основные методы анализа сетевого трафика / А. М. Гладких // М. : Вопросы науки и образования, 2020. – М. : МГТУ им. Н. Э. Баумана, 2020. – 52 с.

2. Выбор анализатора сетевого трафика, производительности сети и приложений [Электронный ресурс]. – Режим доступа: https://skomplekt.com/vybor_analizatora_setevogo_trafika_proizvoditelnosti_seti_i_prilozhenij/. – Дата доступа : 25.03.2025