DOI 10.37882/2223–2966.2020.08.05

# ОБНАРУЖЕНИЕ АНОМАЛИЙ СЕТЕВОГО ТРАФИКА: ОСНОВНЫЕ АСПЕКТЫ, ПРОБЛЕМЫ И МЕТОДЫ

## DETECTING NETWORK TRAFFIC ANOMALIES: MAIN ASPECTS, PROBLEMS AND METHODS

***M. Budko***
***A. Malko***
***D. Starodubova***
***R. Starodubov***

*Summary.* Solving the issue of detecting network traffic anomalies is an important aspect of monitoring the operation of a computer network and ensuring a high level of its security. The purpose of this work is to categorize the sources and causes of anomalies, as well as the most promising methods for detecting them, based on modern research of the problem. The result of this work is a generalized classification of sources of network traffic anomalies and the main methods for detecting them.

*Keywords:* information security; anomalies; network traffic analysis; information protection; computer networks; intrusion detection.

***Будько Марина Борисовна***
*К.т.н., доцент, Университет телекоммуникаций, механики и оптики, г. Санкт-Петербург*
***Малько Алексей Дмитриевич***
*Аспирант, Университет телекоммуникаций, механики и оптики, г. Санкт-Петербург*
***Стародубова Дарья Дмитриевна***
*Независимый исследователь, г. Санкт-Петербург*
***Стародубов Роман Дмитриевич***
*Санкт-петербургский государственный университет телекоммуникаций им. проф. Бонч-Бруевича, г. Санкт-Петербург*
*starodubova.95@mail.ru*

*Аннотация.* Решение вопроса обнаружения аномалий сетевого трафика является важным аспектом мониторинга работы компьютерной сети и обеспечения высокого уровня ее защищенности. Цель настоящей работы — на основе современных исследований проблемы произвести категоризацию источников и причин возникновения аномалий, а также наиболее перспективных методов их детектирования. Результатом работы являются обобщенные классификации источников аномалий сетевого трафика и основных методов их обнаружения.

*Ключевые слова:* информационная безопасность; аномалии; анализ сетевого трафика; защита информации; компьютерные сети; обнаружение вторжений.

На сегодняшний день вопрос обеспечения высокого уровня информационной безопасности большинства организаций включает в себя решение проблемы обнаружения и предотвращения неправомерных действий, осуществляемых внутри защищенного периметра локальной сети. Согласно ежегодному отчёту "Cyber Security Report 2020" компании Check Point Software Technologies, по статистике 34% всех кибератак совершаются инсайдерами, что демонстрирует необходимость внедрения систем сетевой безопасности, способных обнаруживать подобные атаки и противодействовать им за минимально приемлемое время [5, с. 59–65].

Одним из наиболее перспективных методов идентификации атак внутри телекоммуникационной сети организации является обнаружение аномалий сетевого трафика, позволяющее выявлять общеизвестные злонамеренные действия пользователей или машин, в том числе и «атаки нулевого дня». В общем случае «аномалия» — это отклонение от нормы, нарушение закономерности. Важно понимать, что не каждая аномалия в сетевом трафике представляет собой угрозу информационной безопасности, и для повышения точности определения неправомерных действий внутри защищенного периметра сети необходимо учитывать множество факторов: источники и причины возникновения сетевых аномалий, количество аномалий и их потенциальную связь между собой, процесс преобразования зарегистрированных аномалий сетевого трафика в событие информационной безопасности [1, с. 180–182].

Изучение вопроса обнаружения сетевых аномалий в первую очередь требует обозначения основных источников аномальных событий. Любая корпоративная сетевая инфраструктура включает в себя множество составляющих, функционирующих независимо или взаимодействующих между собой, и каждый из этих компонентов является потенциальным источником сетевых аномалий. Полное перечисление всех возможных первоисточников аномалий сетевого трафика является сложной задачей, в связи с чем на основании работ [4,

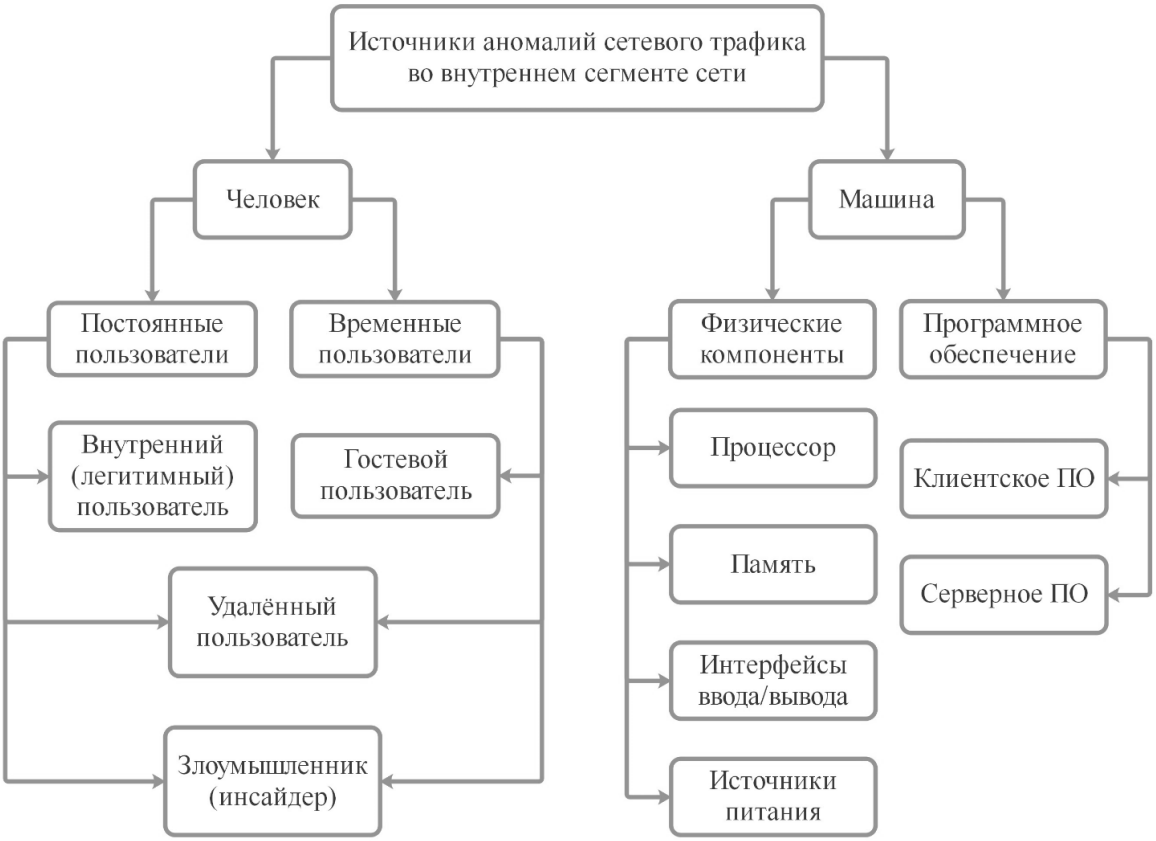


Рис. 1. Классификация потенциальных источников сетевых аномалий внутреннего сегмента корпоративной сети

с. 323–328; 7, с. 5–27, 9, с. 305–306] в целях визуальной демонстрации была разработана обобщенная классификация потенциальных источников аномалий во внутреннем сегменте корпоративной сети, представленная на рисунке 1.

Как видно из рисунка 1, глобально источники сетевых аномалий можно разделить на пользовательские и машинные. Первой категорией являются пользователи внутреннего сегмента сети, которые могут подразделяться на постоянных — являться сотрудниками организации, владеющей сетью, и временных — привлекаемых для решения краткосрочных задач. Удаленные сотрудники и потенциальные злоумышленники могут быть как постоянными пользователями, так и временными, и должны быть обязательно учтены при общем описании потенциальных источников аномалий сетевого трафика. Второй категорией являются машинные источники, которые представляют собой физические компоненты, такие как процессор, память, интерфейсы ввода/вывода и источники питания, и программное обеспечение (ПО), обычно подразделяемое на клиентское и серверное. Перечисленные физическое компоненты и категории ПО являются основными составляющими всех элементов компьютерной сети, таких как пользовательские компьютеры, серверы, средства защиты и мониторинга. Таким образом, каждое устройство в компьютерной сети включает в себя сразу несколько потенциальных источников аномалий сетевого трафика. Стоит отметить, что источники могут быть как независимыми при генерации аномалий, так и непосредственно влиять на возникновение аномального трафика со стороны других перечисленных источников.

Помимо описания основных источников, важным аспектом изучения проблемы аномалий в сетевом трафике является исследование причин их появления в компьютерной сети. В соответствии с [10, с. 39–42] можно выделить следующие две категории причин возникновения сетевых аномалий: аномалии, связанные с производительностью — причинами появления аномалий данной категории могут быть ошибки проектирования аппаратных и программным составляющих систем, износ физических компонентов, некорректные внедрение, конфигурация, использование и администрирование составляющих компьютерной сети, а также особенности работы телекоммуникационных систем, которые не могут быть исправлены программными средствами;


Рис. 2. Основные методы обнаружения аномалий в сетевом трафике

аномалии, связанные с безопасностью — в этой категории причинами возникновения сетевых аномалий служит использование уязвимостей аппаратного или программного обеспечения, недостаточная настройка средств защиты и мониторинга сети, ошибки в политике безопасности организации, что позволяет пользователям и злоумышленникам совершать неправомерные или непредусмотренные политикой действия во внутреннем защищенном периметре сети.

Авторы [9, с. 307–308] подразделяют аномалии сетевого трафика на следующие типы: точечная аномалия — представляет собой экземпляр информации, который является аномальным по отношению к остальному объему данных; контекстуальная аномалия — данные являются аномальными в конкретном контексте, определяемом с помощью контекстных и поведенческих атрибутов для непосредственного набора данных; коллективная аномалия — набор связанных экземпляров данных, которые являются аномальными по отношению ко всему объему данных, при этом события, входящие в набор, могут не быть аномальными если они происходят независимо друг от друга.

Для решения проблемы обнаружения аномалий в компьютерных сетях средства мониторинга и защиты используют модель «нормального сетевого трафика», которая фиксирует основные взаимодействия между компонентами телекоммуникационной сети. В такой модели событие считается аномалией в случае, если показатель отклонения относительно профиля системы, построенного на основании нормального функционирования сети, превышает допустимое пороговое значение. Большинство систем обнаружения аномалий включают в себя модуль моделирования, который отвечает за построение нормального профиля функционирования сети, и модуль обнаружения, выявляющий аномалии сетевого трафика, в простейшем случае через определение показателя девиации события относительно профиля нормальных взаимодействий и степени его критичности. Модуль обнаружения обычно проектируется адаптивным, с целью обнаружения аномалий без сопоставления с конкретным шаблоном [8, с. 251–253, 10, с. 46–56].

Основные методы обнаружения сетевых аномалий, описанные в работах [2, с. 214–215; 3, с. 11–15; 7,

с. 80–209], могут быть сформированы в виде схемы, приведенной на рисунке 2. Данная схема демонстрирует классы методов обнаружения аномалий, используемые в современных системах защиты и мониторинга, а также активно изучаемые и перспективные технологии детектирования аномальных выбросов в трафике. Необходимо понимать, что все перечисленные методики обнаружения успешно выполняют свои функции исключительно в определенных сценариях, и ни один из методов нельзя считать лучшим решением для всех возможных вариантов работы. Это связано с постоянными изменениями характера трафика в реальной сети, а также с непосредственной точкой развертывания системы обнаружения аномалий внутри периметра компьютерной сети.

Статистические методы работают хорошо в случаях, когда прогнозируемая модель строится на основе наблюдения трафика в реальном времени. Проблемой является получение функции плотности и поиск оптимальных значений используемых параметров. В случаях использования классификации, кластеризации или методы, основанных на выбросах, определение подходящего подмножества признаков в большом многомерном наборе данных является дорогостоящим и трудоемким. Помимо этого, обучение является критически важным для построения системы, которая обнаруживает аномалии в сетевом трафике, и оно обычно предполагает высокие трудозатраты. Методы, основанные на знаниях, создают базу данных правил на основе существующей информации об атаках, а затем обнаруживают аномалии в соответствии с конкретным набором правил. Создание оптимальной и непротиворечивой базы правил является сложной задачей с учетом широкого спектра источников и причин аномалий, а также различных типов атак. Методы мягких вычислений применяются, когда идентификация элемента сетевого трафика как аномального или нормального не определена. Использование методов машинного обучения и нейронных сетей для классификации элементов сетевого трафика как аномальных или нормальных позволяет принимать решения в неопределенных ситуациях. Данные методы являются наиболее перспективными и актуальными для изучения в рамках решения проблемы детектирования аномалий. Методы с комбинированным обучением объединяют в себе различные технологии и методики обнаружения аномалий в единой системе на разных уровнях. Такие методы отличаются своей сложностью в проектировании и реализации, и, как правило, не подходят для обнаружения аномалий сетевого трафика в реальном времени [6, с. 343–351; 10, с. 115–160].

Таким образом, изучение и решение проблемы обнаружения аномалий в сетевом трафике является важным элементом организации стабильного и безопасного функционирования любой телекоммуникационной сети. Описанные источники и причины возникновения сетевых аномалий, а также анализ существующих методов их обнаружения дополняют существующие исследования теории детектирования сетевых аномалий.

ЛИТЕРАТУРА


1. Бондарев, В. В. Анализ защищенности и мониторинг компьютерных сетей. Методы и средства: учебное пособие / В. В. Бондарев.— М.: Издательство МГТУ им. Н. Э. Баумана, 2017.— 225 с.: ил.;
2. Браницкий, А. А. Анализ и классификация методов обнаружения сетевых атак / А. А. Браницкий, И. В. Котенко // Труды СПИИРАН.— 2016.— Т. 2, № 45.— с. 207–244.;
3. Кондратьев, А. А. Методологическое обеспечение интеллектуальных систем защиты от сетевых атак / А. А. Кондратьев, А. А. Талалаев, И. П. Тищенко, В. П. Фраленко, В. М. Хачумов // Современные проблемы науки и образования.— 2014.— № 2.;
4. Олифер, В. Г. Безопасность компьютерных сетей / В. Г. Олифер, Н. А. Олифер.— М.: Горячая линия-Телеком, 2016, 644 с.;
5. Отчет компании Check Point Software Technologies «Cyber Security Report 2020.»,— 80 с.;
6. Шаньгин, В. Ф. Информационная безопасность компьютерных систем и сетей / В. Ф. Шаньгин.— М.: ИД «Форум»,: ИНФРА-М, 2011.— 416 с.;
7. Шелухин, О. И. Обнаружение вторжений в компьютерные сети (сетевые аномалии): учеб. пособие / Д. Ж. Сакалема, А. С. Филинова, О. И. Шелухин.— М.: Горячая линия — Телеком, 2013.— 221 с.: ил.;
8. Li, H. Research on intelligent intrusion prevention system based on snort / H. Li, D. Liu // In Proceedings of the 2010 International Conference on Computer, Mechatronics, Control and Electronic Engineering (CMCE), V.-1,— IEEE. 2010,— pp. 251–253.;
9. Monowar, H. B. Network Anomaly Detection: Methods, Systems and Tools / Monovar H. Bhuyan, Dhruba. K. Bhattacharyya, Jugal K. Kalita // IEEE Communication Surveys & Tutorials, Vol. 16, No. 1, 2014,— pp. 303–336;
10. Monowar, H. B. Network Traffic Anomaly Detection and Prevention. Concepts, Techniques, and Tools / Monovar H. Bhuyan, Dhruba. K. Bhattacharyya, Jugal K. Kalita // Springer International Publishing, 2017,— 285 p.