УДК 658.5.012.7

ОБЗОР МЕТОДОВ КЛАССИФИКАЦИИ СЕТЕВЫХ ТРАФИКОВ

Пономарева Ольга Алексеевна, доцент, кандидат технических наук, Учебно-научный центр «Информационная безопасность», Уральский федеральный университет имени первого Президента России Б.Н. Ельцина

Чистяков Максим Владимирович, магистрант, Учебно-научный центр «Информационная безопасность», Уральский федеральный университет имени первого Президента России Б.Н. Ельцина

Грибов Михаил Андреевич, магистрант, Учебно-научный центр «Информационная безопасность», Уральский федеральный университет имени первого Президента России Б.Н. Ельцина

Барыбин Дмитрий Александрович, магистрант, Учебно-научный центр «Информационная безопасность», Уральский федеральный университет имени первого Президента России Б.Н. Ельцина

Аннотация

В статье проведено исследование влияния составляющих трафика на информационную безопасность. Цель исследования – выявить зависимость компонент трафика от действий оператора автоматизированного рабочего места. Методика исследования – аналитическая. В качестве главных результатов выделяется научно обоснованное предложение о делении трафика на три типа по критерию безопасности и обоснование связанности типа трафика от действий оператора автоматизированного рабочего места. В статье сделан акцент на конкретизацию терминов и определений, затрагивающих понятие «трафик». Кратко упомянуты процессы, происходящие в иерархии эталонной модели взаимодействия открытых систем (ЭМ ВОЗ).

КЛЮЧЕВЫЕ СЛОВА: трафик, интернет, клиент, сервер, инфокоммуникационная среда, защита, генератор трафика.

OVERVIEW OF NETWORK TRAFFIC CLASSIFICATION METHODS

Ponomareva Olga Alexeevna, Associate Professor, Candidate of Sciences (Engineering), Educational and Research Center “Information Security”, Ural Federal University named after the first President of Russia B.N. Yeltsin

Chistyakov Maxim Vladimirovich, Master's Student, Educational and Research Center “Information Security”, Ural Federal University named after the first President of Russia B.N. Yeltsin

Gribov Mikhail Andreevich, Master's Student, Educational and Research Center “Information Security”, Ural Federal University named after the first President of Russia B.N. Yeltsin

Barybin Dmitry Alexandrovich, Master's Student, Educational and Research Center “Information Security”, Ural Federal University named after the first President of Russia B.N. Yeltsin

Abstract

The article studies the influence of traffic components on information security. The purpose of the study is to identify the dependence of traffic components on the actions of the automated workplace operator. The research methodology is analytical. The main results include a scientifically substantiated proposal to divide traffic into three types according to the security criterion and justification for the relationship of the traffic type to the actions of the automated workplace operator. The article focuses on specifying the terms and definitions affecting the concept of "traffic". The processes occurring in the hierarchy of the reference model of open systems interaction (RM OSI) are briefly mentioned.

KEYWORDS: traffic, internet, client, server, infocommunication environment, protection, traffic generator.

Введение

Развитие информационных технологий требует обеспечения информационной безопасности. Угрозы могут возникать как из вне, так и изнутри организации. Реализация угроз возможна как при удаленном взаимодействии с элементами системы, так и локально.

Высокий уровень развития телекоммуникационных систем и сетей обеспечивается развитием технологий передачи и обработки информации. Эволюция сетей и услуг связи наиболее ярко выражается в слиянии этих технологий. Процесс развития методов анализа и построения телекоммуникационных систем являются неотъемлемой частью этого процесса. Телекоммуникационные сети являются неотъемлемым частью нашей современной жизни. От работоспособности этих сетей зависят практически все процессы и отношения в обществе, во всех сферах деятельности человека. Поэтому предъявляются особые требования к состоянию сетей связи и их уровню развития.

С развитием в нашем обществе разнообразных услуг, предоставляемых в глобальной сети «Интернет», создается материальную базу для создания современных телекоммуникационных сетевых технологий с широкими возможностями. В связи с этим возрастают требования к качеству функционирования телекоммуникационных сетей, их безопасности и надежности. С ростом количества и качеством предоставления услуг в глобальной сети «Интернет», необходимо перераспределение трафика в телекоммуникационных сетях общего пользования, что оказывает влияние на качество обслуживания и доходы операторов связи. Необходимо развивать методы анализа, высокие темпы развития технологий и услуг, а также планирование и проектирования современных телекоммуникационных систем. Производительность телекоммуникационных сетей зависят от многих параметров, таких как: пропускная способность коммутационных интерфейсов и задержки в сети. При проектировании телекоммуникационных сетей в основном внимание уделяется к пропускной способности интерфейсов, но задержки при передаче информации в трафике, могут существенно влиять на общую эффективность телекоммуникационной сети. Буферизация информации в конечных и транзитных узлах телекоммуникационного оборудования является одной из причин появления задержек. Для определения эффективного размера буферной памяти необходимо учитывать характер трафика, поступающего из сети. Сложность в выборе телекоммуникационного оборудования создают его разработчики и производители, которые скрывают информацию об технических параметрах и используемых внутренних компонентах из-за коммерческой тайны.

Трафик играет ключевую роль в работоспособности телекоммуникационных сетей, потому что он напрямую влияет на её скорость, надёжность и масштабируемость. Если рассматривать трафик как поток данных, то необходимо анализировать интенсивность запросов или пакетов данных, в системах с низким траффиком все работает гладко: ресурсы (процессоры, память, bandwidth) справляются без проблем.

Высокий спрос на услуги в глобальной сети «Интернет», опережает развитие технологий передачи данных в локальных и глобальных телекоммуникационных сетях. Поэтому требуется постоянно модернизировать и оптимизировать существующее телекоммуникационное оборудование, с целью увеличения безопасности, надежности и производительности телекоммуникационной сети.

В статье рассматривается клиент-серверная модель, по-прежнему являющаяся основной формой взаимодействия структурных элементов глобальной сети «Интернет», которая состоит из специфических компонентов. Она заключается в обращении к какому-либо интерфейсу. После очередного эволюционного этапа в инфокоммуникационных технологиях (выпуск в массы операционных систем Android, IOs, появление систем моментального обмена сообщениями или мессенджеров) пользователь сети реализует свои информационные потребности (поиск информации, оплата услуг, покупка товаров и др.) непосредственно со своего мобильного или стационарного устройства [1, С. 51-57]. На Рисунке 1 приведена иллюстрация взаимодействия пользователей в инфокоммуникационной среде сегодня.

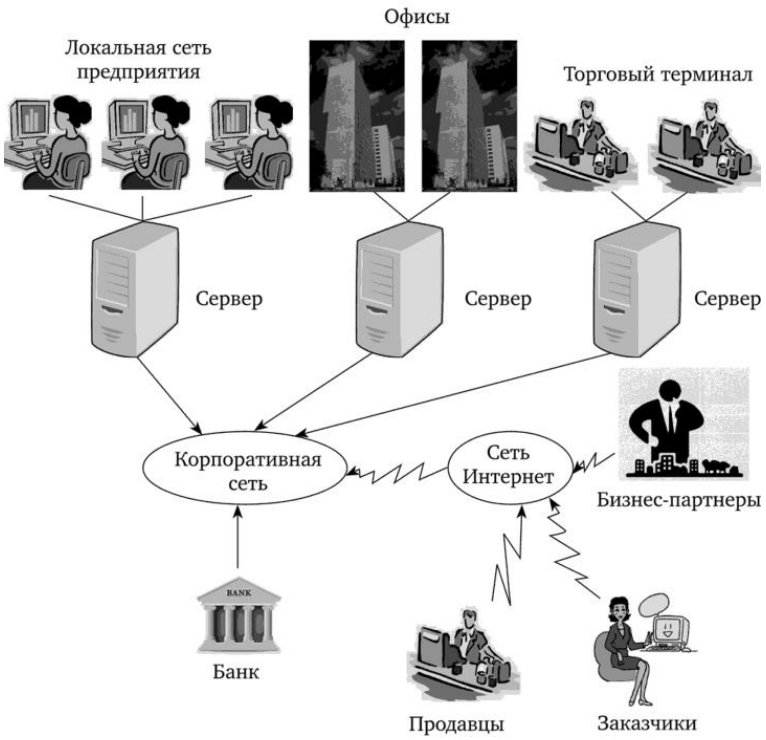

Рис. 1. Взаимодействие пользователя в инфокоммуникационной среде

С точки зрения пользователя поток данных, направляемых от его устройства и принимаемых им, можно назвать трафиком, который циркулирует в информационной сети. Возникает вопрос, насколько безопасно сам трафик может изменяться под внешними воздействиями.

Одним из ключевых вопросов в среде обеспечения безопасности информационного взаимодействия является сетевой трафик. В рамках данной статьи будет рассмотрено понятие «трафик» с точки зрения телекоммуникационной компоненты информационной системы, а также проведена градация трафика по степени потенциальной опасности для нее. Неправильная настройка телекоммуникационного оборудования, вследствие чего возникают задержки в передаче данных также могут оказать отрицательное влияние на информационную безопасность. [2, С. 25-29]. Угрозы информационной безопасности могут быть реализованы по причине наличия в информационных системах уязвимостей. По своей природе любой продукт информационных технологий имеет уязвимости. Поэтому в результате анализа уязвимостей происходит идентификация угроз.

Результаты

Для обеспечения оптимального процесса передачи трафика необходимо соблюдение ряда условий, в которых: качество обслуживания, резервирование, приоретизация и безопасность. Используются механизмы, направленные на обеспечение безопасности сетевого трафика: шифрование, хеширование, стеганография и ряд других. Однако, не от всех угроз можно защититься, применяя данные меры. Выделим три направления защиты сетевого трафика от угроз, они приведены на Рисунке 2 (целостность, доступность и конфиденциальность). [3]

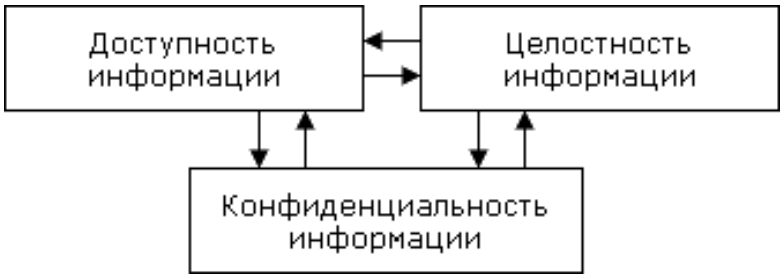

Рис. 2. Направления защиты трафика

Так как выделены направления защиты трафика, по каждому из них есть требования. Они приведены в Таблице 1.

Таблица 1. Требования к защите трафика по направлениям

Наименование направления	Требования	Технологии
Целостность	Применение электронно-цифровых подписей, контрольных сумм, сокрытия факта передачи	Хеширование, контрольное суммирование, стеганография
Доступность	Применение резервирования, сокрытия факта передачи	Программно-аппаратное резервирование, технологии стеганографии
Конфиденциальность	Применение шифрования, политики доступа, сокрытия факта передачи	Шифрование, управление доступом, идентификация объектов информационной системы, стеганография

С точки зрения влияния на информационную безопасность трафик можно условно разделить на легитимный и нелегитимный. В потоках легитимного трафика может быть замаскированный нелегитимный трафик. Как следствие, необходимо конкретизировать меры, направленные на защиту трафика по направлениям. Основное деление трафика с точки зрения телекоммуникационной услуги для пользователя следующее: потоковый и пульсирующий. Для каждого из этих типов трафика стандартами ЭМ ВОС определены правила, называемые протоколами. [4, С. 73-78.]

На рисунке 3 приведена градация трафика с точки зрения телекоммуникаций.

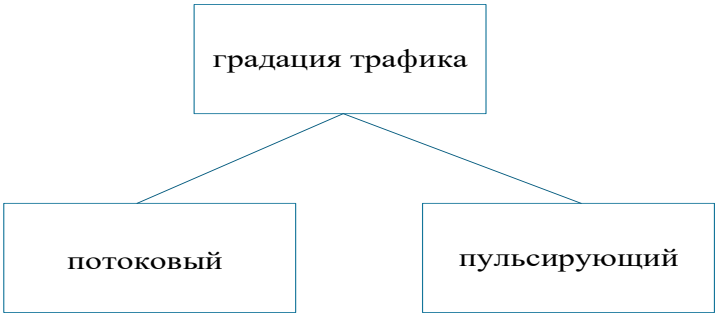

Рис. 3. Градация трафика с точки зрения телекоммуникаций

Отсюда следует, что на пользовательском оконечном оборудовании, которое является потребителем телекоммуникационной услуги, происходит создание трафика. В рамках настоящего исследования данный процесс будет называться генерация трафика, а пользовательские оконечные устройства будут называться генераторами трафика. [5, С. 3-7].

В рамках настоящего исследования обработка и передача трафика будет наименоваться, как циркулирование трафика. Соответственно, задача генерации трафика является по своей сути задачей обеспечения пользователя инфокоммуникационной услугой, такой, как передача данных, голосовая телефония, потоковое видео, телеметрия и т.д..

Следующим вопросом является определение угрозы в самом трафике. Исходя из деления по такому принципу предлагается рассматривать трафик по видам: черный, чистый и серый.

Чистый трафик заведомо и гарантированно не содержит вредоносных элементов и это достоверно известно владельцу инфокоммуникационной сети, в которой он циркулирует.

Черный трафик относится к незаконному или вредоносному трафику. Трафик также может считаться черным, когда происходит информирование владельца информационной системы о непосредственной угрозе его появления из заведомо достоверных источников.

Серый трафик включает в себя легитимные, но возможно имеющие потенциально нежелательные или подозрительные компоненты, такие как уязвимые приложений, реклама и прочее. Серый трафик сам по себе безвреден, однако может спровоцировать успешную реализацию одной из угроз информационной безопасности. [6, С. 67-69].

Серый и черный трафик образуются за счет появления в чистом трафике нежелательных с точки зрения информационной безопасности компонент. Предложено введение понятия «зашумление трафика». Данное понятие будет рассматриваться с точки зрения информационной безопасности, как внесение нежелательных компонент в белый трафик. [7, С. 45-48]

Выводы

В результате можно говорить о том, что пользовательские оконечные устройства являются генераторами трафика. Следовательно, лица, управляющие данными процессами будут в рамках настоящего исследования наименоваться, как операторы данных оконечных устройств или операторы автоматизированных рабочих мест (далее – АРМ). [8, с. 79-80]

Генерация чистого трафика и сценарии работы операторов АРМ могут быть связаны в контексте тестирования и анализа производительности сетевых приложений и решения вопросов обеспечения безопасности информационных систем от угроз, исходящих из самого трафика.

В итоге исследования можно говорить о том, что что генерация трафика по его видам (черный, серый, чистый) находится в прямой зависимости от действий операторов и зашумление трафика является также зависимым от действий операторов процессом. Неправильная настройка оборудования, неверные расчеты пропускной способности полосы пропускания также отрицательно влияют на потоки трафика. [9]

Задачи дальнейших исследований – определение атак, являющихся сетезависимыми, то есть такими атаками, которые зависят от маркирования трафика одним из «цветов» и определение защищенности трафика и уровня его зашумленности. Это можно сделать на основании определения изменения поведения сетевого трафика от его типа. Учитывая большое разнообразие и особенности трафика, а также алгоритмы формирования, маркировка трафика одним из «цветов», определение безопасности движения и уровня его шумового загрязнения является актуальной исследовательской задачей. Разработка методики определения изменений поведения сетевого трафика в зависимости от его характеристик является темой дальнейших исследований.

Литература

1. Абдихалык Ш.С. Методы и средства моделирования атак в больших компьютерных сетях // Студенческий вестник. 2023. № 16-11 (255).
2. Абдулкадыров У.У., Джабраилов И.А., Амерханова З.Ш. Технологии информационной безопасности компьютерных сетей и тенденции их развития // Журнал прикладных исследований. 2023. № 6.
3. Дятлов П.А. Принципы построения и организация компьютерных сетей. Ростов-на-Дону ; Таганрог, 2022.
4. Епифанов Е.К. Различные методы и подходы к проектированию компьютерных сетей // Научно-исследовательский Центр «Science Discovery». 2023. № 12.
5. Поликарпочкина Д.Д. Обзор методов и подходов, используемых для анализа требований к объектам компьютерных сетей // Научно-исследовательский центр «Technical Innovations». 2023. № 14.
6. Попукайло В.С., Столяренко Ю.А., Елисеева С.С. Методы и средства защиты данных в компьютерных сетях // Нанотехнологии: наука и производство. 2023. № 2.
7. Михайлов А.А., Федулов В.И. «Феномен виртуальных организаций в современных условиях».: Московский экономический журнал. (10). 27. Февраль, 2024.
8. Юрчик П.Ф., Максимычев О.И., Голубкова В.Б., «Виртуальное предприятие как инновация в сфере организации бизнеса». Наука и бизнес: пути развития. (6(84)). С. 135-138. Январь, 2023.
9. Халлиган Б., Шах Д. Входящий маркетинг: привлекайте, вовлекайте и восхищайте клиентов в Интернете. / 2-е изд. – Нью-Джерси: John Wiley & Sons, 2014. – 224 сент. 2023.