Министерство образования Республики Беларусь
Учреждение образования
Белорусский государственный университет
информатики и радиоэлектроники

УДК 004.774:004.056

Трофимов
Дмитрий Сергеевич

РАЗРАБОТКА ОТКАЗОУСТОЙЧИВОЙКОРПОРАТИВНОЙ ИНФРАСТРУКТУРЫ

АВТОРЕФЕРАТ
на соискание степени магистра технических наук
по специальности 1 - 53 80 01 Автоматизация и управление технологическими процессами и производствами

Научный руководитель

А.В. Павлова,
кандидат технических наук,
доцент

Минск 2020

Нормоконтроль

А.В. Павлова

ВВЕДЕНИЕ

При разработке отказоустойчивой корпоративной инфраструктуры необходимо учитывать много различных факторов, такие как отказоустойчивость, нагрузка на сеть, помехоустойчивость и т.д.

Отказоустойчивость для современных систем в целом важна по ряду причин. Удалённый доступ с целью хищения информации, похищение конфиденциальной информации, нанесение вреда оборудованию – всё это приводит к финансовым потерям, которые могут нанести огромный вред тому или иному объекту.

Для современных корпоративных инфраструктур главные требования – скорость передачи данных по локальной сети и безопасность передаваемых данных. Так как сейчас ни одна корпоративная структура не может обойтись без выхода в глобальный ресурс Internet, при проектировании локальных сетей необходим серьёзный подход к созданию безопасного хранения данных, а также защиты от сторонних атак, которые могут нарушить или вовсе остановить работы предприятия.

Для исключения проблем с безопасностью данных и повышения помехоустойчивости в локальных сетях и безотказности работы персонала в данной магистерской диссертации производится анализ трёх распространённых протоколов передачи данных прикладного и сетевого уровней стека TCP/IP.

Целью исследования ставлю анализ основных протоколов передачи данных между конечными устройствами корпоративной инфраструктуры, обеспечивающей безотказную работу для персонала.

Предмет исследования: протоколы стека TCP/IP.

Объект исследования: инфраструктура информационно-аналитической системы.

Задачи:

1. Провести обзор источников по теме диссертации.
2. Ознакомиться с особенностями структуры локальной сети.
3. Выполнить сравнительный анализ протоколов TCP/IP.
4. Предложить использование новейших протоколов взамен стандартных распространённых.

В первой главе диссертационной работы производится сравнительный анализ протоколов DHPC и S-DHCP.

Во второй главе диссертационной работы производится сравнительный анализ протоколов HTTP/1.1 и HTTP 2.

В третьей главе диссертационной работы производится сравнение протоколов IP и IPv6 и использование протоколов в мире и в Беларуси.

ОБЩАЯ ХАРАКТЕРИСТИКА РАБОТЫ

Актуальность исследования

Создание помехоустойчивой локальной инфраструктуры в данный момент является актуальной темой и представляется важным для всех организаций различных сфер деятельности. Более того, рассмотренные здесь протоколы передачи данных находят свое применение на крупных предприятиях с большой численностью сотрудников.

Самой актуальной задачей является использование протоколов самых последних версий, что приведёт к увеличению помехоустойчивости, защиты от внешних атак и уменьшению нагрузки локальной сети.

Цель исследования

Целью диссертационной работы ставлю исследование существующих и использование новых улучшенных протоколов передачи данных, которые позволят улучшить показатели помехоустойчивости и ускорить работу локальной сети корпоративной инфраструктуры.

Задачи исследования

1. Обзор существующих протоколов передачи данных стека TCP/IP.
2. Анализ существующих используемых протоколов и их улучшенные версии.
3. Исследование выбранных протоколов и сравнительный анализ на его основе.

Новизна полученных результатов

Научная новизна заключается в том, что было предложено использование обновлённых протоколов стека TCP/IP, что позволит увеличить степень защиты от внешних угроз за счёт усовершенствованных схем работы аутентификации пользователей, скорость загрузки веб-страниц.

Личный вклад соискателя

Соискателем выполнены все изложенные в работе разработки и исследования. Постановка задач и обсуждение результатов проводились совместно с научным руководителем и сотрудниками кафедры систем управления Белорусского государственного университета информатики и радиоэлектроники. Соавторы опубликованных работ принимали участие в

обсуждении промежуточных и конечных результатов. Обработка, интерпретация данных, а также выводы сделаны автором самостоятельно.

Апробация результатов диссертации

Основные положения диссертационной работы докладывались на следующих научных конференциях:

- 55-ая юбилейная научная конференция аспирантов, магистрантов и студентов
- 54-ая юбилейная научная конференция аспирантов, магистрантов и студентов

Опубликованность результатов диссертации

Основные результаты диссертации опубликованы в 1 статье в сборнике материалов научных конференций.

СОДЕРЖАНИЕ РАБОТЫ

Разработка отказоустойчивой корпоративной инфраструктуры требует учёта многих факторов. Для малых и средних предприятий факторы использования протоколов играют менее важную роль, чем на крупных предприятиях, где необходима высокая степень защиты информации, помехоустойчивости и контроль за нагрузкой локальной сети.

В первой главе диссертационной работы производится анализ протокола прикладного уровня стека TCP/IP DHCP и усовершенствованной версии S-DHCP, которые используются для аутентификации конечных пользователей локальной сети.

Протокол DHCP упрощает доступ к сети. Когда хост подключается к сети, DHCP автоматизирует назначение параметров конфигурации стека TCP/IP, таких как IP-адреса, маски подсети и шлюз по умолчанию. Это интернет-протокол, который позволяет сетевым администраторам централизованно управлять сетью. Без использования DHCP IP-адрес должен быть назначен вручную для каждого хоста в сети, и, если хост перемещен в новое место в сети, IP-адрес должен быть настроен вручную.

В первой главе предлагается использование схемы под названием Secure DHCP (S-DHCP) для защиты протокола DHCP, вводится новая схема под названием Secure DHCP (S-DHCP) для защиты протокола DHCP. Предлагаемое решение состоит из двух методик. Первый - это метод аутентификации и управления ключами, который используется для аутентификации объектов и управления ключом безопасности. Он основан на использовании алгоритма обмена ключами Диффи-Хеллмана. Второй метод - это метод аутентификации сообщений, который использует цифровую подпись для аутентификации сообщений DHCP, которыми обмениваются клиенты и сервер.

Во второй главе диссертационной работы рассматривается ещё один распространённый протокол передачи данных – HTTP, а именно анализируются версии HTTP/1.1 и HTTP/2.0 для использования в корпоративной инфраструктуре. В главе рассматривается веб-производительность данных протоколов с помощью различных инструментов, таких как Pagescope, который призван стать инструментом, способным оценить все схемы улучшения производительности сети. Эти системы варьируются от прикладных протоколов, облачных браузеров и оптимизаторов страниц до изменений сетевого уровня.

В третьей главе диссертационной работы производится сравнительный анализ сетевых протоколов IPv4 и IPv6. Протокол IP — является адресным протоколом, который отвечает за адресацию всей сети. То есть, благодаря использованию протокола IP, каждый компьютер (устройство) в сети имеет

свой индивидуальный адрес (IP-адрес). По этим адресам и осуществляется передача данных.

IPv4 использует 32-битные (четырёхбайтные) адреса, ограничивающие адресное пространство 4 294 967 296 (2^{32}) возможными неповторимыми адресами. Классической формой записи IPv4 адреса является запись в виде четырёх десятичных чисел (от 0 до 255), разделённых точками. Через дробь указывается длина маски подсети, например, 255.255.255.0 можно сократить как /24.

Необходимость использования протокола IPv6 обусловлена тем, что каждый год количество конечных пользователей увеличивается в разы, что может привести к переполнению пул адресов протокола IPv4.
Переход с IPv4 на IPv6 освобождает большой пул адресов протокола IPv4.

Протокол IPv6 (Internet Protocol version 6) — это новейший вариант интернет протокола (IP), сделанный с целью решения задач, которые не могла решить предыдущая версия (IPv4) при её применении в интернете, одна из которых это использование длины адреса 128 бит вместо 32, то есть, IPv6 в 4 раза длиннее.

В настоящее время уровень использования сети Интернет очень сильно дифференцирован как по миру в целом, так и по регионам. IPv6 используется уже в 10% сетевых устройств мира. Технические спецификации стандарта Internet Protocol Version 6 были опубликованы ещё 20 лет назад в документе RFC 1883. Однако до последнего времени новый стандарт IPv6 использовался мало. В начале 2013 года его доля в мире составляла 1%, однако за минувшие два года она выросла до 10% по данным Google. Рисунок 3.5 отображает рост числа пользователей с IPv6.

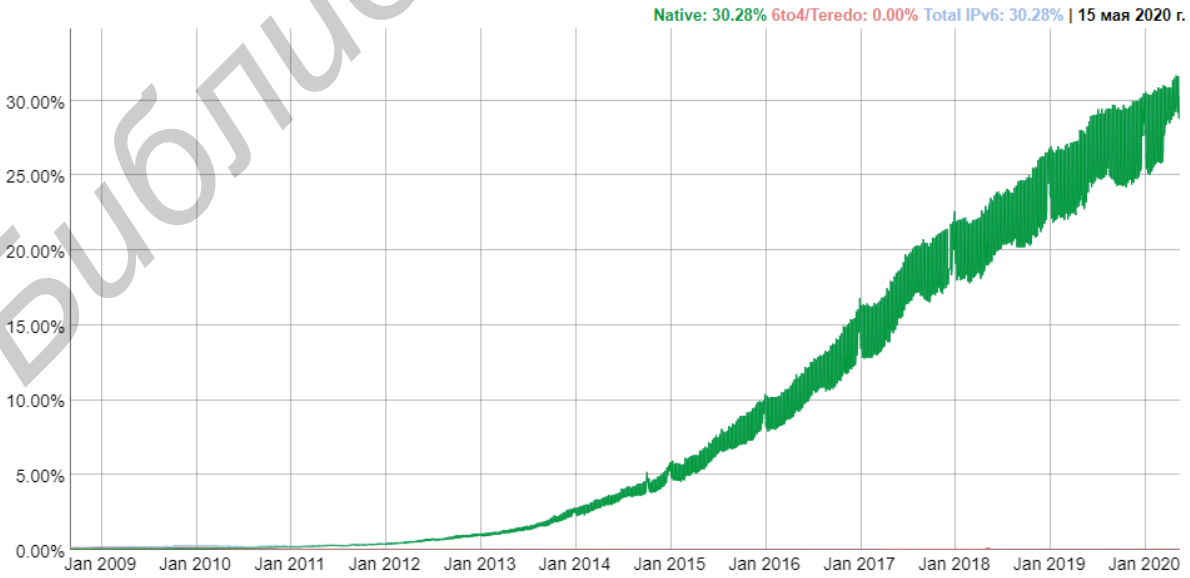

Рисунок 3.5 – Использование IPv6 в мире

Ниже на рисунке 3.6 представлена карта использования IPv6. На май 2020 год в Беларуси протокол IPv6 использует около 4.64% пользователей. Больше всего Бельгия – 56.53%.

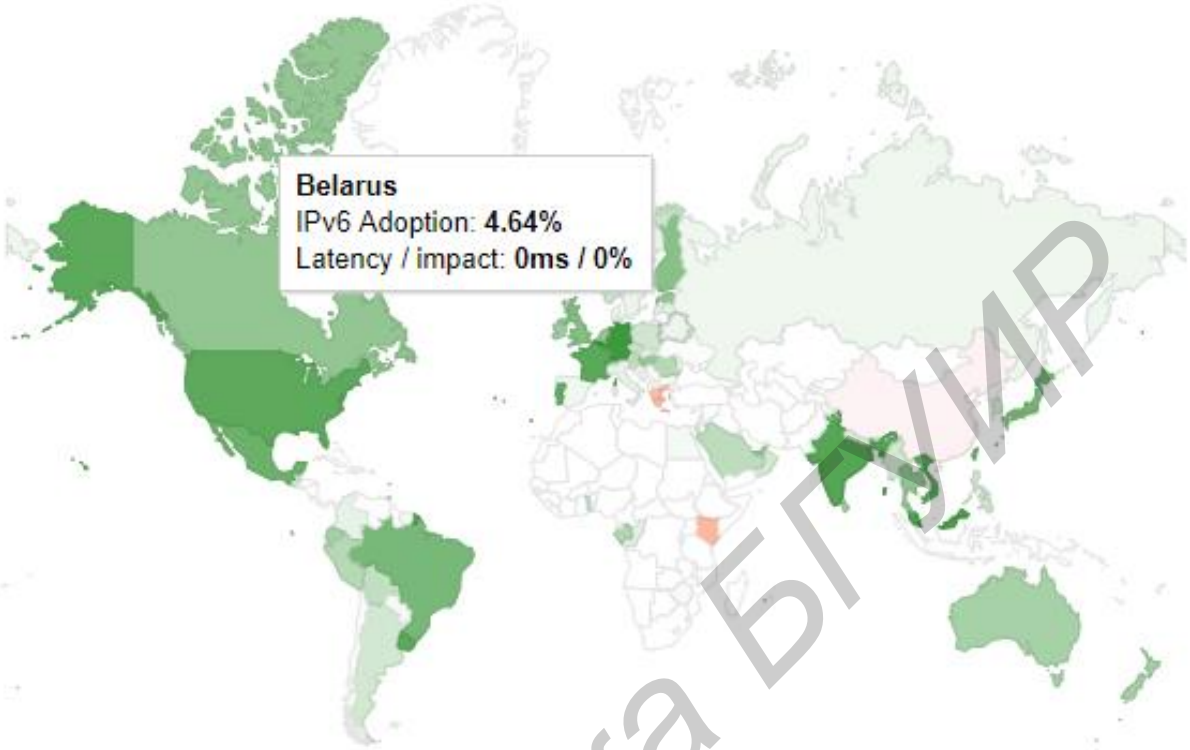

Рисунок 3.6 – Внедрение IPv6 в каждой стране

Страны, которые окрашены в зелёный цвет, - IPv6 используется более широко (чем темнее зеленый, тем больше распространение), и у пользователей возникают нечастые проблемы с подключением к веб-сайтам с поддержкой IPv6.

Страны, которые окрашены в оранжевый цвет, - IPv6 используется более широко, но пользователи по-прежнему испытывают значительные проблемы с надежностью или задержками при подключении к веб-сайтам с поддержкой IPv6.

Страны, которые окрашены в красный цвет, - IPv6 широко не используется, и пользователи испытывают значительные проблемы с надежностью или задержками при подключении к веб-сайтам с поддержкой IPv6.

ЗАКЛЮЧЕНИЕ

Проблема защиты локальной сетевой информации ставится и, с той или иной степенью эффективности, решается с момента появления сетей на основе протоколов семейства TCP/IP.

В эволюциях технологий защиты можно выделить три основных направления. Первое — разработка стандартов, имплиментирующих в сеть определенные средства защиты, прежде всего административной. Второе направление — это культура межсетевых экранов (firewalls), давно применяемых для регулирования доступа к подсетям. Третье, наиболее молодое и активно развивающееся, направление — это так называемые технологии виртуальных защищенных сетей (VPN, virtual private network, или intranet).

В данной диссертационной работе рассмотрены распространённые протоколы передачи данных первого направления. Использование усовершенствованного протокола S-DHCP позволит минимизировать риск вторжения злоумышленника в локальную сеть предприятия на основе двух методик. Первый - это метод аутентификации и управления ключами, который используется для аутентификации объектов и управления ключом безопасности. Он основан на использовании алгоритма обмена ключами Диффи-Хеллмана. Второй метод - это метод аутентификации сообщений, который использует цифровую подпись для аутентификации сообщений DHCP, которыми обмениваются клиенты и сервер.

В крупных организациях с большой численностью сотрудников важным показателем является бесперебойность в работе, которая зависит от скорости загрузки веб-ресурсов. Был произведён анализ протокола прикладного уровня HTTP/2.0, который способствует загрузке страниц с большей скоростью. HTTP/2 не всегда превосходит HTTP/1.1 по производительности. Вместо этого существует оптимальный диапазон для каждого типа свойства. Эти диапазоны предполагают, что HTTP/2 работает хуже на страницах большего размера, чем в среднем. Это нелогично, учитывая, что мультиплексирование HTTP/2 позволяет распараллеливать выборки ресурсов. В пределах нижних диапазонов каждого свойства мы видим результаты, более соответствующие интуиции. В HTTP/2 кластер страниц загружается с одинаковым минимальным временем загрузки страницы, несмотря на различия в значении свойства.

Количество конечных пользователей глобального ресурса Internet с каждым годом возрастает в разы. Для доступа в сеть Internet каждое устройство имеет свой IP-адрес. Большая часть конечных устройств настроена с помощью протокола IPv4. Это приводит к тому, что пул адресов протокола IPv4 постепенно исчерпывается. Это обуславливает необходимость перехода

организаций на протокол IPv6, которая кроме того не имеет ограничений пул адресов для конкретного предприятия.

Подводя итоги данной диссертационной работы стоит отметить, что для создания отказоустойчивой корпоративной инфраструктуры необходимо учитывать множество таких факторов, как помехоустойчивость, нагрузка локальной сети, скорость передачи данных в локальной сети. Использование усовершенствованных протоколов, предложенных автором данной работы, позволит достичь эффективных показателей локальной сети.