УДК 004.56

СРАВНЕНИЕ ТЕХНИЧЕСКИХ РЕШЕНИЙ ЗАЩИТЫ ОТ АТАК КЛАССА "ОТКАЗ В ОБСЛУЖИВАНИИ"

Кашицин Н.О. (Университет ИТМО), **Гатчин Ю.А.** (Университет ИТМО), **Глебов Р.Г.** (Университет ИТМО), **Левкович С.С** (Университет ИТМО)
Научный руководитель – д.т.н., профессор Гатчин Ю.А.
(**Университет ИТМО**)

В статье рассматриваются вопросы, которые относятся к защите информации от атак класса "отказ в обслуживании". Основная задача статьи изучить рынок программно-аппаратных средств анализа сетевого трафика (далее ПАСАСТ). Проанализировать имеющиеся на это рынке решения - выявить отрицательные и положительные свойства каждого средства.

Современный человек потребляет 34 ГБ медийного контента в день. Поэтому даже не стоит говорить о том, сколько информации протекает в небольшой организации за месяц. Растёт не только объём информации, но и системы хранения и распределения этой информации, а также средства взлома и защиты различных информационных потоков. Отследить данную тенденцию можно по росту объемов накопителей информации. Временная дестабилизация сети информации является одним из наиболее распространённых элементов вредительства у злоумышленников. По данным Лаборатории Касперского второй квартал 2019 года оказался богаче предыдущего на громкие DDoS-атаки. Правда, большинство кампаний, ставших объектами внимания СМИ, по всей видимости, имели политический, а не коммерческий подтекст, несмотря на то что некоторые специалисты по безопасности отмечают явный спад хактивизма в последние годы. Однако стоит заметить, что, например, по информации сайта РБК количество DDoS-атак на онлайн-кассы выросло на 836%, что позволят нам говорить о том, что данный рынок всё ещё стабилен и продолжает «идти в ногу со временем». Вливаясь во все сферы нашей жизни, использующие так или иначе широковещательные каналы информации.

Поэтому было предложено провести исследование программно-аппаратных решений защиты от атак класса "отказ в обслуживании" по нескольким критериям. Исходя из представленной информации, можно сделать заключение, что анализ сетевого трафика может быть использован и используется для предотвращения путей хищения информации. Благодаря этим знаниям, можно определить, на каком уровне OSI можно исследовать трафик, а также определить, куда и в каком виде уходит информация. В связи с тем, что в основе всех перечисленных продуктов, используется стек протоколов TCP/IP, необходимо отметить тот факт, что в нём также реализована защита от потери важных данных за счёт использования протоколов защиты данных, передача которых осуществляется по межсетевому протоколу IP, реализованная в IP Security. На других уровнях это обеспечивается другими методами, например, на уровне сессии применяется шифрование трафика при помощи TLS протокола.

Из приведённого обзора можно сделать вывод о том, что в связи с прорывным скачком в росте предоставляемого провайдерами трафика, а также увеличением новых прикладных задач, растёт и проблема защиты информации в открытых информационных сетях. Это порождает рост потребности в анализе трафика. Результаты анализа можно использовать для защиты информации. При этом, несмотря на огромное многообразие конкретных решений, реализующих различные виды анализа, в их основе лежит примерно одинаковая схема, что хорошо видно на примере внедрения концепции «DPI как сервис». В связи с этим открывается огромное поле для изучения этой темы.

Кашицин Н.О. (автор)

Гатчин Ю.А. (научный руководитель)