

МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ РОССИЙСКОЙ ФЕДЕРАЦИИ

**ФЕДЕРАЛЬНОЕ ГОСУДАРСТВЕННОЕ БЮДЖЕТНОЕ**

**ОБРАЗОВАТЕЛЬНОЕ УЧРЕЖДЕНИЕ ВЫСШЕГО ОБРАЗОВАНИЯ**

**«ДОНСКОЙ ГОСУДАРСТВЕННЫЙ ТЕХНИЧЕСКИЙ УНИВЕРСИТЕТ»**

**(ДГТУ)**

Факультет «Информатика и вычислительная техника»

Кафедра «Вычислительные системы и информационная безопасность»

|  |  |  |
| --- | --- | --- |
| И.о. Зав. кафедрой | | «ВСиИБ» |
| \_\_\_\_\_\_\_\_\_\_\_\_ | | А.Р. Газизов |
| подпись | | И.О. Фамилия |
|  | «03» февраля 2023 г. | |

**ПОЯСНИТЕЛЬНАЯ ЗАПИСКА**

Тема «МЕТОДИКА МАСКИРОВАНИЯ VPN-ТРАФИКА ПРИ ПЕРЕДАЧЕ ПО ТЕЛЕКОММУНИКАЦИОННОЙ СЕТИ»

Направление подготовки 10.05.02 Информационная безопасность телекоммуникационных систем

Специализация Защита информации в системах связи и управления

Обозначение ВКР 10.05.02.240000.000 группа ВИБТ62

Обучающийся \_\_\_\_\_\_\_\_\_\_\_\_\_\_ И.А. Черкесов

(подпись, дата) И.О.Ф.

Руководитель ВКР \_\_\_\_\_\_\_\_\_\_\_\_\_\_ доц., к.т.н. В.В. Галушка

(подпись, дата) должность, И.О.Ф.

Консультанты по разделам:

Безопасность и экологичность работы \_\_\_\_\_\_\_\_\_\_\_\_\_ проф., д.т.н. В.Л. Гапонов

(подпись, дата) (должность, И.О.Ф.)

Технико-экономическое обоснование \_\_\_\_\_\_\_\_\_\_\_\_\_ ст преп. А.В. Белоусова

(подпись, дата) (должность, И.О.Ф.)

Нормоконтроль \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ ст. преп. М.А. Ганжур

(подпись, дата) (должность, И.О.Ф.)

Ростов-на-Дону

2023



МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ РОССИЙСКОЙ ФЕДЕРАЦИИ

**ФЕДЕРАЛЬНОЕ ГОСУДАРСТВЕННОЕ БЮДЖЕТНОЕ**

**ОБРАЗОВАТЕЛЬНОЕ УЧРЕЖДЕНИЕ ВЫСШЕГО ОБРАЗОВАНИЯ**

**«ДОНСКОЙ ГОСУДАРСТВЕННЫЙ ТЕХНИЧЕСКИЙ УНИВЕРСИТЕТ»**

**(ДГТУ)**

Факультет «Информатика и вычислительная техника»

Кафедра «Вычислительные системы и информационная безопасность»

|  |  |  |
| --- | --- | --- |
| Зав. кафедрой | | «ВСиИБ» |
| \_\_\_\_\_\_\_\_\_\_\_\_ | | В.А. Фатхи |
| подпись | | И.О. Фамилия |
|  | «23» июня 2022 г. | |

**ЗАДАНИЕ**

на выполнение выпускной квалификационной работы

Тема «МЕТОДИКА МАСКИРОВАНИЯ VPN-ТРАФИКА ПРИ ПЕРЕДАЧЕ ПО ТЕЛЕКОММУНИКАЦИОННОЙ СЕТИ»

Обучающийся Черкесов Ислам Аджиисламович

Обозначение ВКР 10.05.02.240000.000 группа ВИБТ62

Тема утверждена приказом по ДГТУ от «23» июня 2022 г. № 2831-ЛС-О

Срок представления ВКР к защите «\_\_» \_\_\_\_\_\_\_\_\_ 2023 г.

Исходные данные для выполнения выпускной квалификационной работы:

Методы и средства защищенного обмена информацией через сеть Интернет: протоколы OpenVPN, WireGuard, SoftEther VPN; средства маскирования трафика Stunnel, Cloak.

Содержание выпускной квалификационной работы

Введение: Во введении необходимо изложить актуальность выбранной темы, обозначить объект и предмет исследования, цель и задачи выпускной квалификационной работы, теоретическую и практическую значимость работы, структуру работы.

Наименование и краткое содержание разделов:

1. Задача маскирования трафика виртуальных частных сетей. Виртуальные частные сети. Правовое регулирование использования виртуальных частных сетей. Технологии построения виртуальных частных сетей. Методы анализа трафика для выявления соединений виртуальных частных сетей.

2. Методы и средства передачи трафика в сетях VPN и его маскирования. Протокол OpenVPN. Маскирование VPN–трафика с использованием SoftEther. Маскирование VPN–трафика с использованием Stunnel.

3. Практическая реализация методики маскирования VPN–трафика. Общая структура телекоммуникационной системы. Программно–аппаратные средства реализации . Настройка маскирования VPN–трафика в OpenVPN. Настройка маскирования VPN–трафика в SoftEther. Настройка маскирования VPN–трафика в WireGuard. последний Анализ эффективности предложенных методов и средств.

4. Безопасность и экологичность проекта. Влияние шума на организм человека и защита от них. Расчет уровня шума на рабочем месте. Экологичность работы. Организация и обеспечение пожарной безопасности на предприятии. Выводы.

5. Экономическое обоснование. Спецификация проекта. План–график проектирования и разработки системы. Расчет затрат на разработку проекта.

Заключение: Заключение должно содержать обобщенные результаты проведенной работы в соответствии с поставленной целью и задачами, необходимо указать чем завершается работа – усовершенствованием, модернизацией, дать свои предложения.

Перечень графического и иллюстративного материалов:

1. Общая структура телекоммуникационной систем
2. Структура пакета OpenVPN
3. Маскировка трафика в SoftEther VPN

Руководитель ВКР \_\_\_\_\_\_\_\_\_\_\_\_\_\_ доц., к.т.н. В.В. Галушка

(подпись, дата)

Задание к исполнению принял \_\_\_\_\_\_\_\_\_\_\_\_\_\_ И.А. Черкесов

**Аннотация**

Выпускная квалификационная работа посвящена проблеме обеспечения надежности виртуальных частных сетей, являющихся одной из важнейших составных частей функционирования корпоративных сетей. В работе проведен выполнен анализ протоколов VPN и особенностей маскирования VPN–трафика, а также определены возможные способы реализации. На основе полученных данных предложен проекты систем на базе протоколов OpenVPN, WireGuard, SoftEther VPN, с использованием программ Stunnel и Cloak для маскировки трафика.

Объем текстового материала 82 листа (А4), количество иллюстраций 33, таблиц — 11, использованных источников — 15.

**Abstract**

The final qualification work is devoted to the problem of ensuring the reliability of virtual private networks, which are one of the most important components of the functioning of corporate networks. The paper analyzes VPN protocols and features of masking VPN traffic, and also identifies possible implementation methods. Based on the data obtained, projects of systems based on the OpenVPN, WireGuard, SoftEther VPN protocols, using Stunnel and Cloak programs for traffic masking, are proposed.

The volume of text material is 82 sheets (A4), the number of illustrations is 33, tables - 11, sources used - 15.

Содержание

[Введение 6](#_Toc124934228)

1. [Задача маскирования трафика виртуальных частных сетей 7](#_Toc124934229)

[1.1 Виртуальные частные сети 7](#_Toc124934230)

[1.2 Правовое регулирование использования виртуальных частных сетей 13](#_Toc124934231)

[1.3 Технологии построения виртуальных частных сетей 17](#_Toc124934232)

[1.4 Методы анализа трафика для выявления соединений виртуальных частных сетей 21](#_Toc124934233)

1. [Методы и средства передачи трафика в сетях VPN и его маскирования 24](#_Toc124934234)

[2.1 Протокол OpenVPN 24](#_Toc124934235)

[2.2 Маскирование VPN–трафика с использованием SoftEther 28](#_Toc124934236)

[2.3 Маскирование VPN–трафика с использованием Stunnel 33](#_Toc124934237)

[3. Практическая реализация методики маскирования VPN–трафика 34](#_Toc124934238)

[3.1 Общая структура телекоммуникационной системы 34](#_Toc124934239)

[3.2 Программно–аппаратные средства реализации 36](#_Toc124934240)

[3.3 Настройка маскирования VPN–трафика в OpenVPN 38](#_Toc124934241)

[3.4 Настройка маскирования VPN–трафика в SoftEther 45](#_Toc124934242)

[3.5 Настройка маскирования VPN–трафика в WireGuard 50](#_Toc124934243)

[3.6 Анализ эффективности предложенных методов и средств 57](#_Toc124934244)

[4. Экономическое обоснование 59](#_Toc124934245)

[4.1 Спецификация проекта 59](#_Toc124934246)

[4.2 План–график проектирования и разработки системы 60](#_Toc124934247)

[4.3 Расчет затрат на разработку проекта 64](#_Toc124934248)

[5. Безопасность и экологичность проекта 68](#_Toc124934249)

[5.1 Влияние шума на организм человека и защита от них. Расчет уровня шума на рабочем месте 68](#_Toc124934250)

[4.2 Экологичность работы 70](#_Toc124934251)

[5.3 Организация и обеспечение пожарной безопасности на предприятии 75](#_Toc124934252)

[5.4 Выводы 79](#_Toc124934253)

[Заключение 80](#_Toc124934254)

[Перечень использованных информационных ресурсов 81](#_Toc124934255)

**Введение**

На сегодняшний день всё большее количество информации обрабатывается и передаётся по сети интернет, но вместе с тем и увеличивается число кибератак. Чтобы защитить данные, передаваемые через сеть Интернет, используются различные средства защиты информации. Одним из которых является технология виртуальных частных сетей (VPN). VPN создает защищенный зашифрованный туннель поверх открытых каналов связи. Благодаря данной технологии появляется возможность построения корпоративных сетей, а именно объединения сетей филиалов организаций, удаленной работы сотрудников, подключения к сети Интернет через публичные сети Wi–Fi. Но иногда бывает так, что подключения по VPN блокируются, а так как при помощи данной технологии создаются защищенные каналы связи, передаются конфиденциальные данные, то нужно иметь возможность обходить эти блокировки. Решению данной задачи посвящена выпускная квалификационная работа. Её целью являлось улучшение надежности VPN–каналов.

Для достижения поставленной цели были решены следующие задачи:

— выполнен анализ протоколов VPN;

— выполнен анализ особенностей маскирования VPN–трафика;

— предложены способы практической реализации маскировки трафика виртуальных частных сетей;

— проведена оценка эффективности предложенных методов защиты.

1. **Задача маскирования трафика виртуальных частных сетей**
   1. **Виртуальные частные сети**

Развитие современных информационных технологий, а именно, сети Интернет, вызвало острую потребность в защите информации, передаваемой в распределенных корпоративных сетях, использующих открытые каналы связи. При использовании собственных каналов доступа эта проблема не так актуальна, так как в сеть никто из посторонних доступа не имеет. Стоит отметить высокую стоимость таких каналов, ввиду этого не каждая компания может их себе позволить, исходя из этого Интернет является наиболее доступным.

VPN объединяет корпоративные узлы, сети и пользователей через открытые не доверенные сети. Любая организация, будь она коммерческой или государственной, обязательно сталкивается с проблемой защищенной передачи информации между своими удалёнными зданиями. Однако не каждая организация может себе позволить иметь собственные каналы связи, и здесь помогает VPN, на основе которой и соединяются удаленные подразделения или офисы.

Виртуальная частная сеть создается на базе общедоступной сети Интернет, главной проблемой которой является потенциальная подверженность атакам, нарушениям конфиденциальности информации, то технология виртуальных частных сетей может гарантировать, что трафик, направленный через Интернет, будет защищен так же, как и передача внутри локальной сети.

VPN – технология, которая создает логическую сеть, поверх другой сети, например Интернет. Несмотря на то, что передача информации производится по открытым сетям с использованием небезопасных протоколов, за счёт шифрования создаются закрытые каналы обмена информацией.

По своей сути VPN является выделенной линией передачи информации, однако развертывается она в пределах публичной сети. С помощью технологии туннелирования пакеты данных передаются через публичную сеть, как будто они соединены непосредственно между собой. Между каждой парой «отправитель–получатель данных» устанавливается своеобразный туннель – защищенное логическое соединение, которое позволяет позволяющее «заворачивать» данные одного протокола в данные другого. Основными составляющими такого туннеля являются:

* инициатор VPN–сессии;
* маршрутизатор, поддерживающий VPN;
* маршрутизируемая сеть.

Туннелирование дает возможность передать пакеты одного протокола в логической сети, использующей другой протокол. Исходя из этого становится возможны решить проблемы взаимодействия разных сетей, включая проблемы потребности обеспечения конфиденциальности и целостности передаваемых данных, вплоть до несоответствия протоколов.

Туннелирование обеспечивает передачу пакетов данных, скрывая всю сетевую инфраструктуру, которая находится между ними, будто узлы виртуальной частной сети подключены непосредственно.

Трансляция данных по туннелю, как паром, который берет пакеты используемого сетевого протокола в начале туннеля и без изменений доставляет их к выходу. Построенный туннель, соединяющий сетевые узлы, для программного обеспечения этих узлов выглядит будто бы они подключены к одной локальной сети, тем не менее, нельзя игнорировать то, что на самом деле перед тем, как пакет придет к адресату, он должен пройти множество промежуточных роутеров сети Интернет.

В результате этого возникает проблема. Первая заключается в том, что информация, которая передается через открытые публичные сети, может быть перехвачена злоумышленником. Если в ней содержатся конфиденциальные данные, такие как: личные данные, информация о банковских картах, внутренние корпоративные данные, то вполне реальна угроза ее компрометации. Также, злоумышленники могут изменить передаваемую информацию так, что адресат не сможет проверить их подлинность. Из вышесказанного, можно сделать вывод, что туннель в чистом виде не пригоден для использования его при передаче чувствительной информации. Однако эта проблема решается современными средствами криптографической защиты информации.

Хотя и PPTP считается достаточно безопасным протоколом, все же протокол L2TP/IPSec будет лучше, так как помимо аутентификации пользователей еще и шифрует данные.

Аутентификация в протоколе L2TP/IPSec двухэтапная. На первом этапе используются локальные сертификаты, полученные от центра сертификации. Далее сервер и клиент обмениваются сертификатами и создают защищенное соединение ESP SA. После того как L2TP/IPSec завершает процесс аутентификации компьютера, выполняется аутентификация на уровне пользователя. Для аутентификации можно задействовать любой протокол, который передаст пароль и имя пользователя. Можно использовать протоколы, передающие имя пользователя и пароль в открытом виде, так как все данные, которые будут переданы в рамках данной VPN–сессии будут зашифрованы. Однако рекомендуется использовать протокол MSCHAP ввиду того, что он использует различные ключи шифрования для аутентификации компьютера и пользователя.

Шифрование трафика гарантирует защиту конфиденциальных данных, при передаче их через сеть Интернет, так как никто не сможет подслушать VPN–соединение. VPN–шифрование позволяет скрыть конфиденциальную информацию при ее трансляции через публичные сети от посторонних глаз.

При подключении VPN–клиента к VPN–серверу, все запросы шифруются перед отправкой. Далее на VPN–сервере запросы расшифровываются и ретранслируются на целевой сервер, это может быть веб–сервер, почтовый или файловый серверы. При получении ответа от целевого сервера данные снова зашифровываются и отправляются клиенту.

Как правило различают два типа алгоритмов шифрования:

Симметричное шифрование — это тип алгоритмов шифрования, использующих один ключ шифрования. За счет того, что данный тип шифрования использует только один ключ, он является более быстрым, но в то же время появляется проблема надежной передачи ключа шифрования пользователю. Примером алгоритма симметричного шифрования является AES.

Асимметричное шифрование — этот тип алгоритма шифрования, использующий два ключа шифрования, открытый и закрытый. Открытый ключ шифрования используется для шифрования данных, а закрытый для их расшифровки. Хотя это может быть удобно, это также очень рискованно, поскольку закрытый невозможно восстановить, если он будет утерян. Хорошим примером алгоритма асимметричного шифрования является шифр RSA.

В зависимости от протокола VPN могут использоваться различные алгоритмы шифрования ниже будут приведены наиболее популярные:

Blowfish — незапатентованный, свободно распространяемый симметричный алгоритм шифрования, использующий 128–битный ключ. Был разработан 1993 году Брюсом Шнайдером. В связи с тем, что размер блока в данном алгоритме равен 64 не рекомендуется к использованию.

Twofish — более современная версия шифра Blowfish.Отличие от Blowfish заключается в том, что в данном алгоритме используется 128–битный блок.

AES — наиболее популярный алгоритм шифрования. В AES могут быть использованы 128–битные, 192–битные и 256–битные ключи шифрования

Camellia — алгоритм блочного симметричного шифрования. Размер блока у данного шифра равен 128 битам, Ключи могут быть 128–битными, 192–битными и 256–битными.

RSA — ассиметричный алгоритм шифрования, как правило используются для установки VPN–соединения и передачи секретного ключа симметричного шифра.

Таким образом, использование туннелирования совместно с аутентификацией и шифрованием делает возможным безопасную передачу данных между двумя узлами через открытую сеть. Иными словами, рассмотренные технологии дают возможность построить виртуальную частную сеть.

Технология виртуальных частных сетей имеет и свои недостатки, в число которых входят: увеличение задержек при отправке пакетов данных и проблемы защиты данных.

В связи с тем, VPN–сервер может находится в другой стране и физическое расстояние до сервера может достигать более нескольких тысяч километров, и соответственно весь трафик, проходящий через туннель, должен пройти это расстояния перед тем, как дойдет до веб–сервера и потом снова должен пройти этот путь при получении ответа от веб–сервера увеличивается задержка пакетов данных. Помимо этого, на увеличение задержки влияет шифрование, которое используется в виртуальных частных сетях, так как шифрование данных занимает определенное количество машинного времени.

Также при использовании VPN–сервисов возможна компрометация данных, в частности настоящего IP–адреса, из–за утечек DNS. Утечка DNS – процесс, при котором VPN–клиент отправляет DNS–запросы за пределы защищенного VPN–туннеля, то есть с настоящего IP–адреса. При утечке DNS исходящий трафик становится уязвим к мониторингу, ввиду того что провайдер Интернет–услуг может анализировать DNS–запросы

Но также технология VPN имеет преимущества, главные из которых: экономичность, гибкость и удобство использования.

1. Экономичность. С помощью виртуальных частных сетей у организаций получается ограничить рост числа сетевого оборудования, которое они вынуждены внедрять, чтобы организовать удаленным работникам доступ к корпоративной сети. Кроме того, VPN дает возможность удаленным работникам обращаться к корпоративным ресурсам не по дорогостоящим линиям, взятым в аренду, а через мобильную сотовую связь. Крайне выгодна технология VPN в тех случаях, когда работникам удалены на большие расстояния и поэтому арендованные линии обходятся очень дорого, особенно когда таких работников много, в следствии чего требуется большое количество арендованных каналов связи.
2. Гибкость и удобство. Это объясняются тем, что виртуальные частные сети могут организовать удаленный доступ к ресурсам организации любому VPN–клиент, имеющему доступ в сеть Интернет. Благодаря данной возможности виртуальные частные сети позволяют контрагентам получить доступ к сетевым ресурсам организации через сеть Интернет, что способствует укреплению партнерских отношений. Этого трудно добиться с помощью традиционных частных сетей, так как организации, желающие совместно использовать сетевые ресурсы, часто имеют несовместимые системы.

**1.2 Правовое регулирование использования виртуальных частных сетей**

Технология виртуальных частных сетей – это совокупность протоколов, которые повышают защищённость, обеспечивают конфиденциальность и целостность данных при подключении к каким-либо сервисам через общедоступную сеть Интернет с помощью применения криптографических алгоритмов.

При рассмотрении вопроса законности применения технологии виртуальных частных сетей в первую очередь нужно учесть в каком стране используется VPN и с какой целью. Используется ли VPТ, как средство для доступа к запрещенным сайтам в обход блокировок или же используется для обеспечения безопасности конфиденциальных данных.

Технологией VPN пользуются и преступники для противоправных действий, например, для распространения вредоносного программного обеспечения, для торговли и сбыта запрещенных товаров, похищенных данных и иной противозаконной деятельности. Ввиду применения VPN в действиях такого рода, данная технология вызывает представление чего–то противозаконного. Но, при правильном использовании, протокол виртуальных частных сетей предстает с хорошей стороны. VPN дает возможность организациям и людям обмениваться данными в защищенном виде. Например, при помощи VPN создаются защищенные каналы связи между удаленными сетями организации, VPN дает возможность удаленным сотрудникам безопасно подключаться к информационной системе организации через открытую сеть.

В 2017 году в России был принят закон, запрещающий применении VPN на территории Российской Федерации. Согласно данному закону, VPN-сервисы и анонимайзеры должны сотрудничать с властями. Организации, не исполнявшие требования властей, должны были быть заблокированы на территории России. Позднее, для того чтобы доступ к запрещенным сайтам отсутствовал даже при использовании виртуальных частных сетей Роскомнадзор обязал VPN-сервисы подключиться к реестру запрещенных сайтов.

Согласно ст. 15.8 ФЗ «О внесении изменений в ФЗ «Об информации, информационных технологиях и о защите информации» от 29.07.2017 № 276 – ФЗ использование технологии виртуальных частных сетей не запрещено, если не нарушается законодательство страны. Важно отметить, что блокируются те VPN-сервису, которые были уведомлены Роскомнадзором и не подключились Федеральной государственной информационной системе (ФГИС) в течении 30 дней после уведомления.

**1.3 Технологии построения виртуальных частных сетей**

Виртуальные частные сети создаются с использованием технологии туннелирования, причем протоколы туннелирования обеспечивают шифрование и передачу данных между VPN–клиентом и VPN–сервером. Наиболее распространенными VPN–протоколами считаются PPTP, L2TP/IPsec, IKEv2/IPsec, OpenVPN.

PPTP – это VPN протокол, представленный в 1995 году, поддерживающий туннелирование типа «точка–точка». PPTP улучшен по сравнению с предыдущим стандартом PPP, в котором отсутствовала функция туннелирования. Изначально PPTP проектировался как реализация протокола в системах Windows, но быстро стал широко распространенным протоколом VPN, доступным на многих платформах.

PPTP инкапсулирует сетевые данные и помещает их в IP–пакет. Далее каждый последующий пакет также инкапсулирован и, когда маршрутизатор или любое другое устройство сталкивается с таким пакетом, он будет рассматривать его как IP–пакет. Как только данные получены сервером PPTP, они пересылаются в Интернет или на целевое устройство.

Туннель PPTP устанавливается путем связи с одноранговым узлом через TCP–порт 1723. Затем это соединение используется для установки инкапсулирующего туннеля с тем же одноранговым узлом и управления им. Кроме того, на обоих концах туннеля шифрования PPTP протокол будет аутентифицировать передаваемые пакеты данных.

Протокол PPTP поддерживает два типа туннелирования:

1. Добровольное туннелирование. Этот тип туннелирования инициируется клиентом, поэтому поддержка интернет–провайдера или моста не требуется.
2. Обязательное туннелирование. Поскольку этот тип туннелирования инициируется сервером PPTP, необходима поддержка маршрутизатора и сервера доступа к сети.

Раньше PPTP был безопасным, но это уже не так. Проще говоря, безопасность PPTP крайне устарела по современным стандартам, и использование этого протокола для защиты ваших онлайн–данных очень рискованно.

PPTP может использовать MS–CHAP–v1 для аутентификации. Проблема в том, что MS–CHAP–v1 не является безопасным, поскольку существуют инструменты, позволяющие киберпреступникам извлекать хэши паролей NT из обмена.

Хотя PPTP также может использовать MS–CHAP–v2 для аутентификации, но это тоже небезопасный вариант. Так как, MS–CHAP–v2 уязвим для атак по словарю, а кодовую фразу MS–CHAP–v2 D4 можно взломать примерно за 23 часа.

Поскольку MPPE (шифрование, используемое PPTP) использует потоковый шифр RC4, хакер может использовать атаку с переворачиванием битов, чтобы воспользоваться тем фактом, что зашифрованный текст уязвим из–за отсутствия аутентификации потока зашифрованного текста.

Все рассмотренные выше проблемы безопасности уже хорошо известны, и это делает PPTP–трафик весьма вероятной мишенью для хакеров, поскольку он очень уязвим для вредоносных атак.

На сетевом уровне используется протокол Internet Protocol Security (IPSec). IPsec — это совокупность протоколов для обеспечения безопасности информации, передаваемой по публичным сетям. В отличие от SSL–VPN, работающего на прикладном уровне, IPsec работает на сетевом уровне и может использоваться нативно со многими операционными системами, что позволяет использовать его без сторонних приложений.

IPsec шифрует трафик, используя:

* Authentication Header (AH), подписывающий каждый пакет ЭП;
* Encapsulating Security Protocol (ESP), обеспечивающий конфиденциальность, целостность и аутентификацию пакета при передаче.

Очень популярно использования протокола IPsec в паре с L2TP или IKEv2, о чем будет сказано ниже.

Протокол L2TP был представлен в 1999 году в качестве замены устаревшим протоколам L2F и PPTP. Ввиду того, что L2TP не может обеспечить аутентификацию и шифрование, зачастую он используется вместе с IPsec. L2TP/IPsec стандартизирован в RFC 3193 поддерживается и поддерживается многочисленными операционными системами.

По умолчанию L2TP использует 500 порт протокола UDP, но из–за этого легко блокируется брандмауэрами.

L2TP в паре с IPsec является защищенным протоколом и не имеет серьезных проблем в безопасности, в отличие от PPTP. L2TP/IPsec поддерживает такие алгоритмы шифрования как 3DES, AES. Следует отметить, что в настоящее время шифр 3DES считается слабым и редко используется.

Итак, связка протоколов L2TP с IPsec обеспечивает высокую безопасность передаваемого трафика, прост в настройке и поддерживается многими операционными системами. Однако L2TP/IPsec является более медленным и менее эффективным в сравнении с другими протоколами VPN из–за того, что L2TP инкапсулирует данные дважды.

Также вместе с протоколом IPsec применяется Internet Key Exchange version 2 (IKEv2). IKEv2 используется для выполнения взаимной аутентификации и генерации Security Associations (SA). Хоть у IKEv2 закрытый исходный код, ввиду того что он разрабатывался Cisco совместно с Microsoft, существуют реализации протокола с открытым исходным кодом, например, StrongSwan или Openswan.

За счет поддержки технологии Mobility and Multi–homing Protocol (MOBIKE) IKEv2 устойчив к смене сетей, что делает его хорошим выбором для смартфонов, которые регулярно переключаются между различными точками доступа.

Также IKEv2/IPsec может похвастаться поддержкой криптографических алгоритмов Camellia, AES, Blowfish и с 256–битными ключами шифрования.

На сеансовом уровне используются протоколы Secure Socket Layer (SSL) и Transport Layer Security (TLS), который реализует аутентификацию и шифрование между клиентом и сервером. Для функционирования VPN на основе SSL/TLS нет нужды в разработке специального программного обеспечения (ПО) так как любой браузер и почтовый клиент поддерживают этот протокол. К SSL–VPN протоколам относятся протоколы OpenVPN и WireGuard.

OpenVPN — это, на сегодняшний день, один самых популярных VPN–протоколов. Данный протокол разработан компанией OpenVPN Technologies. В связи с тем, что OpenVPN имеет открытый исходный код прошел не одну независимую проверку безопасности.

Протокол OpenVPN стабилен и предлагает хорошую скорость передачи данных. Протокол может работать на любом из портов TCP и UPD, что позволяет ему стать хорошей заменой IPsec, когда провайдер блокирует некоторые протоколы VPN. Также OpenVPN может использоваться на всех основных операционных системах: Windows, Mac OS, Linux, Apple iOS, Android. Следует отметить, что для работы OpenVPN нужно специальное клиентское ПО.

WireGuard — это новый протокол VPN с открытым исходным кодом, представленный в 2018 году. Несмотря на то, что протокол WireGuard так «молод», он уже включен в основной состав ядра Linux 5.6. Это означает, что пользователи Linux могут начать использовать WireGuard после запуска обновления 5.6

Хотя WireGuard был разработан для Linux, это не означает, что им можно пользоваться только на нем WireGuard поддерживается многими операционными системами, в частности Windows, IOS, Android, macOS, BSD.

WireGuard использует современные криптографические алгоритмы такие ​​как Noise, Curve25519, ChaCha20, Poly1305, BLAKE2, SipHash24, HKDF, а также безопасные доверенные конструкции.

WireGuard отличается более высокой производительностью в сравнении с протоколом OpenVPN, но вместе с тем не может работать на TCP.

WireGuard работает только с UDP и официально не поддерживает TCP. Он может свободно использовать любой порт из диапазона незарезервированных портов. Порт UDP по умолчанию — 51820.

**1.4 Методы анализа трафика для выявления соединений виртуальных частных сетей**

Существуют различные индикаторы, указывающие на применение технологии виртуальных частных сетей.

Если перехватить трафик VPN–клиента при подключении к VPN–серверу, то можно понять, что пользователь использует VPN по следующим признакам:

* Отправка большого количества аналогичных запросов на подключение к различным узлам. Представлена на рисунке 1.1.

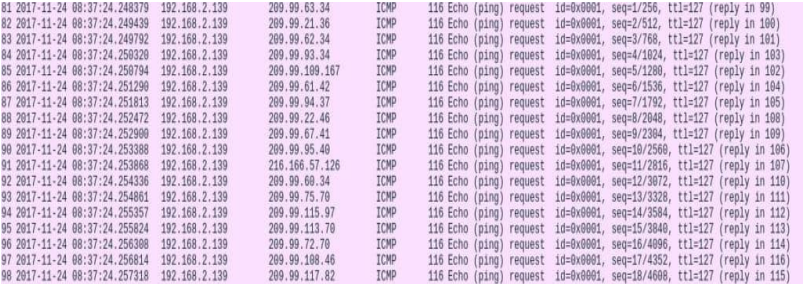


Рисунок 1.1 – Отправка аналогичных запросов на множество IP–адресов

* Далее наблюдается отправка шифрованного трафика к одному из этих IP–адресов. А именно к тому, от которого ответ на эхо–запрос пришел раньше.

Если перехватить трафик VPN–клиента после подключения к серверу VPN, то применив метод глубокого анализа сетевых пакетов (DPI, Deep Packet Inspection), анализирующий не только заголовки, перехваченных пакетов, но и часть данных пакета, можно понять, что пользователь использует VPN по времени жизни пакета – TTL (Time to Live), длине пакета, одинаковому размеру пакетов при регенерации ключа шифрования, максимальному объему данных, который передать одним пакетом – MTU (Maximum Transmission Unit) и по фрагментации трафика.

Значения размера пакетов, TTL и MTU зависят от используемой операционной системы, и установив, что операционной системой является Unix–подобной можно предположить, что используется технология виртуальных частных сетей, так как практически все серверы VPN работают на Unix–подобных серверах. Однако данные параметры пакетов можно изменить, но на это идет небольшое количество энтузиастов.

Существует 2 метода определения протокола с помощью средств DPI:

1) Сигнатурный анализ, включающий в себя разбор пакета «по косточкам», сопоставления заголовков и структуры с образцами. Таким образом детектируются многие туннели, например OpenVPN, SSTP, WireGuard и другие. Детектирование протоколов VPN анализатором трафика представлено на рисунках 1.2 – 1.4.

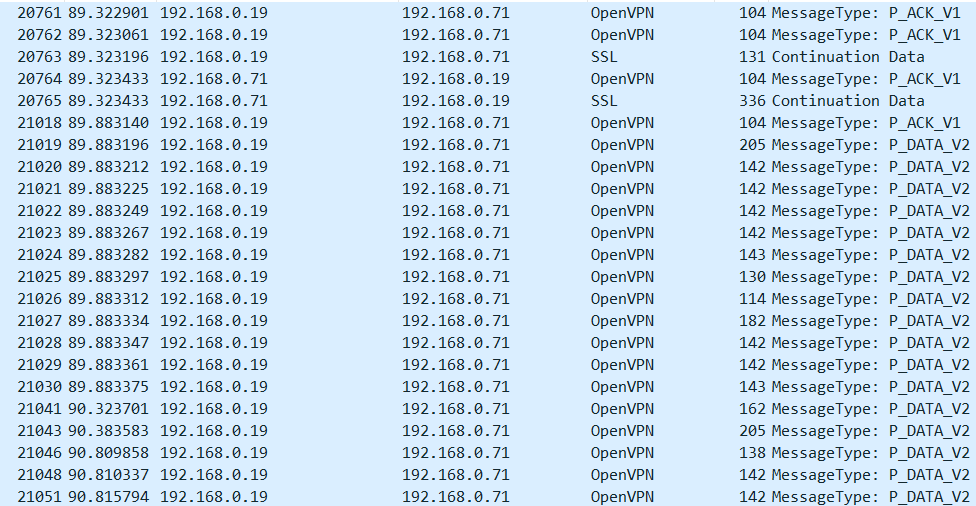


Рисунок 1.2 – Детектирование пакетов OpenVPN

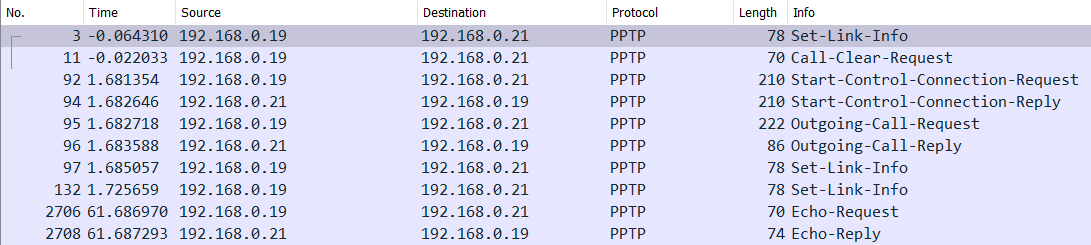


Рисунок 1.3 – Детектирование пакетов PPTP

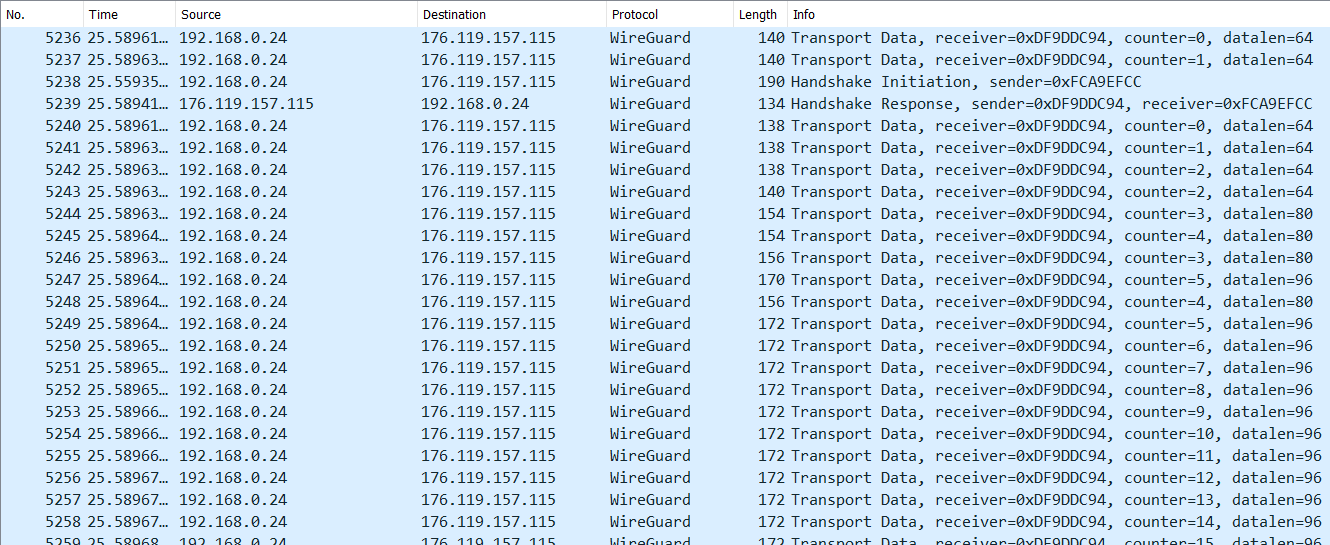


Рисунок 1.4 – Детектирование пакетов WireGuard

2) Предварительный анализ паттернов обмена трафиком, т.е. анализ соотношения входящего трафика к исходящему, периодичности запросов и ответов и других критериев, которые могут позволить определить трафик определенного сетевого протокола.

1. **Методы и средства передачи трафика в сетях VPN и его маскирования**

**2.1 Протокол OpenVPN**

OpenVPN — это, созданное в 2002 году, протокол VPN с открытым исходным кодом, которое использует протокол TLS и позволяет использовать широкий круг конфигураций.

Протокол TLS — это усовершенствованная версия SSL (Secure Socket Layers). Библиотека OpenSSL поддерживает многие алгоритмы симметричного и ассиметричного шифрования, а также хеширования среди которых: Blowfish, Camellia, DES, RC5, AES, ГОСТ 28147–89, RSA, Diffie–Hellman key exchange, ГОСТ Р 34.10–2001, MD5, SHA, ГОСТ Р 34.11–94.

В случае применения симметричного алгоритма перед началом передачи трафика всем узлам сети необходимо разослать секретные ключи шифрования. Однако при этом появляется проблема передачи ключа шифрования без нарушения его конфиденциальности и целостности через общедоступные сети.

В случае использования ассиметричного алгоритма шифрования у клиента и у сервера имеется открытый и секретный ключи шифрования. Открытый ключ применяется для шифрования данных, а секретный для их расшифровки. Алгоритм шифрования с открытым ключом гарантирует возможность расшифровки только с помощью определенного секретного ключа. Секретный ключ должен хранится в пределах компьютера, на котором был сгенерирован. Открытый ключ, в свою очередь, передается всем сторонам, принимающим участие в обмене информацией.

Чтобы передача информации была безопасной нужно идентифицировать всех участников. Иначе можно стать жертвой атаки типа «Человек по середине» (Man in the Middle, MITM). В процессе такой атаки злоумышленник «вклинивается» в канал передачи данных между клиентом и сервером и может перехватить, удалить или модифицировать данные.

Для обеспечения аутентификации в протоколе SSL/TLS используется асимметричные алгоритмы шифрования и инфраструктура открытых ключей (PKI, Public Key Infrastructure).

Необходимо понимать, что расшифровка данных без наличия секретного ключа тоже возможна, например, атакой методом «грубой силы». Несмотря на то что такая атака требует больших вычислительных мощностей, расшифровка данных лишь вопрос времени.

Как уже было сказано, при использовании ассиметричных алгоритмов шифрования публичный ключ применяется для шифрования данных, а секретный для их расшифровки. Во избежание подделки публичного ключа, нужно чтобы этот ключ заверила третья сторона. Для этой цели создан так называемый сертификат открытого ключа.

Данный сертификат должен быть заверен авторитетной организацией. Роль этой организации играет удостоверяющий центр (УЦ).

Если сертификат необходим для публичного использования, например сайт доступный в сети Интернет, то в качестве УЦ должна выступить государственная или коммерческая организация с неоспоримой авторитетом.

Но для сети VPN, создаваемой для личного пользования или своей компании, можно создать свой УЦ и выпустить так называемые самозаверенные сертификаы.

Самозаверенные сертификаты будут использоваться в качестве публичных ключей, которыми шифруются данные клиента OpenVPN.

Где можно разместить OpenVPN протокол в модели OSI? Стандартная модель OSI состоит из семи уровней, в то время как четырехуровневая модель наиболее подходит для TCP/IP, который используется огромным количеством приложений.

Так как протоколы TLS (и SSL) находятся между уровнем протокола приложения и уровнем TCP/IP, где они могут защищать и отправлять данные приложения на транспортный уровень, то и OpenVPN работает на тех же уровнях. Инкапсуляция пакетов в OpenVPN представлена на рисунке 2.1.

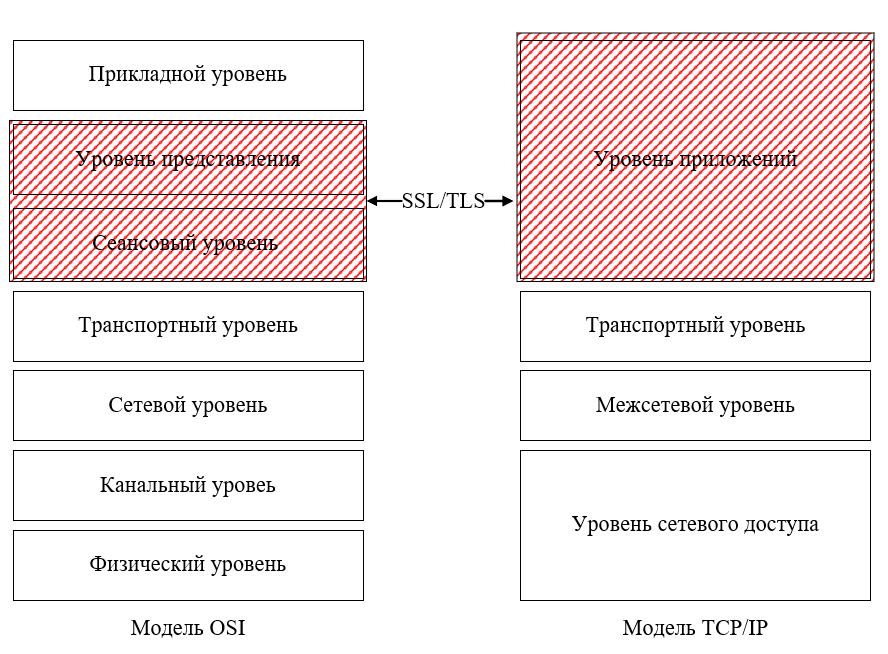


Рисунок 2.1 – Инкапсуляция пакета OpenVPN

В OpenVPN шифрованные кадры инкапсулируются в сегменты TCP или дейтаграммы UDP. Далее дейтаграммы шифруются одним из алгоритмов, поддерживаемых библиотекой OpenSSL, и получают заголовки с информацией о VPN–сервере. Затем пакеты передаются поверх IP в виде сегментов TCP или дейтаграмм UDP через виртуальное сетевое устройство TUN в физическую сеть к удалённому получателю. На рисунке 2.2 показано структура пакетов в OpenVPN.

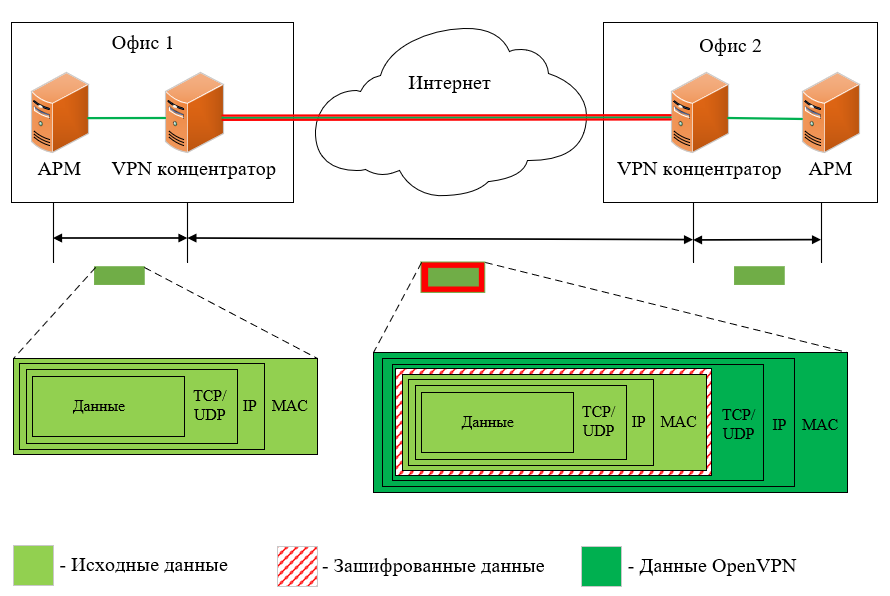


Рисунок 2.2 – Структура пакета OpenVPN

**2.2 Маскирование VPN–трафика с использованием SoftEther**

SoftEther VPN — это бесплатное, кроссплатформенное, многопротокольное программное обеспечение VPN–клиента и VPN–сервера с открытым исходным кодом, разработанное в рамках исследования кандидатской диссертации Дайю Нобори в Университете Цукуба.

Решение имеет большой спектром возможностей:

– собственный протокол SSL–VPN, который не отличим от HTTPS траффика. Также имеется функция маскировки трафика под DNS или ICMP.

– Поддержка большинства существующих протоколов VPN: L2TP/IPsec, SSTP, OpenVPN, причем для L2TP указана строгая совместимость со встроенными клиентами в iOS и Android. Т.е. к серверу SoftEther VPN можно подключить клиента OpenVPN или подключиться с использованием встроенных VPN–механизмов Windows. Причем одновременно.

– Сервер может быть установлен на Windows, Linux, OS X, FreeBSD и Solaris.

– Обладает высокой пропускной способностью.

– Поддержка стандартов шифрования и хеширования таких как: RC4, AES128, AES256, DES, 3DES, MD5, SHA–1.

Программное обеспечение состоит из серверной и клиентской части и бридж–сервер. Графический интерфейс предусмотрен только для Windows. Клиент нужен для подключения одного компьютера к LAN (Remote Access VPN), а бридж–сервер для соединения двух или более сетей (Site–to–Site VPN). Нужно заметить, что GUI–утилита может работать не только с локальным сервером, т.е. предусмотрена возможность удаленного администрирования сервера на Linux через GUI–утилиту под Windows.

В SoftEther инкапсулирование трафика производится с помощью протокола TLS/SSL. Кадры исходного трафика «заворачиваются» в данные HTTPS и шифруются при помощи одного из алгоритмов шифрования. Далее данные получают заголовки с информацией о VPN–сервере. Затем пакеты передаются поверх IP в виде TCP сегментов в физическую сеть к удалённому получателю. На рисунке 2.3 показана структура пакетов SoftEther:

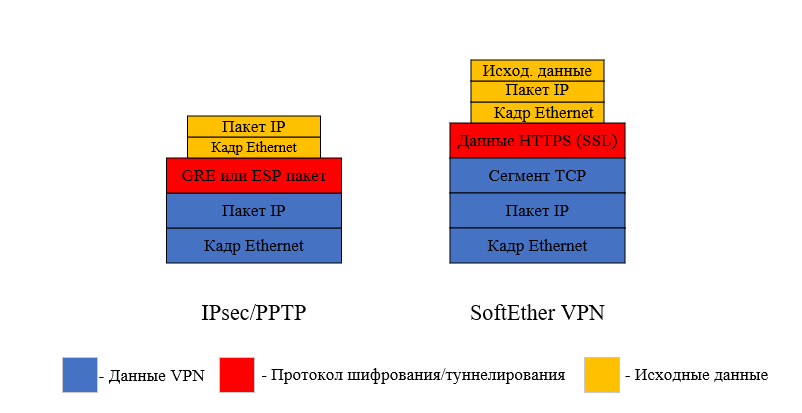


Рисунок 2.3 – Сравнение структуры пакетов IPsec/PPTP и SoftEther VPN

Некоторые сети, такие как Wi–Fi в аэропортах и Интернет в гостиничных номерах, ограничивают использование протоколов, кроме HTTP и HTTPS, по соображениям безопасности. В такой жестко ограниченной сети, где невозможно использование протоколов таких как IPSec и PPTP, единственным способом использования VPN является SoftEther VPN, который основан на SSL–VPN. Технически это HTTPS (HTTP через SSL).  HTTPS может проходить любые брандмауэры, которые запрещают VPN на основе IPsec. Маскировка трафика в SoftEther представлена на рисунке 2.4.

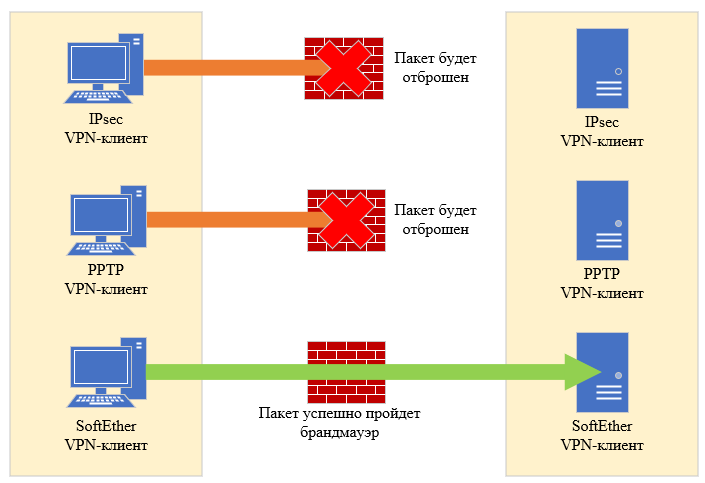


Рисунок 2.4 – Маскировка трафика в SoftEther VPN

Также SoftEther умеет обходить глубокую проверку пакетов за счёт построения множественных соединений TCP.

Некоторые брандмауэры на современном рынке могут обнаруживать ненормальное поведение TCP–соединений, проходящих через брандмауэр. При наличии такого брандмауэра при выходе в Интернет в сети VPN–сессия SoftEther VPN может быть определена как аномальное TCP–соединение и также может быть прервана брандмауэром. Поддерживать надежные и стабильные сеансы VPN будет рискованно.

Поскольку SoftEther VPN использует протокол HTTPS в качестве туннеля для передачи внутренних пакетов VPN, соединение HTTPS/TCP будет двунаправленным. В стандартном поведении HTTPS есть максимальные числа переключений направления в одной и той же TCP–сессии от установления сессии до ее завершения, и они равны 15, как определено в RFC протокола HTTP 1.1.И если SoftEther VPN использует одно соединение HTTPS/TCP для туннелирования, количество переключений направления должно превышать 15, что невозможно при обычном использовании HTTPS, то средство DPI, отключит этот сеанс HTTPS.

Чтобы уменьшить риск быть обнаруженным, как аномальное соединение, у SoftEther VPN есть два механизма. Первый, SoftEther VPN делит все TCP–соединения, составляющие логическую сессию VPN, на две группы. Первая группа предназначена только для исходящего трафика, а другая группа предназначена только для входящего трафика. Этот дешевый трюк должен помочь скрыть ненормальное поведение. Второй, SoftEther VPN устанавливает время жизни для каждого из всех TCP–соединений, так как брандмауэр может определить слишком длительное TCP–соединение как ненормальное и разорвать его. Перед этим SoftEther VPN добровольно завершит жизнь TCP–соединения и установит новое.

Эти два механизма могут помочь предотвратить обнаружение сеанса VPN как ненормального брандмауэрами с полной проверкой пакетов. Маскировка трафика в SoftEther VPN представлена на рисунке 2.5.

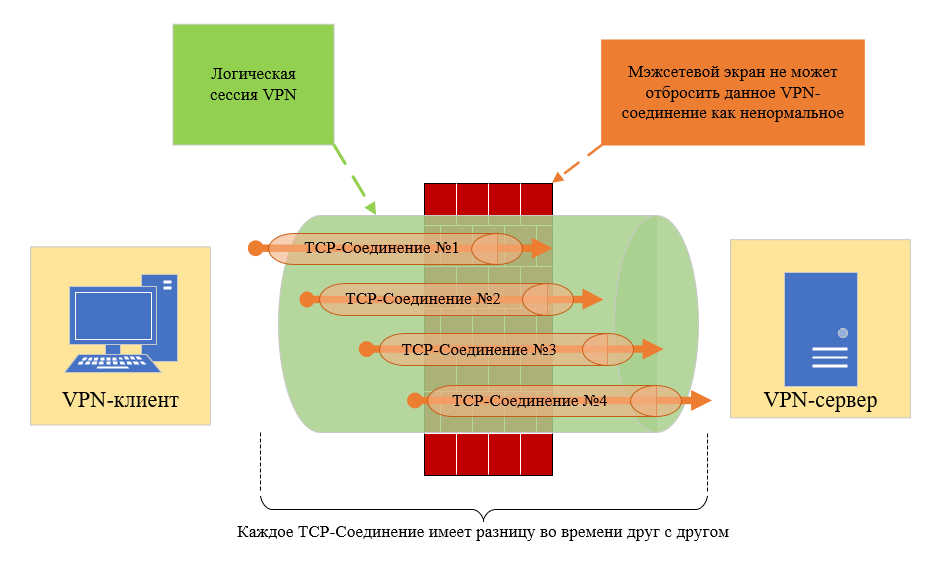


Рисунок 2.5 – Маскировка трафика в SoftEther VPN

Логический сеанс VPN состоит из множества соединений TCP.  
Каждое TCP–соединение имеет очень короткий срок жизни.  
Брандмауэр на пути трафика не может идентифицировать их как сеанс VPN.

В некоторых ограниченных сетях разрешают передавать только пакеты ICMP или DNS. И чтобы можно было установить клиент–серверный сеанс SoftEther VPN через такую ​​очень ограниченную сеть, SoftEther VPN имеет функцию «VPN через ICMP» и «VPN через DNS».

Эта функция позволяет проникнуть через такой ограниченный брандмауэр. Все пакеты VPN объединяются в пакеты ICMP или DNS для передачи через брандмауэр. Конечная точка на стороне получателя извлекает внутренний пакет из капсулированного пакета.

Это очень полезно для использования общедоступного Wi–Fi. Некоторые общедоступные сети Wi–Fi могут передавать только пакеты ICMP или DNS. Они фильтруют пакеты TCP или UDP.

VPN через ICMP и VPN через DNS реализованы на основе спецификаций протоколов ICMP и DNS. Однако иногда они использование этой функции может привести к переполнению памяти или другим проблемам на маршрутизаторах. На рисунке 2.6 представлена функция VPN через ICMP/DNS.

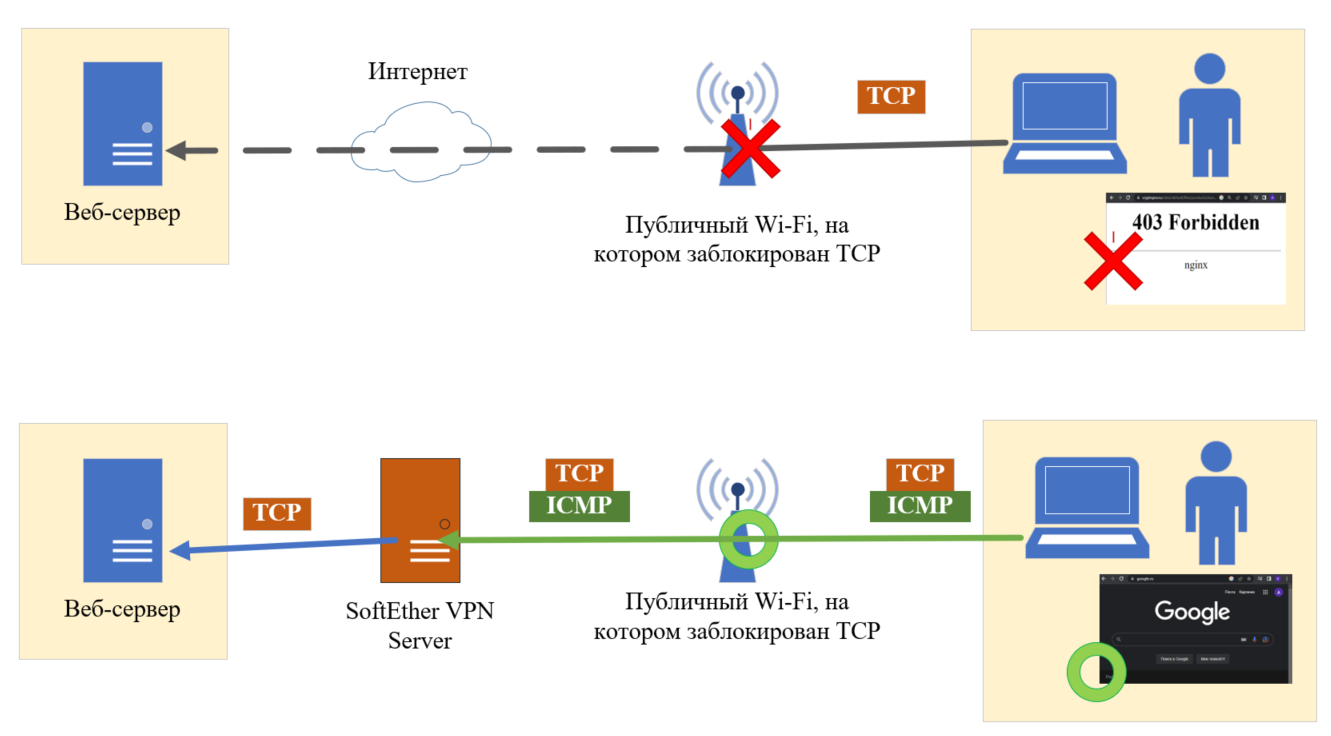


Рисунок 2.6 – Функция VPN через ICMP/DNS

**2.3 Маскирование VPN–трафика с использованием Stunnel**

Stunnel — это приложение, которое «заворачивает» во внешний слой шифрования TLS пакеты любого сетевого протокола.

Stunnel дает возможность шифрования данных между каким–либо приложением на стороне клиента, которое взаимодействует с серверной частью этого приложения на удаленном узле. Шифрование производится между клиентской и серверной частью Stunnel без надобности вносить изменения в конфигурацию программного обеспечения, трафик которого хотим скрыть. Помимо шифрования, имеется возможность организации аутентификации по сертификату.

Особенность Stunnel заключается в том, что данное ПО позволяет «завернуть» в ssl–туннель данные абсолютно любого приложения, не имеющего встроенных средств шифрования, но в то время зашифрованные данные можно передать через Stunnel–туннель, чтобы замаскировать его под обмен по https–траффик, что дает возможность обхода блокировок и средств глубокой проверки пакетов.

Имеется возможность использовать Stunnel в клиентском либо в серверном режимах. В режиме клиента Stunnel получает данные от произвольного приложения, шифрует его и транслирует трафик на Stunnel–сервер. Сервер Stunnel, в свою очередь, расшифровывает полученные данные и перенаправляет их целевому приложению или службе.

Для работы Stunnel в режиме сервера необходимо наличие сертификата аутентификации. Клиенту для установления соединения с сервером наличие сертификата не обязательно.

**3. Практическая реализация методики маскирования VPN–трафика**

**3.1 Общая структура телекоммуникационной системы**

Общая структура телекоммуникационной системы состоит из VPN–клиента, VPN–сервера и веб–сервера и имеет следующий вид и представлена на рисунке 3.1.

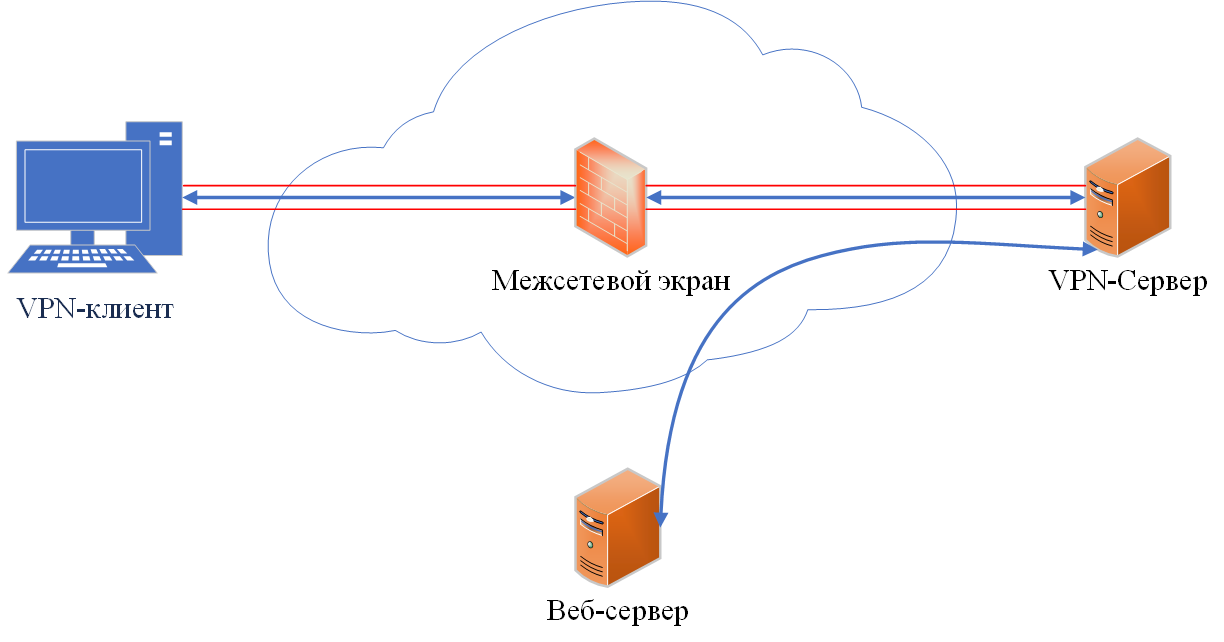


Рисунок 3.1 – Общая структура телекоммуникационной системы

Сначала трафик генерируется и обрабатывается на стороне клиента. Затем, с VPN–клиента в замаскированном виде отправляется на VPN–сервер через сеть Интернет. После получения, VPN–сервер расшифровывает и передает трафик на веб–сервер.

Разница между реализациями маскировки с помощью Openvpn с Stunnel и WireGuard в паре с Cloak заключается в том, что трафик с OpenVPN–клиента попадает на Stunnel клиент по 1194 порту TCP, а в случае с Wireguard трафик с Wireguard–клиента попадает на Cloak клиент по 51820 порту UDP.

В случае с SoftEther трафик сразу шифруется и маскируется в клиентском ПО SoftEther VPN.

Схемы сетей, на примере которых было реализовано маскирование с помощью OpenVPN+Stunnel, Wireguard+Cloak, SoftEther приведены на рисунках 3.2 – 3.4.

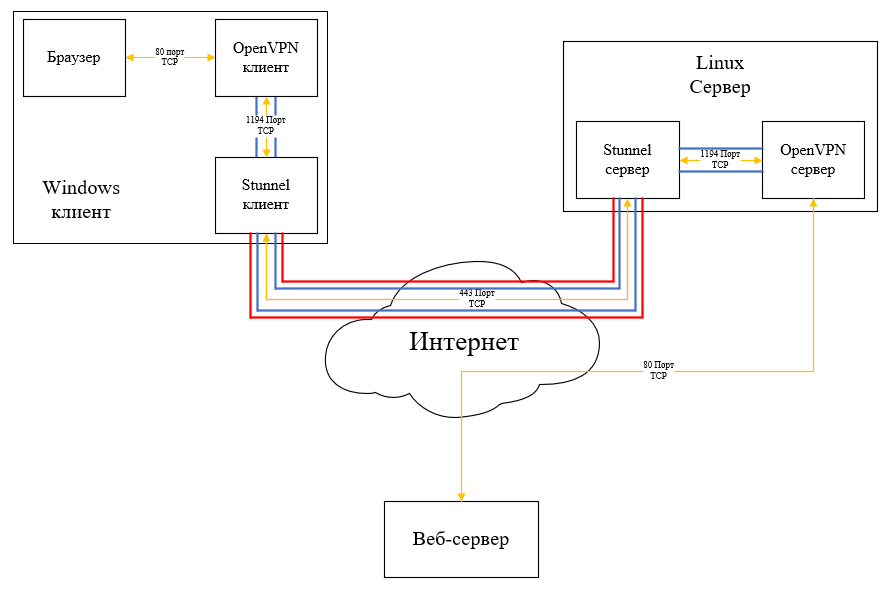


Рисунок 3.2 – Схемы сети, на примере которой было реализовано маскирование с помощью Stunnel

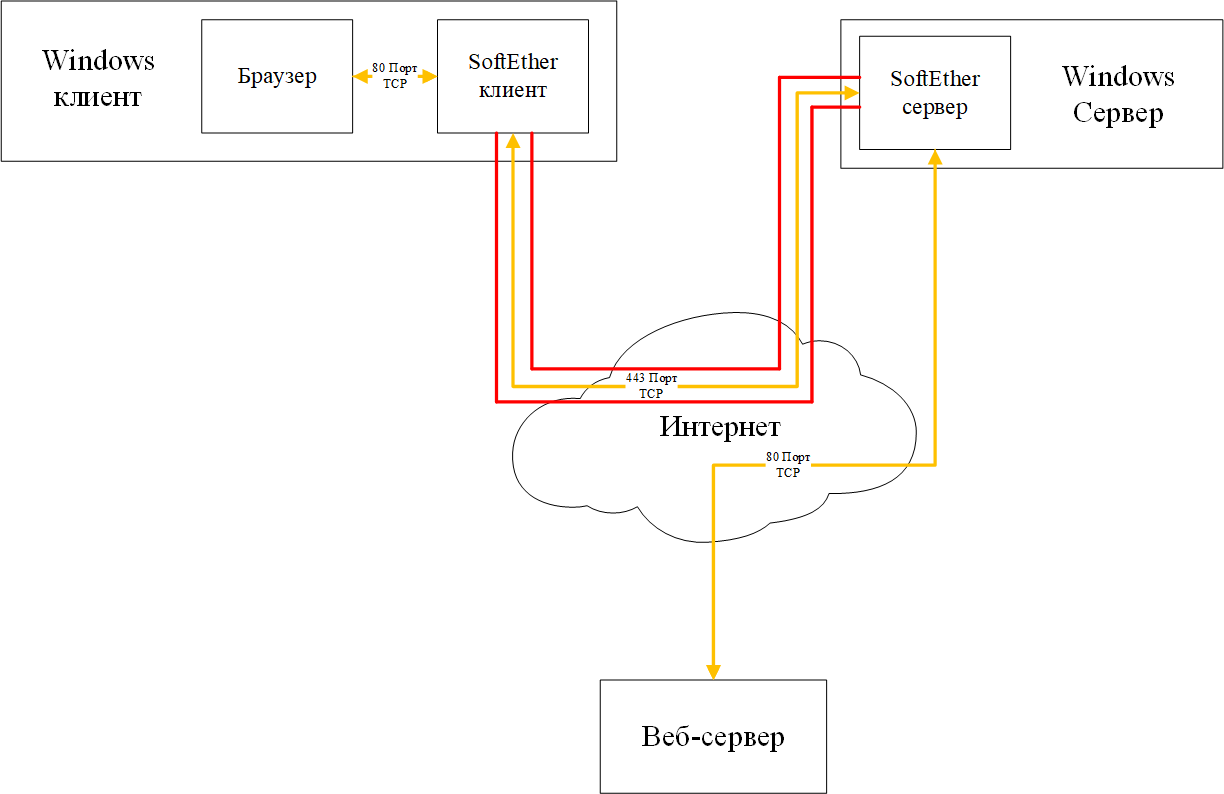


Рисунок 3.3 – Схемы сети, на примере которой было реализовано маскирование с помощью SoftEther.

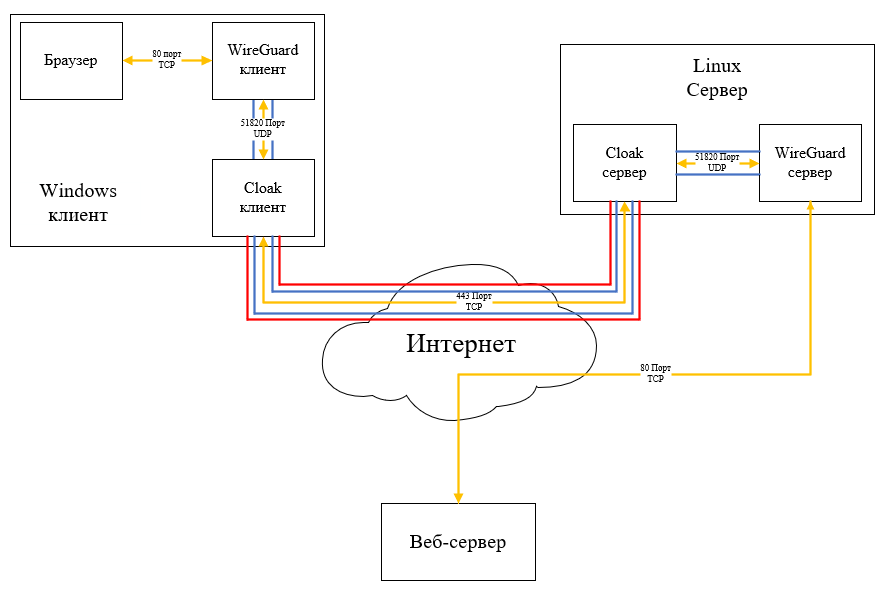


Рисунок 3.4 – Схемы сети, на примере которой было реализовано маскирование с помощью Cloak.

**3.2 Программно–аппаратные средства реализации**

В качестве VPN–клиента использовалась виртуальная машина на операционной системе «Windows» и выходом в глобальную сеть Интернет, IP–адрес динамический, серый.

Технические характеристики виртуальной машины:

* 4 выделенных ядра процессора Intel(R) Core (TM) i5 CPU 11400;
* ОЗУ 4 ГБ;
* ПЗУ 40 ГБ SSD;
* Тип системы (64–разрядная ОС);
* Версия Windows (Windows 10 Pro).

На виртуальной машине установлено следующее программное обеспечение:

* OpenVPN 2.5.8–l604 amd64;
* OpenVPN Connect
* Stunnel
* SoftEther VPN Client
* WireGuard
* Cloak Client v2.6.0
* Wireshark 4.0.2 64-bit
* WinSCP 5.21.6;
* NPcap.

Для настройки серверной части OpenVPN использовалась виртуальная машина на операционной системе «Debian» по причине того, что данный дистрибутив нетребователен к техническим параметрам устройства, имеет высокий уровень быстродействия, стабилен ввиду долгосрочной поддержки, а также бесплатный. Данная виртуальная машина имеет выход в глобальную сеть Интернет, статичный белый IP–адрес – 45.82.153.151.

Технические характеристики виртуальной машины:

* ЦП 1 ядро 2.2 ГГц;
* ОЗУ 512 МБ;
* ПЗУ 10 HDD;
* Тип системы (64-разрядная ОС);
* Версия Windows (Debian 10).

На виртуальной машине установлено следующее программное обеспечение:

* OpenVPN;
* Stunnel4;
* OpenSSH Server.

В качестве VPN–сервера для реализации маскировки с помощью WireGuard использовалась виртуальная машина на операционной системе «Debian» и выходом в глобальную сеть Интернет со статичным белым IP–адресом – 176.119.157.115.

Технические характеристики виртуальной машины:

* ЦП 1 ядро 2.2 ГГц;
* ОЗУ 512 МБ;
* ПЗУ 10 HDD;
* Тип системы (64-разрядная ОС);
* Версия Windows (Debian 10).

На виртуальной машине установлено следующее программное обеспечение:

* WireGuard;
* Cloak Server v2.6.0;
* OpenSSH Server.

Для настройки серверной части SoftEther VPN было принято решение использовать виртуальную машину на операционной системе «Windows» ввиду того, что программное обеспечение SoftEther VPN для Windows имеет удобный графический интерфейс. Виртуальная машина имеет выход в глобальную сеть Интернет, IP–адрес статический, серый – 192.168.0.22.

Технические характеристики виртуальной машины:

− 4 выделенных ядра процессора Intel(R) Core (TM) i5 CPU 11400;

− ОЗУ 4 ГБ;

− ПЗУ 40 ГБ SSD;

− Тип системы (64-разрядная ОС);

− Версия Windows (Windows 10 Pro).

На виртуальной машине установлено следующее программное обеспечение:

− SoftEther VPN Server.

**3.3 Настройка маскирования VPN–трафика в OpenVPN**

Создание VPN–канала начинается с настройки серверной части. Настройка VPN–сервера выполнялась с помощью команд, перечисленных ниже. Все команды были выполнены в режиме суперпользователя.

В Debian 10 межсетевым экраном по умолчанию является утилита командной сроки iptables. Для использования утилиты требуются привилегии суперпользователя.

Для обеспечения информационной безопасности сервера необходимо закрыть все входящие соединения, кроме соединений по портам использующимся SSH (22 порт TCP) и Stunnel (443 порт TCP). Закроем все входящие соединения, кроме вышеуказанных с помощью команд:

iptables -A INPUT -p tcp --dport 22 -j ACCEPT

iptables -A INPUT -p tcp --dport 443 -j ACCEPT

iptables -P INPUT DROP

Установим OpenVPN и Easy–RSA. Easy–RSA — это инструмент управления инфраструктурой открытых ключей (PKI), который будет использоваться на сервере OpenVPN для генерации запроса сертификата, который затем будет проверяться и подписываться в Центре Сертификации (ЦС).

apt install openvpn easy-rsa

Далее создадим папку для ключей и перейдём в неё:

mkdir /etc/openvpn/keys

cd /etc/openvpn/keys

Все операции для генерации ключей и сертификатов можно выполнить с помощью утилиты OpenSSL, но легче воспользоваться специально созданной для этого программой Easy–RSA. Ранее Easy–RSA установилась вместе с OpenVPN, но это уже отдельный проект. Теперь необходимо скачать её и создать файл настроек из прилагаемого образца:

wget https://github.com/OpenVPN/easy-rsa/archive/master.zip

unzip master.zip

cd /etc/openvpn/keys/easy-rsa-master/easyrsa3

cp vars.example vars

Далее нужно перейти в директорию /etc/openvpn/keys/easy-rsamaster/easyrsa3 и в ней открыть файл vars. В данном файле нужно раскомментировать строки с ключом с ключом «REQ», наличие этих параметров обязательно для генерации ключа. Также раскомментируем параметры, задающие длину ключа:

#set\_var EASYRSA\_KEY\_SIZE 2048

#set\_var EASYRSA\_DIGEST «sha256»

Для повышения стойкость шифрования RSA, увеличим длину ключей до наибольшей – заменим 2048 на 4096, а sha256 на sha512.

Теперь необходимо создать инфраструктуру публичных ключей (PKI). В целом, PKI основывается на использовании криптосистемы с открытым ключом и наличии удостоверяющего центра. Ключи создаются парами – закрытый и открытый. Для обмена с кем–либо защищённой информацией мы обмениваемся открытыми ключами. В данном случае сервер будет иметь свой закрытый ключ и открытые ключи клиентов. У клиентов есть свои закрытые ключи и открытый ключ сервера. А удостоверять подлинность ключей будет удостоверяющий центр, который мы также создадим самостоятельно, и у всех участников обмена корневой будет его корневой сертификат. Порядок действий для создания PKI следующий:

1. Инициализировать PKI;
2. Создать удостоверяющий центр – Certificate Authority;
3. Сгенерировать сертификаты сервера;
4. Сгенерировать сертификаты клиента;
5. Создать файл параметров Диффи–Хеллмана;

Выполним команду инициализации и создадим свой удостоверяющий центр (СА) с помощью команд:

./easyrsa init-pki

./easyrsa build-ca

В результате получаем файлы: ca.crt (корневой сертификат – открытый ключ, который будет передаваться клиентам) и ca.key (закрытый ключ, который не должен быть скомпрометирован)

Теперь необходимо создать пару ключей, собственно, для VPN–сервера. Закрытый ключ сервера мы не будем защищать паролем, так как вводить этот пароль пришлось бы при каждой перезагрузке сервера. Создадим запрос на сертификат с помощью команды:

./easyrsa gen-req server nopass

Будут созданы два файла: server.key – закрытый ключ сервера, server.req – файл запрос удостоверяющему центру на подписание сертификата. Далее требуется подписать его:

./easyrsa sign-req server server

Подтверждаем операцию и вводим пароль закрытого ключа удостоверяющего центра (УЦ). Получим подписанный открытый ключ сервера – server.crt.

Далее, в случае с выбором алгоритма RSA, следует сгенерировать файл параметров Диффи–Хеллмана. Это обеспечит использование надёжной схемы шифрования, при которой даже компрометация секретного ключа не позволит расшифровать записанный трафик с предыдущих сессий. Сгенерируем файл с помощью команды:

./easyrsa gen-dh 67

На выходе получаем файл dh.pem. Также можно создать список отозванных сертификатов на случай утери какого–либо устройства с OpenVPN–клиентом. Процедура отзыва сделает утерянный ключ недействительным

Дополнительно мы задействуем механизм HMAC (hash-based message authentication code), который служит для проверки целостности передаваемых данных, чтобы исключить возможность «атаки посредника». Для включения HMAC потребуется сгенерировать специальный ключ и добавить в конфигурационный файл сервера директиву tls–auth, указывающую на данный ключ. Тогда сервер будет добавлять подпись HMAC ко всем пакетам рукопожатия SSL/TLS. Любой UDP–пакет, не имеющий правильной подписи, может быть отброшен без дальнейшей обработки. HMAC–подпись, устанавливаемая директивой tls-auth, обеспечивает повышенный уровень безопасности в дополнение к механизмам самого протокола SSL/TLS. Это может защитить от:

– DoS–атак или флуда на UDP–порт OpenVPN.

– Сканирования портов с целью определения, прослушиваемых сервером UDP–портов.

– Уязвимостей, связанных с переполнением буфера в реализации SSL/TLS.

– Попыток инициации SSL/TLS–рукопожатия от несанкционированной машины (хотя, в конечном итоге, такие рукопожатия не пройдут аутентификацию, tls-auth может отсечь их на гораздо более ранней стадии).

Сгенерируем ключ:

openvpn --genkey --secret ta.key

Данный ключ будет также передан клиенту.

На данном этапе сервер уже готов к работе, но необходимо ещё создать ключи клиентов и правильные файлы конфигурации. Переходим снова в папку EasyRSA, создаём и подписываем ключ:

cd /etc/openvpn/keys/easy-rsa-master/easyrsa3

./easyrsa gen-req client\_name nopass

./easyrsa sign-req client client\_name

Теперь, когда все ключи созданы, конфигурируем и запускаем сервер. В папке /etc/openvpn создаём файл server.conf (или заменяем существующий). Содержимое использованного файла приведено в приложении.

Для перенаправления трафика через сеть VPN необходимо в файле /etc/sysctl.conf раскомментировать строки:

net.ipv4.ip\_forward = 1

net.ipv6.conf.all.forwarding=1

Для применения настроек выполняем команду:

sysctl -p /etc/sysctl.conf.

Запустим OpenVPN и включим автозапуск службы OpenVPN при загрузке сервера с помощью команд:

systemctl -f enable openvpn-server@server.service

systemctl start openvpn-server@server.service

Затем необходимо проверить, активна ли служба командой:

systemctl status openvpn@server

Результат проверки активности Openvpn представлен на рисунке 3.5.

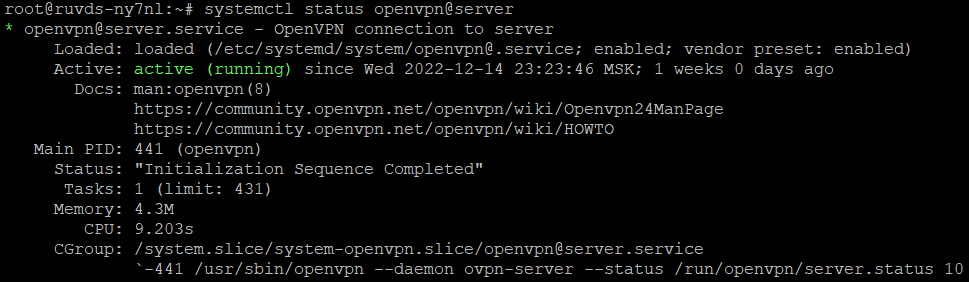


Рисунок 3.5 – Результат проверки активности Openvpn

Настройка серверной части Stunnel выполняется в три этапа:

1. Установка Stunnel
2. Генерация закрытого ключа и сертификата
3. Настройка конфигурационного файла

Установка Stunnel производится с помощью команды:

apt install stunnel4 -y

Сгенерируем закрытый ключ и сертификат для сервера Stunnel с помощью утилиты OpenSSL:

openssl genrsa -out key.pem 2048

openssl req -new -x509 -key key.pem -out cert.pem -days 3650

Далее требуется отредактировать файл конфигурации Stunnel. Откроем файл с помощью текстового редактора:

nano /etc/stunnel/stunnel.conf

И вставим следующие строки:

pid = /var/run/stunnel4/stunnel.pid

output = /var/log/stunnel4/stunnel.log

setuid = stunnel4

setgid = stunnel4

[openvpn]

cert=/etc/stunnel/cert.pem

key=/etc/stunnel/key.pem

accept = 0.0.0.0:443

connect = 127.0.0.1:1194

Строка accept говорит о том, что stunnel будет прослушивать порт 443, а строка connect о том, что трафик пришедший трафик будет перенаправлен на 1194 порт, который прослушивается OpenVPN.

После настройки Stunnel следует включить его автозапуск. Для этого необходимо в конфигурационном файле “stunnel4”, который находится в директории /etc/default/, значение параметра “ENABLED” поменять на 1.

На последнем этапе остается только запустить Stunnel и проверить активен ли он. Результат проверки активности Stunnel представлен на рисунке 3.6.

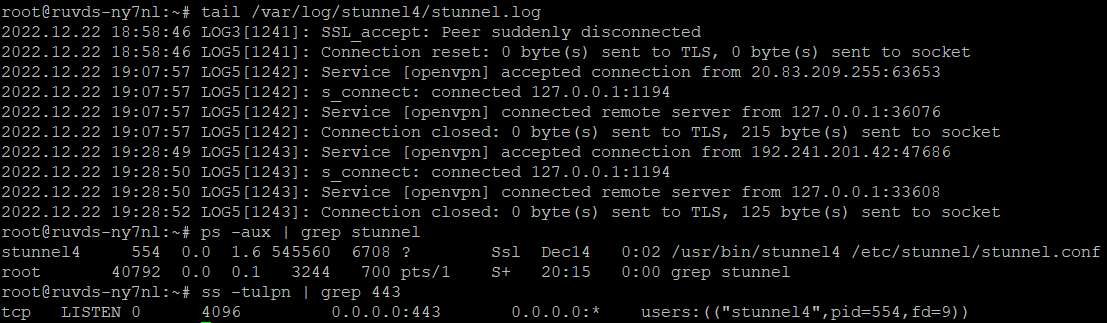


Рисунок 3.6 – Результат проверки активности Stunnel

Теперь, когда VPN–сервер полностью готов, настроим клиентскую часть. Для этого загрузим файл конфигурации клиента OpenVPN с помощью scp инструмента, входящего в состав Windows PowerShell командой:

scp -P 22 root@45.82.153.151:client1.ovpn Downloads

Далее требуется установить Stunnel и его после успешной установки запустить. Для этого необходимо щелкнуть правой кнопкой мыши значок Stunnel на панели задач в правом нижнем углу рабочего стола Windows.

Далее нужно выбрать **«**Edit Configuration**»** и настроить Stunnel следующим образом:

output = stunnel.log

client = yes

[openvpn]

sni = www.bing.com

accept = 127.0.0.1:1194

connect = 45.82.153.151:443

После окончания настройки Stunnel установим на клиент OpenVPN. Затем нужно добавить конфигурацию добавить VPN–клиента, предварительно загрузив ее с сервера. Содержимое файла приведено в приложении

В конце можно проверить VPN соединение, для этого нужно узнать свой IP–адрес, с которого идут обращения в Интернет. Результат проверки VPN–соединения представлен на рисунке 3.7.

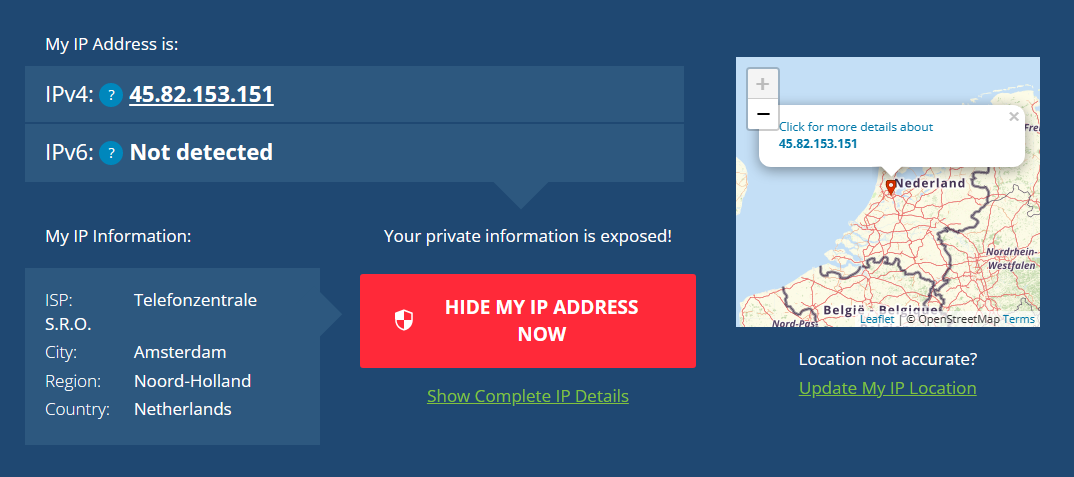


Рисунок 3.7 – Результат проверки VPN–соединения

**3.4 Настройка маскирования VPN–трафика в SoftEther**

Сначала настроим VPN–сервер, для этого загрузим последнюю версию программного обеспечения и установим его. Единственный компонент, который понадобиться для данной цели — это SoftEther Server. Окно установщика SoftEther VPN представлено на рисунке 3.8.

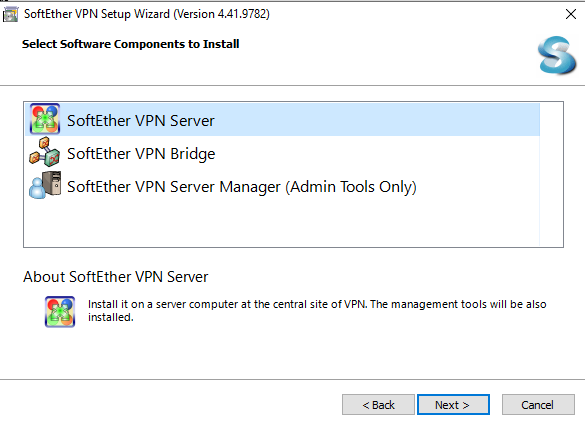


Рисунок 3.8 – Окно установщика SoftEther VPN

После установки программного обеспечения откроется окно диспетчера серверов. Необходимо выбрать localhost (этот сервер) и нажать «Connect». Интерфейс диспетчера серверов SoftEther VPN представлен на рисунке 3.9.



Рисунок 3.9 – Окно диспетчера серверов SoftEther VPN

Далее требуется придумать название для виртуального концентратора и выбрать тип VPN. На выбор доступно создание сервера для удаленного подключения или VPN типа точка–точка.

После создания сервера появится диалоговое окно для настройки динамического DNS. Динамический DNS гарантирует, что VPN–сервер может быть доступен через брандмауэры или если интернет–провайдер назначил динамический IP–адрес. В этом диалоговом окне можно придерживаться настроек по умолчанию и выйти.

Затем необходимо создать пользователя. В появившемся нужно указать имя пользователя и пароль, также можно добавить пользователя в группу и выбрать тип аутентификации. Окно создания пользователя представлено на рисунке 3.10.

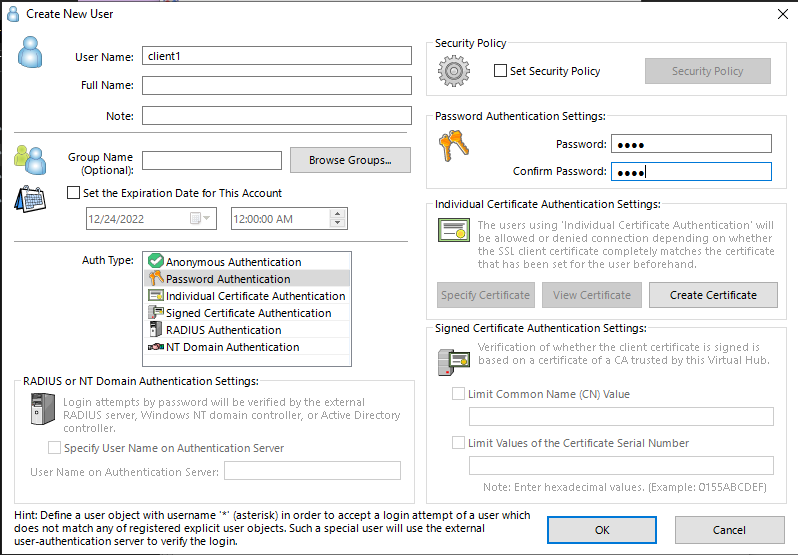


Рисунок 3.10 – Окно создания пользователя

Затем, когда центр управления пользователями будет закрыт, отрытым останется окно управления VPN–сервером. Здесь можно поменять алгоритмы шифрования трафика, порты, которые будет прослушивать сервер, производится настройка DNS. Также, в данном окне имеется возможность конфигурирования OpenVPN, IPsec/L2TP, MS–SSTP соединений. Окно управления сервером представлено на рисунке 3.11.

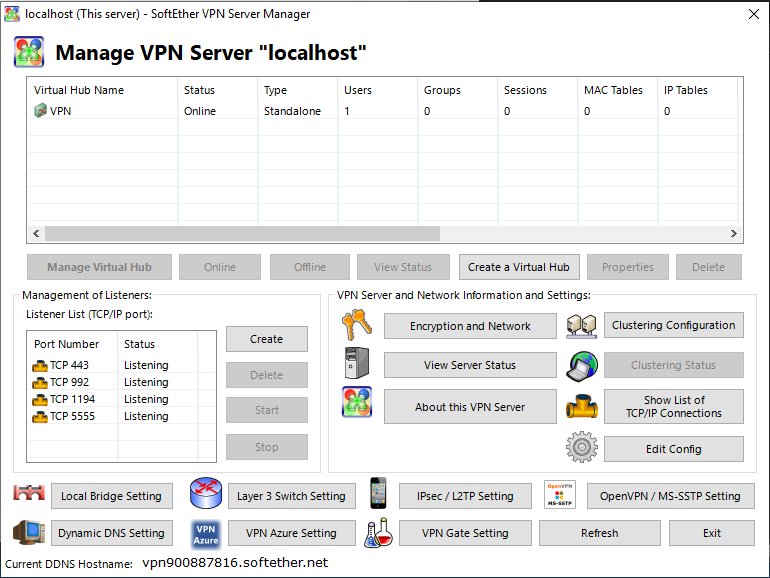


Рисунок 3.11 – Окно управления сервером

Следующий шаг необязателен, но рекомендуется. Он гарантирует, что подключенные пользователи могут использовать VPN в качестве точки доступа в Интернет, но не могут получить доступ к вашей локальной сети. Для включения этой функции нужно выбрать «Управление виртуальным концентратором» далее «Виртуальный NAT и виртуальный DHCP (SecureNAT)» затем «Включить SecureNAT».

Также рекомендуется отключить прослушивание сервером 992, 1194, 5555 портов TCP.

После подготовки VPN–сервера настроим клиентскую часть. Для начала требуется скачать и установить SoftEther VPN Client.

Чтобы подключиться к серверу SoftEther, нужно выбрать пункт создания нового подключения и, в открывшемся окне, заполнить поля: «Host name», «Port number», «Virtual Hub Name», «Username», «Password». Окно настройки VPN–клиента представлено на рисунке 3.12.

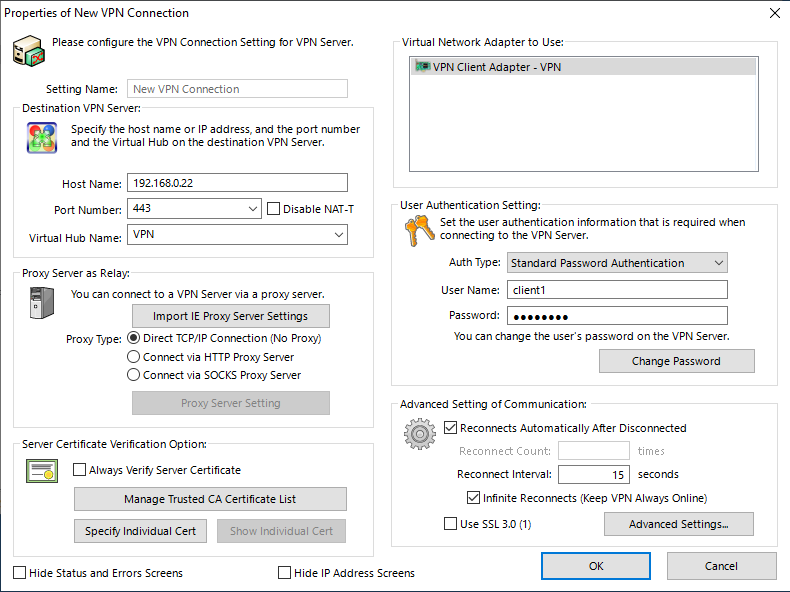


Рисунок 3.12 – Окно настройки VPN–клиента

Также для маскировки следует отключить функцию «UDP Acceleration». Эта функция увеличивает скорость передачи данных по VPN–каналу за счёт параллельной отправки данных по протоколу UDP, но в тоже время это деанонимизирует VPN подключение. Для отключения данной функции необходимо выбрать пункт «Disable UDP Acceleration». Продвинутые настройки представлены на рисунке 3.13.

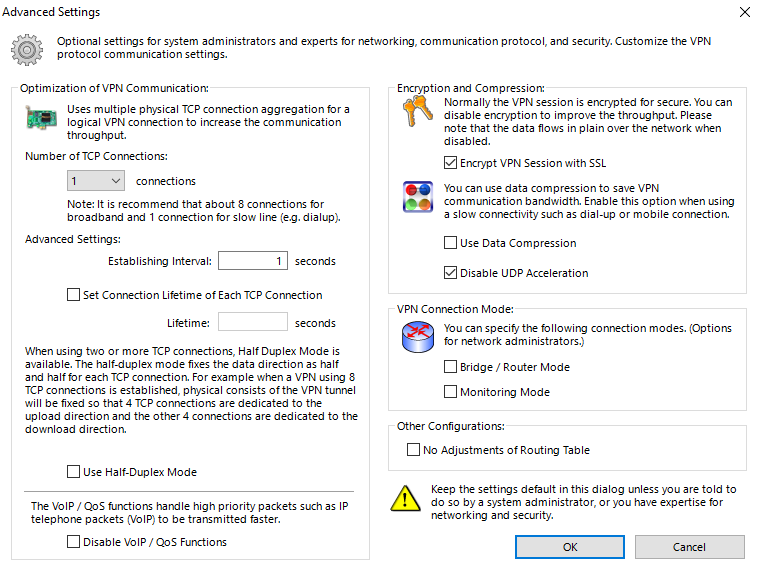


Рисунок 3.13 – Продвинутые настройки SoftEther

Для того чтобы удостовериться что VPN соединение успешно создано попробуем подключиться к серверу по VPN. При успешном подключении статус сессии должен поменяться на «Connected». Результат проверки VPN–соединения представлен на рисунке 3.14.

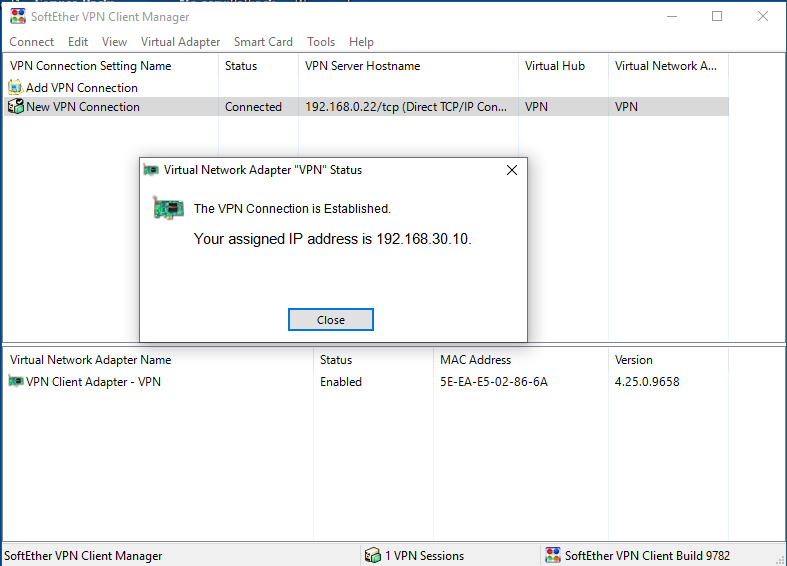


Рисунок 3.14 – Результат проверки соединения

**3.5 Настройка маскирования VPN–трафика в WireGuard**

Создание VPN–канала начинается с настройки серверной части. Настройка VPN–сервера выполнялась с помощью команд, перечисленных ниже. Все команды были выполнены в режиме суперпользователя.

В Debian 10 межсетевым экраном по умолчанию является утилита командной сроки iptables. Для использования утилиты требуются привилегии суперпользователя.

Для обеспечения информационной безопасности сервера необходимо закрыть все входящие соединения, кроме соединений по портам использующимся SSH (22 порт TCP) и Cloak (443 порт TCP). Закроем все входящие соединения, кроме вышеуказанных с помощью команд:

iptables -A INPUT -p tcp --dport 22 -j ACCEPT

iptables -A INPUT -p tcp --dport 443 -j ACCEPT

iptables -P INPUT DROP

После подготовки межсетевого экрана настроим серверную часть WireGuard. Установка и настройка WireGuard состоит из следующих этапов:

1. Установка WireGuard
2. Генерация секретного и публичного ключа сервера и редактирование конфигурационного файла сервера
3. Генерация секретного и публичного ключа клиента и редактирование конфигурационного файла клиента

Для начала требуется установить WireGuard с помощью команды:

apt install wireguard

Теперь, когда WireGuard установлен, следующим шагом является создание пары закрытого и открытого ключей сервера:

wg genkey | tee /etc/wireguard/private.key | wg pubkey | tee /etc/wireguard/public.key

Команда wg genkey генерирует приватный ключ, далее с помощью оператора «|» передает секретный ключ команде tee, которая сохраняет данный файл в /etc/wireguard/private.key и передает его на вход команде wg pubkey, которая на основе секретного ключа генерирует открытый ключ сервера и сохраняет его в /etc/wireguard/public.key с помощью команды tee.

Сгенерировав открытый и закрытый ключ, необходимо отредактировать конфигурационный файл с помощью текстового редактора:

nano /etc/wireguard/wg0.conf

Конфигурационный файл представлен в приложении.

Для перенаправления трафика через сеть VPN необходимо в файле /etc/sysctl.conf раскомментировать строки:

#net.ipv4.ip\_forward = 1

#net.ipv6.conf.all.forwarding=1

Для применения настроек выполняем команду:

sysctl -p /etc/sysctl.conf.

После генерации пары ключей сервера и его настройки необходимо создать конфигурационный файл клиента. Создадим пару открытого и закрытого ключей, создание ключей клиента производится аналогично созданию ключей сервера:

wg genkey | tee /etc/wireguard/private.key | wg pubkey | tee /etc/wireguard/public.key

После создания ключей клиента необходимо создать конфигурационный файл клиента с помощью команды:

nano /root/wg0-client-pc.conf

Конфигурационный файл клиента представлен в приложении.

Запустим WireGuard и включим автозапуск службы OpenVPN при загрузке сервера с помощью команд:

systemctl enable wg-quick@wg0.service

systemctl start wg-quick@wg0.service

Проверим, активна ли служба WireGuard, с помощью команды:

systemctl status wg-quick@wg0.service

По итогу должно быть выведено «active (exited)» — это значит, что служба запущена и активна. Результат проверки активности WireGuard представлен на рисунке 3.15.

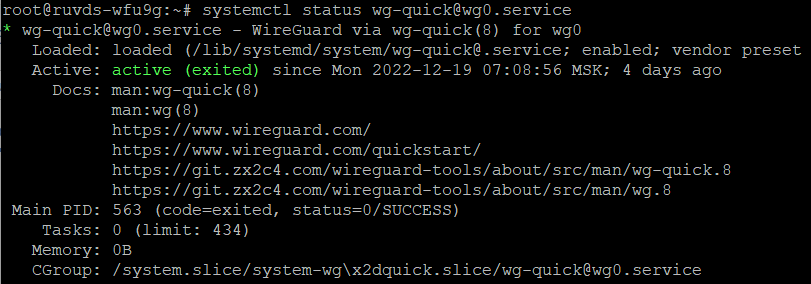


Рисунок 3.15 – Результат проверки активности WireGuard

Итак, VPN–сервер готов, теперь необходимо настроить Cloak. Порядок действий для настройки Cloak следующий:

1. Установить Cloak;
2. Сгенерировать открытый и секретный ключи;
3. Сгенерировать ключ администратора;
4. Создать конфигурационный файл сервера Cloak и настроить его;
5. (Опционально) Включить автозагрузку Cloak;
6. Запустить службу и проверить ее активность.

Для начала загрузим на сервер Cloak с помощью команды:

wget https://github.com/cbeuw/Cloak/releases/download/v2.6.0/ck-server-linux-amd64-v2.6.0

Далее требуется скопировать данный файл в каталог с именем ck-server и с помощью команды chmod добавить флаг «x» чтобы сделать файл исполняемый файл.

cp ck-server-linux-amd64-v2.6.0 /usr/local/bin/ck-server

chmod +x /usr/local/bin/ck-server

Также, для того чтобы Cloak прослушивал и мог принимать соединения по 443 порту TCP нужно разрешить Cloak привязываться к привилегированным портам (т. е. к портам TCP/IP с номером ниже 1024):

setcap CAP\_NET\_BIND\_SERVICE=+eip /usr/local/bin/ck-server

После загрузки Cloak сгенерируем пару публичный и секретный ключ с помощью команды:

ck-server -k

В результате будут выведены 2 строки base-64, где значение до запятой – это открытый ключ сервера, который предоставляется пользователям, а значение после запятой – это секретный ключ сервера, который храниться на сервере. Результат выполнения вышеуказанной команды имеет вид:

EjzZwdesObTyBWW9rI97uyztwK+4XFlDxxSrv9qyNFU=,cL2kY7rvneraJTyqbjy33rDAC/DQ3hyamRPAVolqgnI=

Теперь, когда пара ключей создана сгенерируем секретный идентификатор для клиента командой:

ck-server -u

Будет создан ключ и в консоль будет выведена строка base-64. Для того чтобы пользователь мог без ограничений по пропускной способности подключаться к серверу сгенерируем еще один ключ, для этого снова введем команду:

ck-server -u

Итак, все ключи созданы и теперь нужно настроить серверную часть Cloak. Настраивается Cloak с помощью конфигурационного файла, в данном файле необходимо указать следующие параметры:

* ProxyBook. В данном параметре указывается куда будет перенаправлен аутентифицированный прокси–трафик;
* BindAddr. В данном параметре указываются порты, которые Cloak будет прослушивать;
* Параметр RedirAddr — это адрес перенаправления, когда входящий трафик поступает не от аутентифицированного клиента Cloak
* Параметр PrivateKey — это статический закрытый ключ Диффи–Хеллмана.
* AdminUID — это идентификатор клиента
* StreamTimeout – параметр, отвечающий за время отсутствия соединения, после которого входящее клиентское соединение Cloak будет разорвано.

Также следует отметить то, что конфигурационный файл имеет расширение формата .json. Создадим директорию для хранения конфигурационного файла и отредактируем его с помощью текстового редактора nano.

Содержимое конфигурационного файла представлено в приложении.

На последнем этапе включим службы Cloak и запустим ее. Для этого нужно создать служебный файл systemd и вставить следующее содержимое:

[Unit]

Description=Cloak Server

After=network.target

[Service]

Type=simple

ExecStart=/usr/local/bin/ck-server -c /etc/cloak/ckserver.json

Restart=on-failure

[Install]

WantedBy=multi-user.target

Далее необходимо включить автозапуск службы и запустить саму службу с помощью команд:

systemctl enable cloak

systemctl start cloak

На последнем этапе проверим активен ли Cloak и прослушивает ли он порты 80и файлы 443 командами:

systemctl status cloak

По итогу должно быть выведено «active (exited)» — это значит, что служба запущена и активна. Результат проверки активности Cloak представлен на рисунке 3.16.

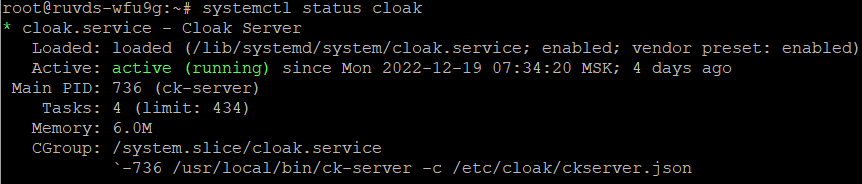


Рисунок 3.16 – Результат проверки активности Cloak

Итак, VPN–сервер готов, теперь настроим клиентскую часть. Порядок действий для настройки VPN–клиента следующий:

1. Установить Cloak;
2. Создать конфигурационный файл сервера Cloak;
3. Установить WireGuerd;
4. Вставить конфигурационный файл клиента;
5. Запустить WireGuard
6. Запустить Cloak

Скачаем Cloak. Затем в папке, где находится Cloak, необходимо создать файл конфигурации клиента для Cloak с расширением .json и заполнить данные для следующих параметров:

* ProxyMethod – название VPN;
* EncryptionMethod — это название алгоритма шифрования, который используется в Cloak;
* UID – секретный ключ клиента;
* PublicKey — это статический открытый ключ curve25519;
* NumConn — количество базовых TCP–соединений;
* BrowserSig — это браузер, который хотите использовать;
* StreamTimeout — параметр, отвечающий за время отсутствия соединения, после которого входящее клиентское соединение Cloak будет разорвано.

Полный текст конфигурационного файла клиента Cloak представлен в приложении.

После настройки Cloak нужно установить WireGuard для клиента и вставить содержимое конфигурационного файла взятого с VPN–сервера. Только в параметре Endpoint вместо IP–адреса сервера необходимо указать IP–адрес адаптера LoopBack. Полный текст конфигурационного файла клиента Cloak представлен в приложении.

На последнем этапе остается только запустить WireGuard и Cloak. Cloak запускается с консоли с помощью команды:

ck-client-windows-amd64-v2.6.0.exe -u -c ckclient.json -s 176.119.157.115

Где, после флага «-с» указывается название конфигурационный файла, а после флага «-s» IP–адрес сервера Cloak.

Для того чтобы удостовериться что VPN соединение успешно создано можно посмотреть IP–адрес, с которого идут обращения в Интернет на ресурсе https://whatismyipaddress.com. Результат проверки VPN–соединения представлен на рисунке 3.17.

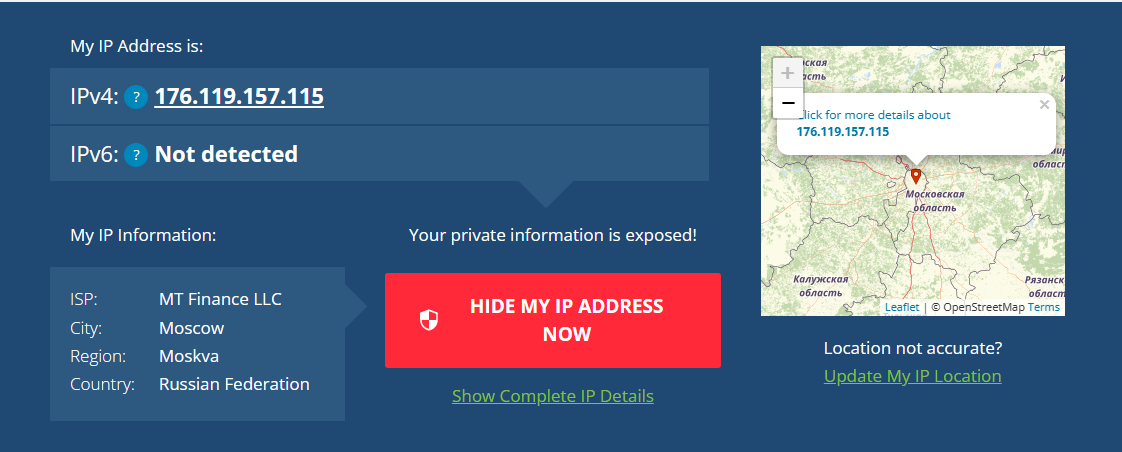


Рисунок 3.17 – Результат проверки VPN–соединения

**3.6 Анализ эффективности предложенных методов и средств**

Теперь, после создания VPN каналов необходимо убедиться, что маскировка трафика надёжно работает, а анализаторы трафика не распознают протоколов VPN. В виртуальной машине с Windows было выполнено подключение к настроенным VPN серверам через Stunnel, Cloak и SoftEther. При работе не было замечено проблем с подключением. Для проверки VPN на предмет «необнаружимости» использовался анализатор трафика WireShark. Результаты проверки приведены на рисунках 3.18 – 3.20.

Проверки на обнаружение использования технологии виртуальных частных сетей показали, что каналы VPN замаскированы.

Вывод: предложенная конфигурация ПО обеспечивает эффективное противодействие средствам глубокой проверки пакетов. Успешно проверена также правильность настройки Wireguard, OpenVPN, SoftEther в отношении его маскировки.

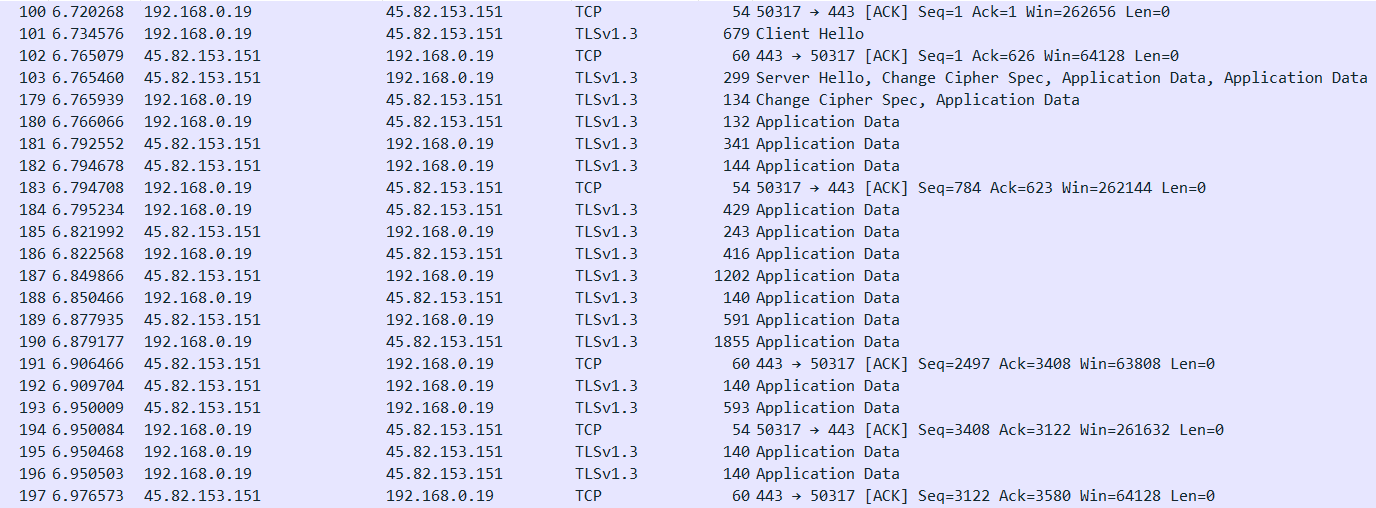


Рисунок 3.18 – Результат проверки маскировки трафика с помощью Stunnel

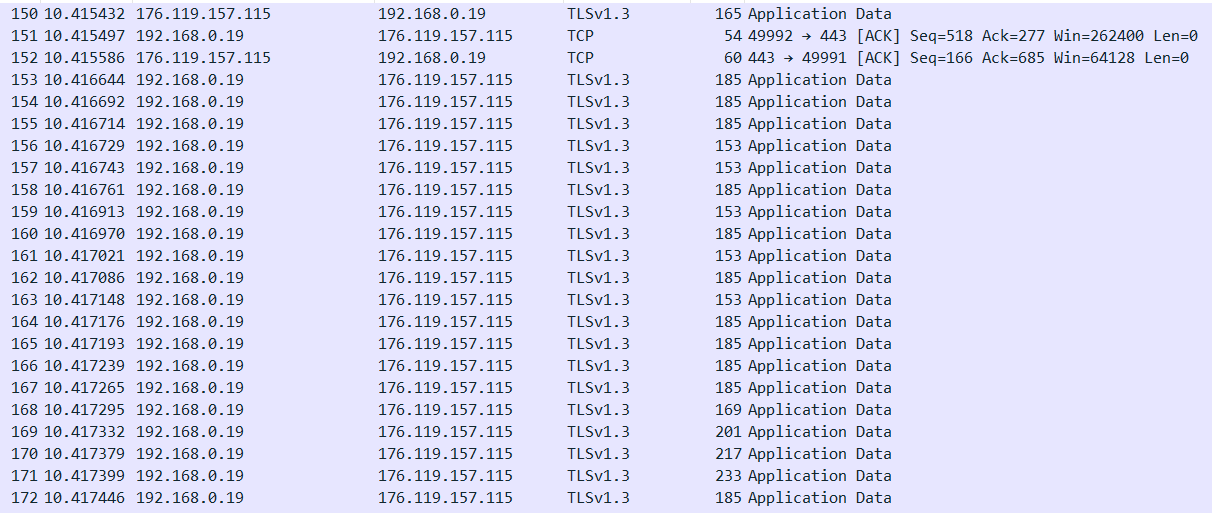


Рисунок 3.19 – Результат проверки маскировки трафика с помощью Cloak

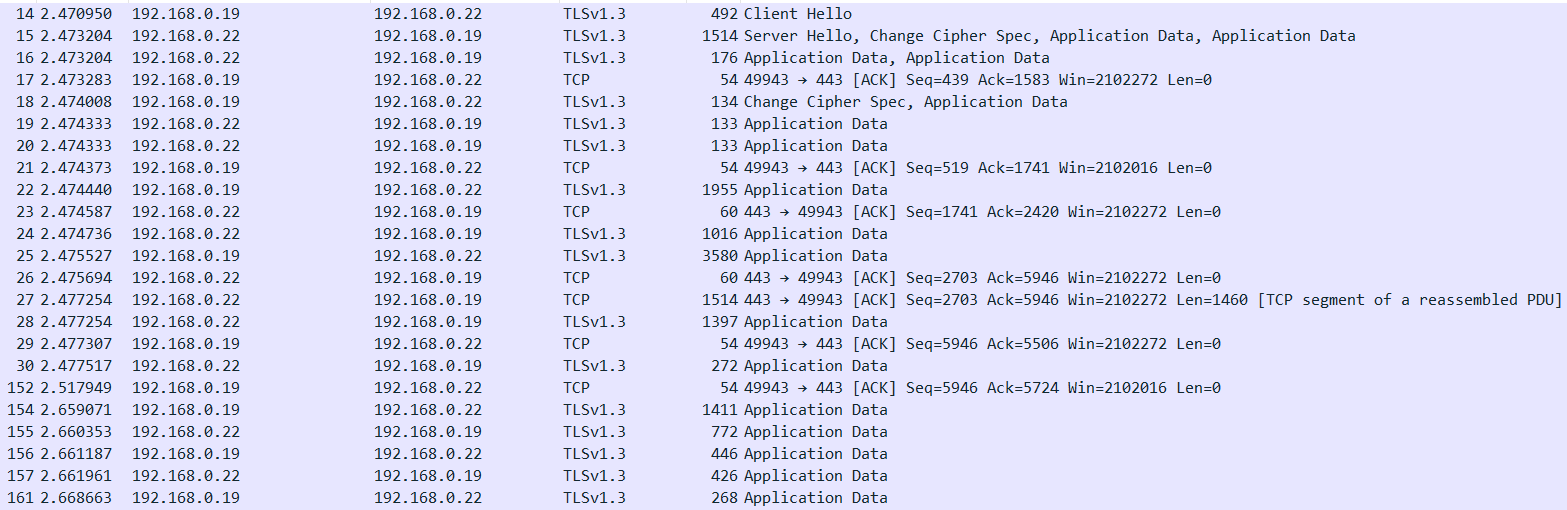


Рисунок 3.20 – Результат проверки маскировки соединения Softether

**4. Экономическое обоснование**

С целью повышения безопасности передачи данных по открытым каналам связи была реализована система маскирования трафика виртуальных частных сетей. Для подсчета экономических показателей разработанной системы был составлен план-график разработки и внедрения системы, определены затраты на её разработку и внедрение, включая затраты на оплату труда, материалы, затраты на использование машинного времени, общехозяйственные затраты.

**4.1 Спецификация проекта**

Спецификация проекта является конструкторским документом в составе проектной документации, который содержит данные о материалах, изделиях и оборудовании. Эти данные необходимы для определения общей потребности, комплектации материальными ресурсами объекта строительства. Спецификация предназначена для:

— определения полного перечня требуемых материалов, изделий, оборудования с их подробным описанием;

— подсчета количества материальных ресурсов.

На основе данных единой ведомости можно определить потребность в материалах, рассчитать стоимость и грамотно составить график их приобретения для обеспечения непрерывности процессов разработки системы.

Спецификация разработанной системы оценки защищённости беспроводных устройств представлена в таблице 4.1.

Таблица 4.1 — Спецификация системы

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Материалы | Единица измерения | Требуемое количество | Цена за единицу руб. | Сумма, руб. |
| Виртуальный выделенный сервер | шт. | 3 | 3 600 | 10800 |
| Ноутбук ASUS VivoBook 15 F513EA-BQ1883 | шт. | 1 | 49990 | 49900 |
| Итого |  | | | 60 790 |

**4.2 План–график проектирования и разработки системы**

Выбор комплекса работ по разработке проекта производится в соответствии со стандартом «ГОСТ Р ИСО/МЭК 12207-99 Информационная технология. Процессы жизненного цикла программных средств», устанавливающим стадии разработки программных продуктов, приведен в таблице 4.2.

Таблица 4.2 — Комплекс работ по разработке системы анализа радиоэфира

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| Содержание работ | Исполнители | Длитель-ность в календар-ных днях | | Загрузка | | |
| в днях | в % | |
| 1 Разработка технического задания | | | | | | |
| 1.1 Исследование и обоснование разработки | | | | | | |
| 1.1.1 Постановка задачи | Руководитель | 3 | | 3 | 100 | |
| Программист | 3 | 100 | |
| 1.1.2 Сбор исходных данных | Руководитель | 5 | | 3 | 60 | |
| Программист | 5 | 100 | |
| 1.2 Поиск аналогов и прототипов | | | | | | |
| 1.2.1 Анализ существующих методов | Руководитель | 7 | | 7 | 100 | |
| Программист | 7 | 100 | |
| 1.2.2 Обоснование необходимости разработки и внедрения | Руководитель | 5 | | 5 | 100 | |
| Программист | 0 | 0 | |
| 1.3 Анализ требований | | | | | | |
| 1.3.1 Определение и анализ требований к разрабатываемой системе | Руководитель | | 4 | 2 | | 50 |
| Программист | | 4 | | 100 |
| 1.3.2 Определение структуры входных и выходных данных | Руководитель | | 5 | 2 | | 40 |
| Программист | | 5 | | 100 |
| 1.3.3 Согласование и утверждение технического задания | Руководитель | | 4 | 4 | | 100 |
| Программист | | 4 | | 100 |
| Итого по этапу 1 | Руководитель | | 33 | 26 | | 80 |
| Программист | | 28 | | 85 |
| 2 Проектирование | | | | | | |
| 2.1 Проектирование архитектуры системы | Руководитель | | 14 | 14 | | 100 |
| Программист | | 0 | | 0 |
|  |  | |  |  | |  |
| Окончание таблицы 4.2 |  | |  |  | |  |
| 2.2 Выбор аппаратных средств цифровой радиосвязи | Руководитель | | 14 | 7 | | 50 |
| Программист | | 14 | | 100 |
| 2.3 Сборка макета системы на основе аппаратных модулей для тестирования и отладки | Руководитель | | 14 | 2 | | 14 |
| Программист | | 14 | | 100 |
| Итого по этапу 2 | Руководитель | | 42 | 23 | | 53 |
| Программист | | 28 | | 67 |
| 3 Разработка и тестирование модулей системы | | | | | | |
| 3.1 Разработка программных модулей системы | Руководитель | | 18 | 9 | | 50 |
| Программист | | 18 | | 100 |
| 3.2 Тестирование программной части | Руководитель | | 7 | 0 | | 0 |
| Программист | | 7 | | 100 |
| 3.3 Сборка и испытание системы | Руководитель | | 14 | 4 | | 29 |
| Программист | | 14 | | 100 |
| 3.4 Анализ результатов экспериментов, формулирование выводов | Руководитель | | 7 | 3 | | 36 |
| Программист | | 7 | | 100 |
| Итого по этапу 3 | Руководитель | | 46 | 16 | | 34 |
| Программист | | 46 | | 100 |
| 4 Оформление рабочей документации | | | | | | |
| 4.1 Проведение расчетов показателей безопасности жизнедеятельности | Руководитель | | 3 | 0 | | 0 |
| Программист | | 3 | | 100 |
| 4.2 Проведение экономических расчетов | Руководитель | | 7 | 0 | | 0 |
| Программист | | 7 | | 100 |
| 4.3 Оформление пояснительной записки | Руководитель | | 31 |  | | 0 |
| Программист | | 21 | | 100 |
| Итого по 4 этапу | Руководитель | | 41 | 0 | | 0 |
| Программист | | 31 | | 100 |
| Итого по проекту | Руководитель | | 162 | 65 | | 40 |
| Программист | | 133 | | 82 |

На основании вышеописанных таблиц, был составлен план–график по проектированию и реализации системы маскирования VPN–трафика, показывающий последовательность и взаимосвязь выполнения комплекса работ.

Таблица 4.3 — Календарный график выполнения работ

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Содержание работ | Исполнители | Длитель-ность в днях | График работ | |
| начало 1 сентября | окончание 31 января |
| Постановка задачи | Руководитель | 3 | 1 авг | 3 авг |
| Программист | 3 | 1 авг | 3 авг |
| Сбор исходных данных | Руководитель | 3 | 3 авг | 5 авг |
| Программист | 5 | 3 авг | 8 авг |
| Анализ существующих методов | Руководитель | 7 | 8 авг | 15 авг |
| Программист | 7 | 8 авг | 15 авг |
| Обоснование необходимости разработки и внедрения | Руководитель | 5 | 15 авг | 20 авг |
| Программист | 0 | 15 авг | 15 авг |
| Определение и анализ требований к системе | Руководитель | 2 | 20 авг | 22 авг |
| Программист | 4 | 20 авг | 24 авг |
| Определение структуры входных и выходных данных | Руководитель | 2 | 24 авг | 26 авг |
| Программист | 5 | 24 авг | 29 авг |
| Согласование и утверждение технического задания | Руководитель | 4 | 29 авг | 2 сен |
| Программист | 4 | 29 авг | 2 сен |
| Проектирование архитектуры системы | Руководитель | 14 | 2 сен | 16 сен |
| Программист | 0 | 2 сен | 2 сен |
| Выбор аппаратных средств цифровой радиосвязи | Руководитель | 7 | 16 сен | 22 сен |
| Программист | 14 | 16 сен | 30 сен |
| Сборка макета системы на основе аппаратных модулей для тестирования и отладки | Руководитель | 2 | 30 сен | 1 окт |
| Программист | 14 | 30 сен | 13 окт |
| Разработка программных модулей системы | Руководитель | 9 | 13 окт | 22 окт |
| Программист | 18 | 13 окт | 31 окт |
| Тестирование программной части | Руководитель | 0 | 31 окт | 31 окт |
| Программист | 7 | 31 окт | 7 ноя |
| Сборка и испытание системы | Руководитель | 4 | 7 ноя | 11 ноя |
| Программист | 14 | 7 ноя | 21 ноя |
| Анализ результатов экспериментов, формулирование выводов | Руководитель | 3 | 21 ноя | 23 ноя |
| Программист | 7 | 21 ноя | 28 ноя |
| Проведение расчетов показателей безопасности жизнедеятельности | Руководитель |  | 28 ноя | 28 ноя |
| Программист | 3 | 28 ноя | 31 ноя |
| Проведение экономических расчетов | Руководитель |  | 31 ноя | 31 ноя |
| Программист | 7 | 31 ноя | 7 дек |
| Оформление пояснительной записки | Руководитель |  | 7 дек | 7 дек |
| Программист | 31 | 7 дек | 10 янв |

На основе данных, приведённых в таблице 4.3 сформирован график этапов работ, представленный на рисунке 4.1.

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| **янв** | **10** |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| **декабрь** | **31** |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| **20** |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| **10** |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| **ноябрь** | **31** |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  | Рисунок 4.1 — План-график разработки проекта |
| **20** |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| **10** |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| **октябрь** | **30** |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| **20** |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| **10** |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| **сентябрь** | **31** |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| **20** |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| **10** |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| **август** | **30** |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| **20** |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| **10** |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| **Содержание работы** | | Постановка задачи | Сбор исходных данных | Анализ существующих методов | Обоснование необходимости разработки и внедрения | Определение и анализ требований к разрабатываемой системе | Определение структуры входных и выходных данных | Согласование и утверждение технического задания | Проектирование архитектуры системы | Выбор аппаратных средств цифровой радиосвязи | Сборка макета системы на основе аппаратных модулей для тестирования и отладки | Разработка программных модулей системы | Тестирование программной части | Сборка и испытание системы | Анализ результатов экспериментов, формулирование выводов | Проведение расчетов показателей безопасности жизнедеятельности | Проведение экономических расчетов | Оформление пояснительной записки |

**4.3 Расчет затрат на разработку проекта**

Предпроизводственные затраты представляют собой единовременные расходы на разработку обеспечивающих или функциональных систем и элементов на всех этапах проектирования, а также затраты на обработку материалов исследования, разработку технического задания, проверки. Сюда включаются затраты на разработку алгоритмов и программ, разработку технического и рабочего проекта системы и её опытной проверки.

Основная заработная плата разработчиков определяется по формуле:

,

где *O* — должностной оклад, руб;

— число рабочих дней в году;

— затраты времени на разработку, рабочие дни.

Число рабочих дней на разработку определяется по формуле:

,

где — календарные дни;

— коэффициент перевода календарных дней в рабочие;

Данный коэффициент равен отношению рабочих дней в году к общему числу календарных дней.

Согласно данным из таблицы 4.1, рассчитаем трудозатраты руководителя:

Рассчитаем трудозатраты программиста:

.

В компании оклад руководителя равен 100 000 руб., а оклад программиста 80 000 руб.

Рассчитаем заработную плату программиста и руководителя по формуле:

Отсюда следует, что основная заработная плата на разработку:

Рассчитаем дополнительную зарплату:

где — коэффициент начисления на дополнительную зарплату.

Премия рассчитывается согласно следующей формуле:

где — коэффициент начисления на премию.

Рассчитаем начисления на единый страховой сбор:

Ввиду того, что проектируемая система должна быть разработана и отлажена с помощью компьютеров, к суммарным затратам на разработку добавляются затраты на их использование.

Доля амортизационных отчислений на компьютерное оборудование, приходящаяся на разработку проекта, определяется по формуле:

где — балансовая стоимость компьютерного оборудования;

— продолжительность использования компьютера программистом, час;

— срок службы компьютерного оборудования. = 6 лет;

число одновременно выполняемых проектов (*z* = 1…3).

 — действительный годовой фонд времени компьютерного оборудования;

Действительный годовой фонд компьютерного оборудования рассчитывается по формуле:

где — номинальный фонд времени работы компьютерного оборудования;

— коэффициент потерь времени; *y* = 3 – 5 %.

Рассчитаем амортизационные отчисления для компьютерного оборудования:

Используемое при конструкторской подготовке системы анализа радиоэфира относится к нематериальным активам предприятия. Амортизационные отчисления на программное обеспечение, приходящиеся на конструкторскую подготовку производства, определяются по формуле:

Где — балансовая стоимость программного обеспечения, руб.;

— срок службы программного обеспечения (при отсутствии фактических данных применяется равным 10 годам).

Рассчитаем затраты электроэнергии, необходимые на проектирование и разработку системы.

где — установленная мощность компьютера, кВт;

— коэффициент загрузки установленной мощности.

— цена электроэнергии, руб/кВт.

Итого затраты на энергию будут следующими:

руб.

Итого затраты на машинное время:

Общехозяйственные расходы:

В таблице 4.4 представлены затраты на разработку и материалы в соответствии со спецификацией, приведённой в п. 5.1.

Таблица 4.4 — Затраты на разработку

|  |  |
| --- | --- |
| Статьи затрат | Затраты |
| Основная заработная плата | 631 578,94 |
| Дополнительная зарплата | 94 736,84 |
| Премия | 252 631,57 |
| Отчисления на социальные нужды | 293 684,20 |
| Затраты на материалы | 60 790 |
| Затраты на машинное время | 3 541,27 |
| Общехозяйственные расходы | 1 705 263,13 |
| ИТОГО | 3 042 225,95 |

В результате проведенных расчетов определено, что себестоимость разработки составляет 3 042 225,95 руб. С учетом нормативной рентабельности *R* = 15% планируемая прибыль *П* составит:

*П* = *С* · *R* = 3 042 225,95 · 15% = 456 333,89 руб.

A цена продукта составит:

*Ц* = *С* + *П* = 3 042 225,95 + 456 333,89 = 3 498 559,84 руб.

Цена продукта с учётом НДС составит:

*ЦНДС* = 1,2·*Ц* = 1,2 · 3 498 559,84 = 4 198 271,80 руб.

Потенциальными покупателями разработанной системы являются компании, занимающиеся производством, продажей или установкой систем безопасности: VPN–провайдеры, а также отделы информационной безопасности организаций, в которых данные системы применяются.

**5. Безопасность и экологичность проекта**

**5.1 Влияние шума на организм человека и защита от них. Расчет уровня шума на рабочем месте**

Одним из неблагоприятных факторов производственной среды в ИВЦ является высокий уровень шума, создаваемый печатными устройствами, оборудованием для кондиционирования воздуха, вентиляторами систем охлаждения в самих ЭВМ.

Шум ухудшает условия труда оказывая вредное действие на организм человека. Работающие в условиях длительного шумового воздействия испытывают раздражительность, головные боли, головокружение, снижение памяти, повышенную утомляемость, понижение аппетита, боли в ушах и т. д. Такие нарушения в работе ряда органов и систем организма человека могут вызвать негативные изменения в эмоциональном состоянии человека вплоть до стрессовых. Под воздействием шума снижается концентрация внимания, нарушаются физиологические функции, появляется усталость в связи с повышенными энергетическими затратами и нервно-психическим напряжением, ухудшается речевая коммутация. Все это снижает работоспособность человека и его производительность, качество и безопасность труда. Согласно ГОСТ 12.1.003-2014 МЕЖГОСУДАРСТВЕННЫЙ СТАНДАРТ. Система стандартов безопасности труда. ШУМ. Общие требования безопасности длительное воздействие шума выше 80 дБ(А) на слух человека приводит к его частичной или полной потере.

В таблице 5.1 указаны предельные уровни звука, являющиеся безопасными в отношении сохранения здоровья и работоспособности.

Таблица 5.1 — Предельные уровни звука, дБ, на рабочих местах

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Категория  напряженности труда | Категория тяжести труда | | | |
| I. Легкая | II. Средняя | III. Тяжелая | IV. Очень тяжелая |
| I. Мало напряженный | 80 | 80 | 75 | 75 |
| II. Умеренно напряженный | 70 | 70 | 65 | 65 |
| III. Напряженный | 60 | 60 | - | - |
| IV. Очень напряженный | 50 | 50 | - | - |

Уровень шума на рабочем месте программистов и операторов видеоматериалов не должен превышать 50дБА, а в залах обработки информации на вычислительных машинах— 65дБА.

Для решения вопросов о необходимости и целесообразности снижения шума необходимо знать уровни шума на рабочем месте оператора.

Уровень шума, возникающий от нескольких некогерентных источников, работающих одновременно, подсчитывается на основании принципа энергетического суммирования излучений отдельных источников:



где *L*i — уровень звукового давления *i*-го источника шума;

*n* — количество источников шума.

Полученные результаты расчета сравнивается с допустимым значением уровня шума для данного рабочего места. Если результаты расчета выше допустимого значения уровня шума, то необходимы специальные меры по снижению шума. К ним относятся: облицовка стен и потолка зала звукопоглощающими материалами, снижение шума в источнике, правильная планировка оборудования и рациональная организация рабочего места оператора.

Уровни звукового давления источников шума, действующих на оператора на его рабочем месте представлены в таблице 5.2.

Таблица 5.2 — Уровни звукового давления различных источников

|  |  |
| --- | --- |
| **Источник шума** | **Уровень шума, дБ** |
| Жесткий диск | 48 |
| Вентилятор | 42 |
| Монитор | 16 |
| Клавиатура | 14 |
| Принтер | 35 |
| Сканер | 43 |

Обычно рабочее место оператора оснащено следующим оборудованием: винчестер в системном блоке, вентиляторы систем охлаждения ПК, монитор, клавиатура, принтер и сканер.

Подставив значения уровня звукового давления для каждого вида оборудования в формулу, получим:

*L*∑ = 10·lg(104,8+104,2+101,6+101,4+103,5+104,3) = 50 дБ.

Полученное значение не превышает допустимый уровень шума для рабочего места оператора, равный 65 дБ. И если учесть, что вряд ли такие периферийные устройства как сканер и принтер будут использоваться одновременно, то эта цифра будет еще ниже.

Для снижения шума следует:

— ослабить шум самих источников, в частности, предусмотреть применение в их конструкции акустических экранов, кожухов и т.д.;

— снизить эффект суммарного воздействия на рабочие места отраженных звуковых волн за счет звукопоглощения энергии прямых звуковых волн поверхностями ограждающих конструкций;

— применять рациональное расположение оборудования;

— использовать архитектурно-планировочные и технологические решения, направленные на изоляцию источников шума.

**5.2 Экологичность работы**

К электронным отходам относятся все отслужившие свой срок устройства, чья работа зависит от электрического тока и/или электромагнитного поля. Телефоны, ноутбуки, телевизоры и т.д. превращаются в отходы, устаревая все быстрее и быстрее, приходя в негодность, чтобы обеспечить необходимость покупки новых устройств.

Большое количество процессов, операций и материалов, используемых при изготовлении электронных средств, являются источниками огромного количества веществ, имеющих неблагоприятное воздействие на человека и биосферу.

При изготовлении элементной базы, электронных изделий, при обработке, выращивании полупроводниковых кристаллов, при изготовлении интегральных схем, в процессе гальванического производства утилизация исходных материалов часто происходит с низким коэффициентом использования, огромное количество их идет в отходы, попадая в атмосферу, гидросферу, загрязняя почву. Таким образом, наряду с истощением природных запасов дефицитных материалов происходит загрязнение окружающей среды, что ведет к гибельным последствиям для отдельных экосистем и биосферы в целом.

Отрицательное воздействие на окружающую среду происходит на протяжении всего жизненного цикла изделия, от приобретения сырья и изготовления изделия до его утилизации по окончании срока полезного применения.

Поиски путей выхода из создавшейся ситуации приводят к выводу, что без знания экологических принципов организации живой материи, без осознания профессиональной ответственности каждого гражданина, каждого участника производственного процесса невозможно дальнейшее решение данной глобальной проблемы. Чрезвычайную роль играют законодательные ограничительные документы, регламентирующие процессы производства новой и утилизации отработанной электронной продукции.

Санитарные правила и нормы СанПиН 1.2.3685-21 «Гигиенические нормативы и требования к обеспечению безопасности и (или) безвредности для человека факторов среды обитания» устанавливают предельно-допустимые уровни (ПДУ) воздействия на людей электромагнитных излучений в диапазоне частот 30 кГц – 300 ГГц (таблица 5.3).

При работе радио и теле и иных передающих станций магнитная составляющая по своей величине не имеет существенного значения, поэтому интенсивность ЭМИ оценивается только по величине напряженности электрического поля (Е, в/м).

Таблица 5.3 — Предельно допустимые уровни ЭМИ, создаваемые передающими станциями

|  |  |
| --- | --- |
| Частота, МГц | ПДУ, в/м |
| 30-60 | 5 |
| 60-120 | 4 |
| 120-240 | 3 |
| 240-300 | 2,5 |

При одновременном облучении от нескольких источников, для которых установлены разные ПДУ, должно соблюдаться следующее условие:

где *Еi* — напряженность электрического поля, создаваемого *i*-источником,

ПДУ*i* — предельно-допустимый уровень для *i*-источника, в/м.

Для защиты населения от ЭМИ мощных передающих станций (свыше 100 кВт) КВ диапазона, они должны размещаться за пределами населенных мест, вдали от жилой застройки.

Вокруг передающих станций создают санитарно-защитные зоны, размеры которых должны обеспечивать предельно-допустимый уровень ЭМИ в населенных местах (таблица 5.4).

Таблица 5.4 — Размеры санитарных зон

|  |  |
| --- | --- |
| Суммарная мощность передатчика,  кВт | Размеры санитарной зоны, м |
| до 10 | в пределах технической территории |
| 10-75 | 200-300 |
| 75-160 | 400-500 |
| более 160 | 500-1000 |

Санитарная зона разделяется на зону строгого режима (50-100 м) и зону ограниченного пользования в зависимости от мощности передатчика. В зоне строгого режима допускается пребывание только работников передающей станции, и ограниченное время. В зоне ограниченного пользования можно располагать объекты, в которых граждане могли бы находиться менее 8 час (гаражи, хозяйственно-бытовые помещения и др.)

Определим напряженности электрического поля на разном расстоянии от передающей антенны. Напряжённость электрического поля на расстоянии от антенны представлена на рисунке 5.1.

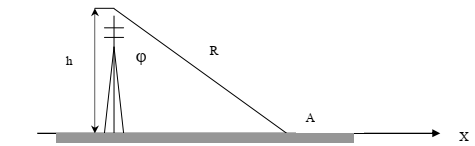


Рисунок 5.1 — Напряжённость электрического поля на расстоянии от антенны

Электрическая напряженность ЭМИ в расчетной точке А определяется по формуле:

где *Р* — мощность источника, Вт,

φ — коэффициент направленности антенны, рад.

где *R* — расстояние от антенны до расчетной точки, м,

*h* — высота антенны, м,

*x* — расстояние от основания антенны до расчетной точки, м.

Электрическая напряженность ЭМИ в жилом помещении определяется по формуле:

*Еж* = *k* · *Е*

где *k* — ослабление ЭМИ стенами здания.

*k* = 1 — для кирпичных стен;

*k* = 0,2 — для панельных стен.

Исходные данные для расчётов приведены в таблице 5.5.

Таблица 5.5 — Исходные данные для расчётов

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| *h*, м | 1 канал | | 2 канал | | 3 канал | |
| *f*1 | *P*1 | *f*2 | *P*2 | *f*3 | *P*3 |
| 100 | 51 | 2100 | 81 | 5100 | 141 | 8100 |

Где *h* — высота антенны;

*fi* — частота, МГц;

*рi* — мощность передатчика, Вт.

Определим ПДУ для каждого канала по таблице 5.5 и занесем в таблицу 5.6.

Определим электрическую напряженность в расчетных точках и результаты расчета сведем в таблицу 5.6 и рисунок 5.2.

Для *x* = 50 м:

Таблица 5.6 — Мощности электромагнитного излучения на разном расстоянии от передающей станции

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| *x* | arctg(*x*/*h*) | *E*1 | *E*2 | *E*3 | *α* |
| 0 | 0 | 0 | 0 | 0 | 0 |
| 50 | 0,464 | 1,53 | 2,38 | 3 | 1,45 |
| 100 | 0,785 | 1,57 | 2,45 | 3,08 | 1,53 |
| 150 | 0,983 | 1,38 | 2,15 | 2,71 | 1,18 |
| 200 | 1,107 | 1,18 | 1,84 | 2,31 | 0,86 |
| 250 | 1,190 | 1,02 | 2,51 | 2 | 0,88 |
| 300 | 1,249 | 0,88 | 1,38 | 1,74 | 0,49 |
| ПДУ | – | 5 | 4 | 3 | 1 |

Суммарная мощность передатчиков: 2100 + 5100 + 8100 = 15300 Вт = 15,3 кВт. Отсюда по таблице 5.4 определяем размер санитарной зоны — 200 м.

Находим по таблице 5.6 величину *Е* для *x* = 200 м и рассчитываем напряженность электрического поля в кирпичном и панельном домах.

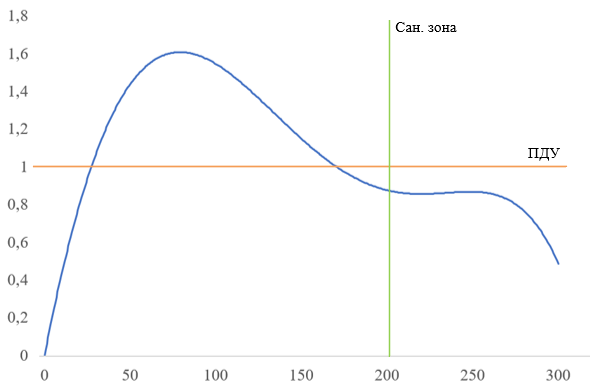


Рисунок 5.2 — Мощности электромагнитного излучения на разном расстоянии от передающей станции

Таблица 5.7 — Напряженность электрического поля в кирпичном и панельном домах

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
|  | *E*1 | *E*2 | *E*3 | *α* |
| *x* = 200 | 1,18 | 1,84 | 2,31 | 0,86 |
| Кирпичный  дом | 1,18 | 1,84 | 2,31 | 0,86 |
| Панельный  дом | 0,236 | 0,368 | 0,462 | 0,172 |
| ПДУ | 5 | 4 | 3 | 1 |

На границе санитарной зоны ЭМИ в кирпичных и панельных домах не превышает допустимые значения.

**5.3 Организация и обеспечение пожарной безопасности на предприятии**

Пожарная безопасность обеспечивается системой предотвращения пожара и системой пожарной защиты в соответствии с техническим регламентом о требованиях пожарной безопасности: федер. закон: [принят Гос. Думой Федер. собрания РФ 22 июля 2008 г. №123-ФЗ] и о противопожарном режиме [утв. и введен в действие постановления Правительства Российской Федерации от 25.04.2012 г. №390 с изм. на 30.12.2017 г.] – Введ. 2012–05–02; НПБ 105–03. Определение категорий помещений, зданий и наружных установок по взрывопожарной и пожарной опасности. Введ. 2003-08-01. Во всех служебных помещениях обязательно должен быть «План эвакуации людей при пожаре», регламентирующий действия персонала в случае возникновения очага возгорания и указывающий места расположения пожарной техники.

Пожар в рабочем помещении представляет особую опасность, так как сопряжен с большими материальными потерями. Как известно, пожар может возникнуть при взаимодействии горючих веществ, окисления и источников зажигания. На анализируемом рабочем месте присутствуют все три основные фактора, необходимые для возникновения пожара.

Как показал анализ, горючими компонентами в помещении являются: строительные материалы для акустической и эстетической отделки помещений, перегородки, двери, полы, изоляция кабелей и др.

Противопожарная защита — это комплекс организационных и технических мероприятий, направленных на обеспечение безопасности людей, на предотвращение пожара, ограничение его распространения, а также на создание условий для успешного тушения пожара.

Источниками зажигания могут быть электронные схемы, приборы, применяемые для технического обслуживания, устройства электропитания, кондиционирования воздуха, где в результате различных нарушений образуются перегретые элементы, электрические искры и дуги, способные вызвать загорания горючих материалов.

В современном электронном оборудовании очень высокая плотность размещения элементов электронных схем. В непосредственной близости друг от друга располагаются соединительные провода, кабели. При протекании по ним электрического тока выделяется значительное количество теплоты. При этом возможно оплавление изоляции. Для отвода избыточной теплоты служат системы вентиляции и кондиционирования воздуха. При постоянном действии эти системы представляют собой дополнительную пожарную опасность.

При проведении обслуживающих, ремонтных и профилактических работ используются различные смазочные вещества, легковоспламеняющиеся жидкости, прокладываются временные электропроводники, ведут пайку и чистку отдельных узлов. Возникает дополнительная пожарная опасность, требующая дополнительных мер пожарной защиты. В частности, при работе с паяльником следует использовать несгораемую подставку с несложными приспособлениями для уменьшения потребляемой мощности в нерабочем состоянии.

Для тушения пожаров на начальных стадиях широко применяются огнетушители. В настоящее время применяются главным образом углекислотные огнетушители, достоинством которых является высокая эффективность тушения пожара, сохранность электронного оборудования, диэлектрические свойства углекислого газа, что позволяет использовать эти огнетушители даже в том случае, когда не удается обесточить электроустановку сразу.

Рассмотрим аналитический прогноз горения зданий.

Расчет протяженности зон теплового воздействия *R*, м, при горении зданий и промышленных объектов производится по формуле:

где *q*соб –– плотность потока собственного излучения пламени пожара, кВт/м2, (таблица 5.8);

*q*кр –– критическая плотность потока излучения пламени пожара, падающего на облучаемую поверхность и приводящую к тем или иным последствиям, кВт/м2 (таблица 5.9);

*R*\* –– приведенный размер очага горения, м, равный:

–– для горящих зданий,



(1,75…2,0)·––для штабеля пиленого леса,



0,8·*D*рез –– для горения нефтепродуктов в резервуаре;

*l*, *h* –– длина и высота объекта горения, м;

*D*рез –– диаметр резервуара, м.

Таблица 5.8 — Теплотехнические характеристики материалов и веществ

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| Плотность потока пламени пожара, *qсоб*, кВт/м2 | | | | | | |
| Ацетон | Бензол | Бензин | Керосин | Мазут | Нефть | Древесина |
| 1200 | 2500 | 1780 —1220 | 1520 | 1300 | 874 | 260 |

Задавая ту или иную степень поражения человека, сооружения и т.п., по формуле определяют искомое расстояние от очага пожара. Определим расстояние от очага пожара, возникшего в здании цеха до границы зоны появления ожогов II степени и возгорания горючих материалов.

Таблица 5.9 — Критические значения плотностей потока, падающего излучения

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Критические значения плотностей потока, *q*кр, кВт/м2 | | | | |
| Безопасное нахождение человека | возгорание древесины через 10 минут | возгорание древесины через 5 минут | возгорание ЛВЖ через 3 минуты | возгорание ГЖ через 3 минуты |
| 1,5 | 14,0 | 17,5 | 35,0 | 41,0 |

Рассчитаем протяженность зоны теплового воздействия *R*, м возгорания ГЖ через 3 минуты при горении деревянного здания и резервуара с ацетоном.

В случае возгорания в деревянном здании высотой 12 м и длиной 140 м, граница зоны возгорания древесины через 5 минут будет равняться:

м.

Определим расстояние от очага пожара, возникшего в резервуаре с ацетоном диаметром 24 м до границы зоны возгорания древесины через 5 минут:

м.

Рекомендовано оборудовать рассматриваемое помещение установками стационарного автоматического пожаротушения. Наиболее целесообразно применять установки газового тушения пожара, действие которых основано на быстром заполнении помещения огнетушащим газовым веществом с резким сжижением содержания в воздухе кислорода.

Пожарная безопасность обеспечивается системой предотвращения пожара и системой пожарной защиты. В служебных помещениях вывешены «Планы эвакуации людей при пожаре», регламентирующие действия персонала в случае возникновения очага возгорания и указывающий места расположения пожарной техники.

В необходимых местах размещены ручные огнетушители (углекислотные ОУ-8 в количестве 2 шт).

Средствами обнаружения и оповещения о пожаре являются автоматические датчики-сигнализаторы о пожаре типа ДТП, реагирующие на повышение температуры. Средством оповещения сотрудников о пожаре служит внутрифирменное радио.

**5.4 Выводы**

В соответствии с принятыми нормами в отделе информационных технологий обеспечивается минимальный уровень шума, созданы удобные и правильные с точки зрения эргономики рабочие места, соблюдены требования технической эстетики.

Для сотрудников отдела в процессе работы одним из важнейших факторов, влияющих на производительность труда при длительной работе, является уровень шума. Это достигается использованием акустических экранов, кожухов, рациональным расположением оборудования, использованием архитектурно-планировочных и технологических решений, направленных на изоляцию источников шума.

Специальные мероприятия обеспечивают электробезопасность и пожаробезопасность сотрудников.

В целом условия труда инженера соответствуют установленным нормам, сотрудникам обеспечены комфорт и благоприятные условия труда.

**Заключение**

В результате выполнения выпускной квалификационной работы были реализованы системы маскировки VPN–трафика на основе SoftEther VPN, на базе OpenVPN с маскировкой трафика с помощью прокси–сервера Stunnel и на базе протокола WireGuard с маскировкой трафика с помощью Cloak. Использование средств маскировки для VPN–трафика предоставляет широкие возможности по обеспечению защиты входящих и исходящих пакетов данных, однако требует тщательной настройки в соответствии с актуальными угрозами и требованиями к информационной безопасности.

Разработанная система может представлять интерес для специалистов в области сетевой безопасности и системных администраторов. Представленные средства защиты, в частности настройки встроенного межсетевого экрана и подходы к ограничению доступа к целевым ресурсам, могут применяться на серверах различного назначения.

**Перечень использованных информационных ресурсов**

1. Олифер В. Компьютерные сети. Принципы, технологии, протоколы: Учебник для ВУЗов / В. Олифер. - СПб.: Питер, 2012. - 944 c.
2. К вопросу о правовом регулировании Интернета. К.В. Прокофьев [Электронный ресурс] // Проект Cyberleninka. – URL: https://cyberleninka.ru/article/n/k-voprosu-o-pravovom-regulirovanii-interneta/viewer (дата обращения 05.10.2022).
3. Киберпреступность правовое регулирование VPN – сервисов. Рева А.А. [Электронный ресурс] // Проект elibrary. – URL: https://www.elibrary.ru/item.asp?id=48462483 (дата обращения 12.10.2022).
4. Разбираемся в VPN протоколах / Хабр – Habr [Электронный ресурс] // Проект Habr. – URL: https://habr.com/ru/company/dsec/blog/499718/ (дата обращения 10.11.2022).
5. What Is PPTP? (Everything You Need to Know) | CactusVPN [Электронный ресурс] // Проект CactusVPN. – URL https://www.cactusvpn.com/beginners-guide-to-vpn/what-is-pptp/ (дата обращения 10.11.2022).
6. What Is OpenVPN & How Does OpenVPN Work? | CactusVPN [Электронный ресурс] // Проект CactusVPN. – URL: https://www.cactusvpn.com/beginners-guide-to-vpn/what-is-openvpn/ (дата обращения 17.11.2022).
7. What Is WireGuard? (An In-Depth Look at the Newest VPN Protocol) | CactusVPN [Электронный ресурс] // Проект CactusVPN. – URL: https://www.cactusvpn.com/beginners-guide-to-vpn/what-is-wireguard/ (дата обращения 19.11.2022).
8. What Is SoftEther? (Complete Guide) | CactusVPN [Электронный ресурс] // Проект CactusVPN. – URL: https://www.cactusvpn.com/beginners-guide-to-vpn/what-is-softether/ (дата обращения 27.11.2022).
9. OpenVPN + Stunnel | Oil and Fish [Электронный ресурс] // Проект Oil and Fish. – URL: https://www.oilandfish.com/posts/openvpn-stunnel.html (дата обращения 28.11.2022).
10. Penetrates Firewall by SSL-VPN [Электронный ресурс] // Проект SoftEther. – URL: https://www.softether.org/4-docs/2-howto/7.Replacements\_of\_Legacy\_VPNs/1.Penetrates\_Firewall\_by\_SSL-VPN (дата обращения 05.12.2022).
11. Security and Reliability [Электронный ресурс] // Проект SoftEther. – URL https://www.softether.org/1-features/3.\_Security\_and\_Reliability (дата обращения 13.12.2022).
12. WireGuard + Cloak | Oil and Fish [Электронный ресурс] // Проект Oil and Fish. – URL: https://www.oilandfish.com/posts/wireguard-cloak.html (дата обращения 15.12.2022).
13. Федеральный закон от 22.07.2008 № 123-ФЗ «Технический регламент о требованиях пожарной безопасности».
14. СанПиН 1.2.3685-21 «Гигиенические нормативы и требования к обеспечению безопасности и (или) безвредности для человека факторов среды обитания».
15. ГОСТ 12.1.003-2014 МЕЖГОСУДАРСТВЕННЫЙ СТАНДАРТ.
16. Трудовой кодекс Российской Федерации от 30.12.2001 № 197-ФЗ (ред. от 19.12.2022) [Электронный ресурс]: справочная правовая система КонсультантПлюс. URL: https://www.consultant.ru/document/cons\_doc\_LAW\_346-83/ (дата обращения: 24.12.2022).
17. Налоговый кодекс Российской Федерации (НК РФ) от 31 июля 1998 года № 146-ФЗ [Электронный ресурс]: справочная правовая система КонсультантПлюс. URL: https://www.consultant.ru/document/cons\_doc\_LAW\_196-71/ (дата обращения: 24.12.2022).

Приложение A

Листинг конфигурационных файлов

Содержимое конфигурационный файла сервера OpenVPN

port 1194

proto tcp6

dev tun

user nobody

group nogroup

persist-key

persist-tun

keepalive 10 120

topology subnet

server 10.8.0.0 255.255.255.0

ifconfig-pool-persist ipp.txt

push "dhcp-option DNS 8.8.8.8"

push "dhcp-option DNS 8.8.4.4"

push "redirect-gateway def1 bypass-dhcp"

server-ipv6 fd42:42:42:42::/112

tun-ipv6

push tun-ipv6

push "route-ipv6 2000::/3"

push "redirect-gateway ipv6"

dh none

Содержимое конфигурационный файла клиента OpenVPN

client

proto tcp-client

remote 45.82.153.151 1194

route 192.168.0.1 255.255.255.255 net\_gateway

dev tun

resolv-retry infinite

nobind

persist-key

persist-tun

remote-cert-tls server

verify-x509-name server\_y3RkuSh7M4Q9zVsG name

auth SHA256

auth-nocache

cipher AES-128-GCM

tls-client

tls-version-min 1.2

tls-cipher TLS-ECDHE-ECDSA-WITH-AES-128-GCM-SHA256

ignore-unknown-option block-outside-dns

setenv opt block-outside-dns # Prevent Windows 10 DNS leak

verb 3

Содержимое конфигурационный файла сервера WireGuard

[Interface]

Address = 10.66.66.1/24,fd42:42:42::1/64

ListenPort = 51820

PrivateKey = EDXNIMSyBWZyNI+u8dXx8De1Mk2/46VzHly8nJOcmGo=

PostUp = iptables -A FORWARD -i eth0 -o wg0 -j ACCEPT; iptables -A FORWARD -i w$

PostDown = iptables -D FORWARD -i eth0 -o wg0 -j ACCEPT; iptables -D FORWARD -i$

Содержимое конфигурационный файла сервера Cloak

{

"ProxyBook": {

"wireguard": [

"udp",

"127.0.0.1:51820"

]

},

"BindAddr": [

":80",

":443"

],

"BypassUID": [

"VgY+2ysltwfsQTkeKhiRgQ=="

],

"RedirAddr": "www.bing.com",

"PrivateKey": "KELYHO/xKQqwdnquPvqOdm+ZS0zehsF/13PhqLTIpVw=",

"AdminUID": "psEqf+oEYa1XBULzWi/HWA==",

"DatabasePath": "/etc/cloak/userinfo.db",

"StreamTimeout": 300

}

Содержимое конфигурационный файла Cloak

{

"Transport": "direct",

"ProxyMethod": "wireguard",

"EncryptionMethod": "plain",

"UID": "JXD42BdCNynBeKq+G0KbFA==",

"PublicKey": "EjzZwdesObTyBWW9rI97uyztwK+4XFlDxxSrv9qyNFU=",

"ServerName": "www.bing.com",

"NumConn": 4,

"BrowserSig": "firefox",

"StreamTimeout": 300

}

Содержимое конфигурационный файла WireGuard

[Interface]

PrivateKey = 8PO4uAUL9OSi+pPr/oz4i5bUxi2XsN8KOWPtCpoKK18=

Address = 10.66.66.2/32, fd42:42:42::2/128

DNS = 94.140.14.14, 94.140.15.15

[Peer]

PublicKey = y+IgvEUbY4i+65jYHRbqiBsV7hcOMkB/sHzSV6D7kB4=

PresharedKey = H68R459kqjm69uyepRoSudr8hyMdjXpqc0OqZa9+XP4=

AllowedIPs = 0.0.0.0/1, 128.0.0.0/1, ::/1, 8000::/1

Endpoint = 127.0.0.1:1984