Министерство образования и науки Российской Федерации
федеральное государственное автономное образовательное учреждение
высшего образования
**«НАЦИОНАЛЬНЫЙ ИССЛЕДОВАТЕЛЬСКИЙ
ТОМСКИЙ ПОЛИТЕХНИЧЕСКИЙ УНИВЕРСИТЕТ»**

Школа информационных технологий и робототехники
Направление подготовки 09.04.01 «Информатика и вычислительная техника»
Отделение школы (НОЦ) информационных технологий

МАГИСТЕРСКАЯ ДИССЕРТАЦИЯ

Тема работы
Разработка методологии противодействия отслеживания и идентификации пользователей интернета

УДК 004.42.056-043.61:004.738.5.056.523

Студент

Группа	ФИО	Подпись	Дата
8ВМ6Б	Айд Михаил Александрович		

Руководитель

Должность	ФИО	Учёная степень, звание	Подпись	Дата
Доцент ОИТ	Шерстнёв Владислав Станиславович	к.т.н		

КОНСУЛЬТАНТЫ:

По разделу «Финансовый менеджмент, ресурсоэффективность и ресурсосбережение»

Должность	ФИО	Учёная степень, звание	Подпись	Дата
Ст. преподаватель	Шаповалова Наталья Владимировна			

По разделу «Социальная ответственность»

Должность	ФИО	Учёная степень, звание	Подпись	Дата
Ассистент	Авдеева Ирина Ивановна			

ДОПУСТИТЬ К ЗАЩИТЕ:

Руководитель ООП	ФИО	Учёная степень, звание	Подпись	Дата
Профессор ОИТ	Спицын Владимир Григорьевич	д.т.н		

Томск – 2018 г.

ПЛАНИРУЕМЫЕ РЕЗУЛЬТАТЫ ОБУЧЕНИЯ ПО ООП

Код результатов	Результат обучения (выпускник должен быть готов)	Требования ФГОС ВО (ФГОС 3+), критерии АИОР, заинтересованных работодателей и студентов
Общепрофессиональные компетенции		
Р1	Воспринимать и самостоятельно приобретать, развивать и применять математические, естественнонаучные, социально-экономические и профессиональные знания для решения нестандартных задач, в том числе в новой или незнакомой среде и в междисциплинарном контексте.	Требования ФГОС 3+ (ОПК-1; ПК 3-6; ОК-4), критерий 5 АИОР (п. 1.1), соответствующий международным стандартам EUR-ACE и FEANI. Запросы студентов, отечественных и зарубежных работодателей.
Р2	Владеть и применять методы и средства получения, хранения, переработки и трансляции информации посредством современных компьютерных технологий, в том числе в глобальных компьютерных сетях.	Требования ФГОС 3+ (ОПК-5; ПК-7; ОК-7), критерий 5 АИОР (п. 1.1, 1.2), соответствующий международным стандартам EUR-ACE и FEANI. Запросы студентов, отечественных и зарубежных работодателей.
Р3	Демонстрировать культуру мышления, способность выстраивать логику рассуждений и высказываний, основанных на интерпретации данных, интегрированных из разных областей науки и техники, выносить суждения на основании неполных данных, анализировать профессиональную информацию, выделять в ней главное, структурировать, оформлять и представлять в виде аналитических обзоров с обоснованными выводами и рекомендациями.	Требования ФГОС 3+ (ОПК-6; ПК-1,2; ОК-1,2), критерий 5 АИОР (п. 1.2), соответствующий международным стандартам EUR-ACE и FEANI. Запросы студентов, отечественных и зарубежных работодателей.
Р4	Анализировать и оценивать уровни своих компетенций в сочетании со способностью и готовностью к саморегулированию дальнейшего образования и профессиональной мобильности. Владеть, по крайней мере, одним из иностранных языков на уровне социального и профессионального общения, применять специальную лексику и профессиональную терминологию языка.	Требования ФГОС 3+ (ОПК-3,4; ПК-11,12; ОК-3), критерий 5 АИОР (п. 1.6, п. 2.2), соответствующий международным стандартам EUR-ACE и FEANI. Запросы студентов, отечественных и зарубежных работодателей.
Профессиональные компетенции		
Р5	Выполнять инновационные инженерные проекты по разработке аппаратных и программных средств автоматизированных систем различного назначения с использованием современных методов проектирования, систем автоматизированного проектирования, передового опыта разработки конкурентноспособных изделий.	Требования ФГОС 3+ (ПК-8–12; ОПК-2, ПК-7,6), критерий 5 АИОР (п. 1.3), соответствующий международным стандартам EUR-ACE и FEANI.Запросы студентов, отечественных и зарубежных работодателей.
Р6	Планировать и проводить теоретические и экспериментальные исследования в области проектирования аппаратных и программных средств автоматизированных систем с использованием новейших достижений науки и техники, передового отечественного и зарубежного опыта. Критически оценивать полученные данные и делать выводы.	Требования ФГОС 3+ (ПК-1–7; ОПК-6; ОК-4,9), критерий 5 АИОР (п.1.4), соответствующий международным стандартам EUR-ACE и FEANI. Запросы студентов, отечественных и зарубежных работодателей.
Р8	Использовать на практике умения и навыки в организации исследовательских, проектных работ и профессиональной эксплуатации современного оборудования и приборов, в управлении коллективом.	Требования ФГОС 3+ (ОК-5,8; ОПК-1,6; ПК-6,7,11,12), критерий 5 АИОР (п. 2.1, п. 2.3, п. 1.5), соответствующий международным стандартам EUR-ACE и FEANI. Запросы студентов, отечественных и зарубежных работодателей.

Код результатов	Результат обучения (выпускник должен быть готов)	Требования ФГОС ВО (ФГОС 3+), критерии АИОР, заинтересованных работодателей и студентов
Р9	Осуществлять коммуникации в профессиональной среде и в обществе в целом, активно владеть иностранным языком, разрабатывать документацию, презентовать и защищать результаты инновационной инженерной деятельности, в том числе на иностранном языке.	Требования ФГОС 3+ (ОК-2,9; ОПК-4; ПК-1), критерий 5 АИОР (п. 2.2), соответствующий международным стандартам EUR-ACE и FEANI. Запросы студентов, отечественных и зарубежных работодателей.
Р10	Совершенствовать и развивать свой интеллектуальный и общекультурный уровень. Проявлять инициативу, в том числе в ситуациях риска, брать на себя всю полноту ответственности.	Требования ФГОС 3+ (ОК-1,6; ОПК-2; ПК-1,2), критерий 5 АИОР (п. 2.4, п. 2.5), соответствующий международным стандартам EUR-ACE и FEANI. Запросы студентов, отечественных и зарубежных работодателей.
Р11	Демонстрировать способность к самостоятельному обучению новым методам исследования, к изменению научного и научно-производственного профиля своей профессиональной деятельности, способность самостоятельно приобретать с помощью информационных технологий и использовать в практической деятельности новые знания и умения, в том числе в новых областях знаний, непосредственно не связанных со сферой деятельности, способность к педагогической деятельности.	Требования ФГОС 3+ (ОК-3,4,7; ОПК-3; ПК-7), критерий 5 АИОР (п. 2.6), соответствующий международным стандартам EUR-ACE и FEANI. Запросы студентов, отечественных и зарубежных работодателей.

Министерство образования и науки Российской Федерации
федеральное государственное автономное образовательное учреждение
высшего образования
**«НАЦИОНАЛЬНЫЙ ИССЛЕДОВАТЕЛЬСКИЙ
ТОМСКИЙ ПОЛИТЕХНИЧЕСКИЙ УНИВЕРСИТЕТ»**

Школа информационных технологий и робототехники
Направление подготовки 09.04.01 «Информатика и вычислительная техника»
Отделение школы (НОЦ) информационных технологий

УТВЕРЖДАЮ:
Руководитель ООП
_____ _____ Спицын В.Г.
(Подпись) (Дата) (Ф.И.О.)

ЗАДАНИЕ
на выполнение выпускной квалификационной работы

В форме:

Магистерской диссертации

Студенту:

Группа	**ФИО**
8ВМ6Б	Айду Михаилу Александровичу

Тема работы:

Разработка методологии противодействия отслеживания и идентификации пользователей интернета		
Утверждена приказом директора (дата, номер)	07.03.2018	№1548/с

Срок сдачи студентом выполненной работы:	14.06.2018

ТЕХНИЧЕСКОЕ ЗАДАНИЕ:

Исходные данные к работе *(наименование объекта исследования или проектирования; производительность или нагрузка; режим работы (непрерывный, периодический, циклический и т. д.); вид сырья или материал изделия; требования к продукту, изделию или процессу; особые требования к особенностям функционирования (эксплуатации) объекта или изделия в плане безопасности эксплуатации, влияния на окружающую среду, энергозатратам; экономический анализ и т. д.).*	Программный комплекс, предназначенный для анонимного использования интернет-ресурсов. Задачи: скрытие и подмена идентифицирующих данных, защита от прослушивания трафика, маскировка присутствия средств анонимизации.

Перечень подлежащих исследованию, проектированию и разработке вопросов *(аналитический обзор по литературным источникам с целью выяснения достижений мировой науки техники в рассматриваемой области; постановка задачи исследования, проектирования, конструирования; содержание процедуры исследования, проектирования, конструирования; обсуждение результатов выполненной работы; наименование дополнительных разделов, подлежащих разработке; заключение по работе).*	Методы и средства обеспечения анонимности и защиты от отслеживания при работе в интернете. Программное обеспечение и поведенческая стратегия. Способы отслеживания, каналы утечки данных. Шифрование и обфускация трафика. Правдоподобность анонимной личности. Выбор, установка и настройка программного обеспечения, формулировка правил использования. Тестирование на обнаружимость, выводы по результатам.
Перечень графического материала *(с точным указанием обязательных чертежей)*	Схема реализации, результаты испытаний

Консультанты по разделам выпускной квалификационной работы
(с указанием разделов)

Раздел	Консультант
Финансовый менеджмент, ресурсоэффективность и ресурсосбережение	Шаповалова Наталья Владимировна, старший преподаватель школы инженерного предпринимательства
Социальная ответственность	Авдеева Ирина Ивановна, ассистент отделения контроля и диагностики
Раздел на иностранном языке	Куркан Наталия Владимировна; Дорофеев Вадим Анатольевич

Названия разделов, которые должны быть написаны на русском и иностранном языках:

2. Методы обеспечения анонимности

Дата выдачи задания на выполнение выпускной квалификационной работы по линейному графику	12.03.2018

Задание выдал руководитель:

Должность	ФИО	Учёная степень, звание	Подпись	Дата
Доцент ОИТ	Шерстнёв Владислав Станиславович	к.т.н		

Задание принял к исполнению студент:

Группа	ФИО	Подпись	Дата
8ВМ6Б	Айд Михаил Александрович		

РЕФЕРАТ

Выпускная квалификационная работа содержит 142 с., 16 рис., 21 табл., 51 источник, 4 прил.

Ключевые слова: информационная безопасность, анонимность, защита от отслеживания, шифрование, Интернет.

Объектом исследования является современные методы и средства обеспечения анонимности и противодействия отслеживанию пользователей при работе с интернет-ресурсами.

Цель работы – исследовать возможность совмещения таких качеств, как безопасность, удобство и незаметность, в ПО для обеспечения анонимности.

В процессе исследования проводились: сбор и анализ актуальной теоретической информации, изучение аналогов, проектирование практического решения, эксперименты по проверке его эффективности.

В результате исследования был подобран, настроен и протестирован комплекс программного обеспечения, решающий поставленные задачи наилучшим образом.

Основные конструктивные, технологические и технико-эксплуатационные характеристики: реализуется скрытие и подмена данных о пользователе, шифрование и обфускация трафика, маскировка наличия средств анонимизации, изоляция веб-браузера от основной системы, защита от случайных утечек реальных данных.

Степень внедрения: тестовый комплекс ПО был установлен и испытан, запущенный VPN-сервер успешно используется по назначению.

Область применения: различная, схожая с применением Tor Browser и других популярных инструментов обеспечения анонимности.

Экономическая эффективность/значимость работы: используется только бесплатное и преимущественно открытое ПО, единственными затратами на проект являлась аренда недорогого виртуального сервера для тестов VPN.

В будущем планируется дальнейшее улучшение полученной сборки с целью автоматизации некоторых функций и повышения удобства работы.

Определения, обозначения, сокращения, нормативные ссылки

Анонимизация трафика — процесс удаления или подмены данных с целью предотвращения идентификации источника трафика и места назначения.
Гостевая ОС — операционная система внутри виртуальной машины.

VPN — Virtual Private Network (виртуальная частная сеть)
TLS — Transport Layer Security (Протокол защиты транспортного уровня)
VPS — Virtual Private Server (виртуальный частный сервер)
SSH — Secure Shell (безопасная оболочка), протокол удалённого доступа
DPI — Deep Packet Inspection (система глубокого анализа пакетов)
ВМ — виртуальная машина
ПО — программное обеспечение

Использованы ссылки на следующие нормативные документы:

1. ГОСТ 12.0.003-2015;
2. СанПиН 2.2.4.548-96;
3. СанПиН 2.2.2/2.4.1340-03;
4. СанПиН 2.2.4.3359-16;
5. СН 2.2.4/2.1.8.562-96;
6. СП 52.13330.2016;
7. ГОСТ Р 12.1.019-2009 ССБТ;
8. СНиП 21-01-97;
9. СанПиН 2.2.1/2.1.1.1200-03;
10. СанПиН 2.1.7.1322-03.

Оглавление

Введение

Данная научно-исследовательская работа рассматривает проблему разработки и использования эффективных программных средств, обеспечивающих анонимность и противодействие отслеживанию при работе в Интернете. В настоящее время существует большое количество подобных инструментов, а VPN-сервисы и различные «анонимайзеры» приобретают всё большую популярность. Однако практически все они имеют те или иные недостатки.

Во-первых, максимально надёжное обеспечение анонимности является сложной комплексной задачей, включающей множество различных факторов, и многие сервисы решают эту задачу лишь частично. Известен ряд случаев идентификации пользователей даже в сети TOR, которая часто позиционируется как наиболее безопасная. Кроме того, многие VPN-провайдеры могут намеренно отслеживать и сохранять историю действий пользователя, а затем предоставлять её по запросу государственных служб.

Во-вторых, при использовании подобных инструментов часто снижается удобство работы из-за невысокой скорости соединения, а также ограничения функциональности браузера. Для надёжной защиты часто предлагается отключать некоторые потенциально небезопасные функции, которые могут привести к утечке данных и раскрытию личности анонимного пользователя, но являются необходимыми для нормальной работы многих интернет-сайтов. Прежде всего сюда относится отключение JavaScript и запрет приёма Cookies.

В-третьих, сам факт использования анонимизации часто выявляется по различным признакам и может привлекать внимание к пользователю. Также это может затруднять работу: например, некоторые сайты ограничивают доступ с IP-адресов, принадлежащих узлам TOR. Существует множество факторов, позволяющих внешнему наблюдателю определить, что пользователь пытается скрыть свою личность. Таким образом, незаметность, скрытность является ещё одним важным параметром надёжного средства анонимизации, но большинство существующих решений не обеспечивают это.

Наконец, не все инструменты и схемы обеспечения сетевой анонимности можно назвать простыми в настройке и использовании, если учитывать, что они должны быть понятны любому интернет-пользователю, а не только «продвинутому». Надёжность работы особо сложных схем будет сильно зависеть от уровня знаний и навыков пользователя, требовать отчётливого понимания принципов и деталей настройки. Однако надёжная сетевая анонимность в современных реалиях может потребоваться самым различным категориям пользователей. Естественно, требуемый уровень безопасности зависит от конкретного сценария использования.

Дополнительной проблемой является нехватка актуальных научных публикаций, особенно русскоязычных, в данной области. Значительная часть полезной информации находится на различных Интернет-ресурсах, форумах, в том числе внутри анонимных сетей, но не в тех источниках, которые считались бы авторитетными. Кроме того, в последнее время подобная информация начинает подвергаться цензуре, однако это лишь подтверждает текущую актуальность проблемы анонимности в Интернете.

Основной целью данного исследования является оценка и изучение возможности создания средства анонимизации, которое должно максимально эффективно сочетать все качества, рассмотренные выше: надёжность, удобство, незаметность использования, простота настройки. Данные качества чаще всего считаются несовместимыми (усиление безопасности снижает комфортность и т.д.), поэтому необходимо определить предельные возможности их совмещения и доступные пути реализации этого. В итоге — спроектировать программный продукт с перспективой его практической реализации и внедрения.

В ходе исследования решаются следующие задачи:

- Сбор и анализ информации о всевозможных средствах и методах обеспечения анонимности в Интернете, актуальных в настоящее время;
- Конкретизация и рассмотрение факторов, по которым возможно отслеживание пользователя при работе в сети;

- Анализ различных путей утечки данных, приводящей к нарушению анонимности;
- Выяснение возможности обеспечения тех или иных аспектов защиты без ущерба удобству работы с сайтами;
- Изучение всех признаков, по которым сам факт использования средства анонимизации может быть замечен Интернет-ресурсом или иным наблюдателем;
- Выявление нетехнических факторов потери анонимности, то есть ошибок поведения анонимного пользователя в Интернете;
- Составление рекомендаций по технической анонимизации и правилам поведения для различных моделей угроз.

Данная работа вносит вклад в научное исследование проблемы анонимной работы в Интернете, противодействия цензуре Интернета и современным системам отслеживания.

1 Проблематика сохранения анонимности и приватности

1.1. Обзор существующей литературы

На первый взгляд, данная тема в основном обсуждается на неофициальных интернет-ресурсах, однако на самом деле существует множество научных публикаций, посвящённых потенциальным уязвимостям анонимных сетей, методикам идентификации устройств, разработке новых средств для защиты от самых современных техник отслеживания и т.д.

Публикация «PriVaricator: Deceiving Fingerprinters with Little White Lies», появившаяся в 2014 году на сайте Microsoft Research, описывала инструмент для случайной подмены некоторых данных о браузере, доступных через JavaScript, для борьбы с его идентификацией. В 2017 году группа исследователей из США опубликовала статью «Cross-Browser Fingerprinting via OS and Hardware Level Features», которая описывает технику распознавания компьютеров с высокой точностью независимо от используемого браузера, причём авторы советуют использовать Tor Browser для противодействия таким методам идентификации. Статья даёт хорошее представление о современных способах так называемого «фингерпринтинга». Значительная часть параметров связана с обработкой трёхмерной графики WebGL.

Работа Авдошина С.М. и Лазаренко А.В. «Система деанонимизации пользователей теневого интернета» (2016) описывает некоторые возможные атаки в сети Tor и демонстрирует одну из таковых. Статья «Исследование устойчивости анонимной сети на основе технологий веб-прокси» (Маркин Д.О. и др., 2016) рассматривает поведение сложных цепочек прокси-серверов. Сразу три статьи по теме использования сети Tor были опубликованы в 2015 году группой авторов из Пермского политехнического университета. Приведены потенциальные слабости Tor, упомянуты некоторые альтернативы и испытана возможность работы Skype через Tor.

Работа «Online Tracking: A 1-million-site Measurement and Analysis» – исследование методов отслеживания, встречающихся в настоящее время, опубликованное Принстонским университетом в 2016 году.

Интернет-ресурс The Free Haven содержит крупную подборку статей [1] на различные темы, имеющие отношение к анонимности и шифрованию, начиная с 1977 года по настоящее время. Например, статья 2018 года «Inside Job: Applying Traffic Analysis to Measure Tor from Within», опубликованная Военно-морской исследовательской лабораторией США, посвящена анализу трафика Tor через промежуточные узлы и отслеживанию использования onion-сервисов. Другой интернет-проект [2], принадлежащий американской правозащитной организации «Фонд электронных рубежей», является начальным пособием по сохранению конфиденциальности и защите от слежения в Интернете. Похожий ресурс [3] запустила и российская организация «Роскомсвобода», а связанный с ней «Центр защиты цифровых прав» публиковал [4] статьи о праве граждан на анонимность.

М. Райтман в книге «Искусство легального, анонимного и безопасного доступа к ресурсам Интернета» (2017) освещает множество тем: шифрование файлов и их надёжное удаление, использование менеджеров паролей, защита от вирусов, безопасное общение с помощью сквозного шифрования, анонимные сети и прочее. Подробно описана работа с системой Tails и инструментами PGP. Книга Д. Колисниченко «Анонимность и безопасность в Интернете» (2012) на более простом уровне описывает использование Tor и I2P, шифрование файлов и электронной почты, а также общие принципы поведения.

1.2. Потребность в анонимности и защите от отслеживания

Проблема обеспечения анонимности в Интернете существовала с самого момента возникновения Всемирной паутины, но особенно актуальной по всему миру она стала в 2013 году, когда Э.Сноуден раскрыл правду о программах глобальной слежки — американской системе PRISM и других комплексах негласного массового сбора данных. Уже тогда это было названо беспрецедентным вторжением в частную жизнь граждан. Что же касается России, то в настоящее время проблемы слежки и интернет-цензуры становятся всё более актуальными даже без учёта деятельности каких-либо зарубежных

организаций. По оценке фонда Freedom House, Россия уже не входит в категорию стран со свободным интернетом [5].

Изначально же Интернет был именно «территорией свободы». Но сейчас стремление государства и некоторых коммерческих структур «знать всё» о каждом интернет-пользователе привело к необходимости настоящей борьбы за неприкосновенность личных данных. Сам факт наличия слежки попросту раздражает, даже независимо от того, какую именно активность в Сети ведёт пользователь — незаконную или абсолютно легальную [6]. Право на приватность является одним из фундаментальных прав любого современного человека, в том числе и в Интернете.

Прежде всего рассмотрим понятие анонимности. При работе в Интернете анонимность — это невозможность связать активность пользователя с его реальной личностью и местоположением. Но формально следует обозначить различие между полной анонимностью и «псевдонимом» (в некоторых англоязычных публикациях используются термины *anonymity* и *pseudonymity*). Анонимное подключение к серверу означает, что сервер не способен выяснить его начальное происхождение (настоящий IP клиента), а также связать его с каким-либо идентификатором. Если же имеется любой идентификатор (Cookie-файл, уникальный отпечаток браузера и т.д.), по которому сервер может определить, что данный клиент подключался к нему раньше, то речь идёт уже о «псевдонимности» [7]. Фактически, во многих случаях этого достаточно, нет необходимости стремиться сделать каждое подключение полностью уникальным. Тем не менее, чем дольше используется один и тот же «псевдоним», тем больше накапливается профилирующей информации о его активности. Поэтому он должен периодически изменяться, иначе анонимность пользователя может быть в конце концов утрачена.

Ошибочно можно предположить, что анонимность означает полное отсутствие данных о пользователе. В ряде случаев это либо невозможно, либо нецелесообразно. Пример — собственно IP-адрес. При посещении сайта пользователь может скрыть свой настоящий IP, но технически невозможно

сделать это так, чтобы сервер не определил вообще никакого IP (и при этом отправил контент по назначению). То есть IP-адрес в конечном счёте не может полностью отсутствовать, его можно только замаскировать. Второй пример — User-agent браузера. Заменить его на пустую строку можно, но категорически нежелательно. Такой браузер будет резко выделяться среди множества других и приобретёт не анонимность, а особенную уникальность. К тому же многие сайты в нём будут работать некорректно. Здесь следует отметить, что User-agent сам по себе не уникален и относится к тем параметрам, по которым невозможно однозначно идентифицировать и отслеживать пользователя — однако сочетание большого количества «неуникальных» данных часто формирует уникальный цифровой отпечаток.

В мае 2015 года Совет по правам человека ООН представил отчёт заседания, посвящённого анонимности и шифрованию в интернете [8]. Главный вывод документа: *возможность анонимного пользования интернетом и использование шифрования личных данных и средств коммуникации необходимы и должны расцениваться как часть прав человека*. Несмотря на то, что средства анонимизации нередко применяются злоумышленниками, сама возможность быть анонимным в Интернете — только средство, которое может быть использовано в самых различных целях и по разным мотивам. Но до сих пор часто встречается мнение, что «обычному законопослушному пользователю» анонимность просто не нужна: ему нечего скрывать от государства, и его деятельность в Интернете никому не интересна [9]. Здесь прежде всего нужно вспомнить, что самого факта сбора данных это не отменяет. А отслеживанием пользователей занимаются не только спецслужбы, но и многие интернет-компании (Google — лишь наиболее яркий пример), и вообще большинство веб-сайтов [10]. Между тем, история действий пользователя в Сети относится к личным данным и не предназначена для посторонних глаз, как и личная переписка. Позиция «мне нечего скрывать» фактически означает «меня не волнует неприкосновенность моей частной жизни». Разработчики TOR придерживаются принципа «возможно, это и не секрет, но это просто не ваше

дело». Но наиболее удачно по этому поводу высказался американский юрист Гленн Гринвальд в 2014 году:

«Последние 16 месяцев, что я обсуждал эту тему по всему миру, каждый раз кто-то говорил мне: «Я не особо беспокоюсь по поводу вторжения в личную жизнь, потому что мне нечего скрывать». Я всегда отвечаю им одинаково. Я достаю ручку, пишу адрес своей электронной почты и говорю: «Вот моя почта. Я хочу, чтобы вы, придя домой, отправили мне пароли ко всем вашим учётным записям, не только к банальной, приличной рабочей почте, но ко всем, потому что я бы хотел иметь возможность покопаться в том, что вы делаете онлайн, почитать, что захочу, опубликовать то, что покажется мне интересным. В конце концов, если вы не плохой человек, если вы не делаете ничего плохого, то вам не нужно ничего скрывать». Ни один человек не принял моего предложения. Я каждый раз добросовестно проверяю свою почту, но она пуста. И тому есть причина, которая заключается в том, что мы, будучи людьми, даже те из нас, кто на словах отрицает важность собственной частной жизни, инстинктивно понимаем её чрезвычайную важность» [11].

Наконец, некоторым людям анонимность необходима в силу специфики их работы. Здесь показательна информация об использовании Tor в легальных целях. Корпорации используют его как безопасный способ проведения анализа на конкурентном рынке, а также в качестве дополнения к VPN. Журналисты могут пользоваться Tor для безопасного общения с информаторами и диссидентами, социальные работники — при общении с учётом тонкой социальной специфики в чатах и веб-форумах для беженцев, жертв насилия. Неправительственные организации используют Tor для подключения своих сотрудников к нужным сайтам в заграничных командировках, если есть смысл не афишировать их работу. Некоторые общественные организации рекомендуют Tor для обеспечения безопасности своих членов. Спецслужбы используют Tor для обеспечения секретности при выполнении особых задач. Гражданские активисты из EFF (Фонд электронных рубежей) поддерживают разработку Tor,

поскольку видят в нём механизм для защиты базовых гражданских прав и свобод в Интернете [12].

1.3. Возможность сохранения анонимности

Итак, в условиях современного мира надёжная интернет-анонимность может потребоваться практически любому человеку. Однако необходимый и достаточный уровень безопасности для разных категорий пользователей будет различным: например, одному человеку жизненно необходимо скрываться от опознания, а другому нужен «анонимайзер» просто для доступа к заблокированным веб-сайтам. Соответственно, выбор метода обеспечения анонимности начинается с чёткого понимания, для чего именно нужна эта анонимность. Общая схема моделирования угроз при защите персональных данных включает 5 основных вопросов (по версии EFF):

1. Что именно вы хотите защитить?
2. От кого вы собираетесь это защищать?
3. Насколько высока вероятность того, что вам придётся это защищать?
4. Каковы могут быть последствия, если вы потерпите неудачу?
5. Какие ресурсы вы готовы потратить на предотвращение этих последствий? [13]

Очевидно, что идеальная безопасность невозможна, любое решение содержит некоторый компромисс. В настоящее время нередко можно встретить высказывания, что анонимности в Интернете уже не существует. Тем не менее, обеспечить анонимную работу в Интернете в случае необходимости — по-прежнему возможно. Необходимо помнить следующее:

1. **Адекватно оценивать потенциального «противника».** Интернет-провайдер или владелец точки доступа Wi-Fi часто имеют возможность прослушать большую часть трафика, но, как правило, не заинтересованы в активном отслеживании и деанонимизации пользователя. Что же касается владельцев используемых ресурсов (веб-сайтов, прокси/VPN-серверов), то у них в распоряжении множество средств по отслеживанию (утечка DNS, Flash-плагины, баннерные сети, различные «отпечатки браузера», несколько разных

видов Cookies) и серьёзный коммерческий интерес к тому, чтобы надёжно отслеживать пользователя (для таргетирования рекламы, продажи данных и т.д). А правительство и спецслужбы могут получить доступ и к данным, собранным веб-сайтами, и к данным, которые хранятся у провайдера. Таким образом, **те, кто имеют возможность и желание отслеживать пользователя — имеют доступ к большинству возможных каналов утечки**.

2. **Каналов утечки информации очень много**, и они очень разнообразны (внезапное отключение VPN, получение реального IP через WebRTC или Flash-плагины браузера, отправка серийного номера каким-нибудь приложением при попытке обновления). При этом регулярно обнаруживаются (и создаются) новые пути утечки. Поэтому попытка блокировать каждый из них в индивидуальном порядке, уникальными для каждого методами, может просто не иметь смысла, всё равно что-то окажется упущено.

3. **При «работе в интернете» используется не только браузер** — у многих пользователей будет также запущен какой-нибудь мессенджер, почтовый клиент, торрент-клиент, что-либо ещё. При этом информация, передаваемая по их каналам, часто пересекается и позволяет связать их между собой (.torrent-файл, скачанный с сайта, загружается в торрент-клиент, пришедшая в письме/сообщении ссылка открывается в браузере и т.д). Добавим к этому то, что сама ОС и многие приложения регулярно соединяются с сетью для поиска обновлений и по иным причинам, передавая различную информацию, которая также может оказаться идентифицирующей [14].

Таким образом, частичная «анонимность» фактически не является анонимностью. Она может быть достаточной для некоторых задач, но почти бесполезна в тех случаях, когда существует потребность в действительно полноценной анонимности. Разумеется, ни одна схема не может быть абсолютно надёжной, к тому же деанонимизация нередко происходит из-за ошибок в поведении самого пользователя — аспекты социальной анонимности нельзя обеспечить техническими методами. Социальная инженерия никогда не утрачивает свою эффективность. Рекомендации по анонимному поведению

также будут рассмотрены далее, но основной темой исследования является техническая анонимность — то, что остаётся в рамках возможностей программного обеспечения.

Защита от отслеживания имеет некоторые технические ограничения, поскольку его блокировка возможна не во всех случаях. С одной стороны, многие веб-сайты используют отслеживающие элементы [10], сторонние трекеры для рекламы, аналитики и других маркетинговых инструментов, и в настоящее время популярны браузерные расширения для «защиты от отслеживания» — большинство таких трекеров действительно можно заблокировать. С другой стороны, все подключения к серверу записываются в лог, поэтому факт посещения сайта будет зафиксирован независимо от уровня анонимности клиента. Также, например, если провайдер может прослушивать весь трафик, то использование VPN не влияет на сам процесс перехвата, хотя и делает его малоэффективным. Таким образом, правильнее говорить не о защите от отслеживания, а о защите конфиденциальности данных в условиях отслеживания. Исключить отслеживание полностью — невозможно.

1.4. Способы идентификации и отслеживания

1.4.1. Основные пути утечки данных

1) IP-адрес, наиболее очевидный идентификатор, позволяет определить провайдера и страну (нередко и город). Если же производится целенаправленный розыск пользователя, запрос к провайдеру даёт множество дополнительных данных и в простейшем случае устанавливает личность. Любой анонимайзер прежде всего подменяет IP-адрес. Следует понимать, что это никак не влияет на реальный IP хоста, выданный провайдером. Запросы так или иначе перенаправляются на некоторый выходной узел, адрес которого будет служить «подставным», но главная задача заключается в том, чтобы сделать определение первоначального IP максимально затруднительным.

2) DNS провайдера. В некоторых случаях DNS-запросы могут идти в обход анонимного канала. Не все средства анонимизации обеспечивают защиту от утечки DNS.

3) Атаки профилирования: если большая часть трафика долго выходит в интернет через один узел, можно провести так называемое профилирование — отнести определённую активность к определённому псевдониму, который может быть деанонимизирован через другие каналы [15].

4) Прослушивание трафика на выходном узле, а также MITM-атаки. Особенно важно при наличии незашифрованного трафика.

5) Одновременное подключение к серверу по анонимному и открытому каналам может в некоторых ситуациях создать проблемы, например, при обрыве интернет-соединения оба канала перестанут функционировать, и на сервере потенциально можно будет определить их связанность, сопоставив время отсоединения пользователей.

6) Деанонимизирующая активность в анонимном сеансе — пользование публичными сервисами, особенно теми, на которых уже есть информация об этом пользователе.

7) MAC-адрес обычно недоступен конечному узлу, но иногда его подмена имеет смысл. Есть и другие идентификаторы, относящиеся к оборудованию и операционной системе, примеры будут рассмотрены далее.

8) Информация из браузеров. Отдельная обширная категория способов идентификации, которую следует рассмотреть очень подробно.

1.4.2. Отслеживание через веб-браузер

- Стандартные HTTP **Cookies**. При первом входе на сайт не приводят ни к каким утечкам данных, но в дальнейшем служат идентификатором пользователя. При этом полная блокировка приёма Cookies может быть неприемлема, так как помешает нормальной работе с сайтом. Противодействием обычно служит регулярная очистка cookies, а иногда их модифицирование.
- Сторонние (третьей стороны, 3rd party) cookies устанавливаются сторонними ресурсами, подключенными к посещаемому сайту. Главным образом связаны с таргетированием рекламы, запрет их приёма обычно не нарушает работу сайта.

- **LSO** (Local Shared Objects) или Flash Cookies являются общими для всех браузеров и не удаляются при стандартной очистке cookies. Настройки Flash Player позволяют отключить возможность хранения LSO.
- **HSTS SuperCookies** использует флаги HSTS, сохраняемые в браузере, для установки двоичного идентификатора. Они удаляются при очистке обычных cookies.
- **HTTP Etag** предназначен для проверки содержимого кэша, но может быть использован как идентификатор. Было описано подобное применение и для заголовка *Last-Modified*, он может хранить произвольную строку вместо даты. Сохранённые Etag удаляются путём очистки кэша.
- **Evercookie** [16], «неудаляемые куки» используют набор механизмов хранения и восстанавливаются из резервных копий после неполной очистки. Включают в себя все упомянутые выше методы, а также: хранение идентификатора в свойстве *window.name*, использование хранилищ HTML5 localStorage, sessionStorage, indexedDB, изолированного хранилища Silverlight и некоторые другие способы в зависимости от их доступности. Из-за способности восстановления (если хотя бы в одном из хранилищ осталась копия, будут восстановлены все остальные копии) также известны как zombie cookie.
- **HTML5 AppCache** также позволяет хранить уникальные данные в качестве идентификатора. Занимает промежуточное значение между механизмами хранения данных в HTML5 и обычным кэшем браузера.
- **SDCH-словари —** разработанный Google алгоритм компрессии, основанный на использовании предоставляемых сервером словарей. Эти словари можно использовать и для хранения уникальных идентификаторов, которые можно поместить как в ID словарей, так и непосредственно в сам контент [17].
- **Ubercookie** описывались как «современная версия Evercookie», но фактически это не разновидность Cookie, а один из способов получения цифрового отпечатка (browser fingerprinting). В данном случае используются AudioContext API (для получения набора данных об аудиоподсистеме) и метод getClientRects (даёт уникальный набор координат). Вообще такие способы

отслеживания могут использовать большое разнообразие параметров, сочетание которых будет уникальным для каждого браузера.

1.4.3. Цифровой отпечаток веб-браузера

- **Canvas fingerprinting** — отрисовка скрытого изображения с использованием HTML5 canvas и последующий перевод его в бинарную форму [18]. Причём рисуется текст, с использованием доступных системе шрифтов и рендерера. Набор шрифтов и методы сглаживания немного отличается на разных машинах. Рендерер зависит от версии браузера, ОС и от GPU. В итоге отрисованное изображение почти уникально (остаётся небольшая вероятность совпадения). Существуют браузерные дополнения, позволяющие либо блокировать отрисовку, либо подменять отпечаток. При этом ложное значение может иметь 100% уникальность, но отслеживать по нему невозможно, поскольку при каждом посещении страницы генерируется новый отпечаток.
- **WebGL fingerprinting** [19] — рендеринг изображения, как и в canvas fingerprint, но с использованием API WebGL. При наличии поддержки WebGL 2 доступный набор данных сильно увеличивается. С учётом того, что большинство сайтов не используют WebGL для работы, отключение WebGL в браузере обычно не вызывает дополнительных проблем, однако это может выглядеть подозрительно для современных антифрод-систем.
- **Audio fingerprinting** — анализ обработки звука аудиоподсистемой, использует AudioContext API [20]. Считается очень эффективным, при сочетании с отпечатком canvas точность идентификации практически достигает 100%. Частично изменить отпечаток можно путём переключения частоты дискретизации в системных настройках динамиков.
- **Метод getClientRects** позволяет получить точный размер и положение прямоугольника в имеющемся элементе DOM. Данные значения могут и с высокой долей вероятности будут различаться на разных компьютерах, даже с одинаковой версией браузера. Изначально был предложен для отслеживания

пользователей Tor Browser [21]. Изменение масштаба страницы повлияет на отпечаток.

- **Mouse fingerprinting:** полезной информацией является скорость прокрутки колеса мыши и движения курсора, доступные для отслеживания с помощью JavaScript. Способ отслеживания пользователей по движениям мыши вначале казался нелепым, но, по некоторым данным, он успешно используется на практике [21]. Такую технологию можно отнести уже к поведенческому анализу.
- **Заголовки HTTP_Accept** содержат набор значений, которые могут показаться стандартными для многих браузеров, но вероятность их совпадения у двух браузеров составляет около 1:1700.
- **Список установленных плагинов**, а также расширений (частично). От плагинов зависит и список поддерживаемых MIME-типов.
- Набор установленных **шрифтов**, помимо влияния на отпечаток canvas, может использоваться и отдельно. На их основе генерируется так называемый **Font fingerprint**.
- **Ход часов.** Если система не синхронизирует свои часы со сторонним сервером времени, то они начнут отставать или спешить, что создаст уникальную разницу между реальным и системным временем, которую можно измерить с точностью до микросекунды с помощью JavaScript. Но даже при синхронизации с NTP-сервером будут небольшие отклонения, которые также можно будет измерить [17].

Для оценки значимости признаков может быть использован энтропийный подход. Под энтропией понимается количество информации, приходящейся на одно элементарное сообщение источника, вырабатывающего статистически независимые сообщения. Поскольку характеристики наподобие «почти уникальный» или «малозначимый» не являются точными, исследователи из Electronic Frontier Foundation предложили количественную оценку в битах энтропии [22]. Так, для Canvas fingerprint энтропия составляет около 15,5 бит, уникальность этого отпечатка (если не включена подмена) — 1 на 48000.

Напротив, информация о том, что в браузере разрешён приём Cookies, имеет самую низкую ценность — около 0,2 бит. Далее приведены признаки с относительно низкой энтропией, пригодные для отслеживания только в сочетании с набором других свойств.

- Разрешение монитора и размер окна браузера (включая параметры второго монитора в случае мультимониторной системы), а также глубина цвета. Отдельно определяется «доступная область» (availWidth и availHeight), часто отличается от основной. Может быть получено не только через JavaScript, но и без него с помощью медиа-запросов CSS.
- User-Agent. Показывает версию браузера и ОС. Может быть легко изменён, но это не всегда имеет смысл, так как есть и другие пути определения платформы.
- Строка javascript *navigator.userAgent*, а также поля javascript-объекта *navigator*: *appCodeName, appName, appVersion, buildID, oscpu, platform, product, productSub, vendor, vendorSub*. Расширения для подмены User-Agent затрагивают и *navigator.userAgent*, но остальные параметры нередко игнорируются и легко выдают несоответствие. Функционал для их подмены замечен в расширении «User-agent Switcher».
- Заголовок HTTP Referer позволяет серверу определить, что пользователь перешёл на данную страницу с другого сайта, что помогает отслеживать перемещения. Часто бывает необходим для нормального функционирования сайта.
- Язык браузера (JavaScript *navigator.language*) и предпочитаемый язык отображения страниц (HTTP Accept-Language).
- Часовой пояс.
- Значение заголовка DNT (Do not track).
- Длина истории вкладок — значение атрибута history.length.
- Наличие сенсорного экрана и поддерживаемое количество касаний.
- Уровень заряда батареи (при наличии) через Battery Status API.

- Доступная информация о CPU и GPU.
- Результат вычисления некоторых математических функций. Пример с сайта browserprint.info: функция Math.tan(-1e300) в Windows и в 64-битном Linux возвращает совершенно разный результат.

Приведённый список параметров и методов составлен на основе данных, предоставляемых интернет-ресурсами *BrowserSpy.dk, panopticlick.eff.org, Whoer.net, browserleaks.com* и не является исчерпывающим.

Некоторые современные технологии отслеживания, теоретически, предназначены для антифрод-систем и не должны встречаться на сайтах, не связанных с электронными платежами. Но фактически это невозможно гарантировать. Значение имеет сам факт того, что некоторая технология существует и применяется на практике. Часть перечисленных выше свойств не зависят от браузера и могут быть использованы для кросс-браузерной идентификации. Как уже упоминалось, современные fingerprinting-методы могут даже не учитывать версию браузера, но всё равно распознавать конкретный ПК с высокой точностью за счёт особенностей его аппаратного обеспечения и операционной системы [23].

В целом можно выделить следующие принципы анонимизации браузера: данные с низкой энтропией могут вообще не нуждаться в защите, а если защита производится, следует подменять параметр на максимально распространённое значение, не придавая ему искусственную нестандартность. Но следует периодически изменять все или некоторые из этих параметров, поскольку в совокупности они всё равно образуют паттерн с высокой энтропией. Что же касается данных наподобие canvas-отпечатка, имеющих наибольшую ценность, то их следует изменять каждый раз, когда требуется «сменить личность».

1.4.4. Особенности некоторых протоколов

1. Origin Bound Certificates (ChannelID) — самоподписанные сертификаты, идентифицирующие клиента HTTPS-серверу. Для каждого нового домена создаётся отдельный сертификат, который используется для соединений,

инициируемых в дальнейшем. Сайты могут использовать ОВС для трекинга пользователей, не предпринимая при этом каких-либо действий, которые будут заметны клиенту. В качестве уникального идентификатора можно использовать криптографический хэш сертификата, предоставляемый клиентом как часть легитимного SSL-рукопожатия.

2. Подобным образом и в TLS есть два механизма — session identifiers и session tickets, которые позволяют клиентам возобновлять прерванные HTTPS-соединения без выполнения полного рукопожатия. Достигается это за счёт использования закешированных данных. Два этих механизма в течение небольшого промежутка времени позволяют серверам идентифицировать запросы, исходящие от одного клиента.

3. Практически все современные браузеры реализуют свой собственный внутренний DNS-кэш, чтобы ускорить процесс разрешения имён (и в некоторых случаях снизить риск DNS rebinding атак). Такой кэш можно использовать для хранения небольших объёмов информации. Например, если обладать 16 доступными IP-адресами, около 8–9 закешированных имён будет достаточно, чтобы идентифицировать каждый компьютер в Интернете. Однако такой подход ограничен размером внутреннего DNS-кэша браузеров и может потенциально привести к конфликтам в разрешении имён с DNS провайдера [17].

1.4.5. Обнаружение присутствия средств анонимизации

1) Утечка реального IP через Flash. Актуально в тех случаях, когда анонимизируется только трафик браузера, а не всей системы. При использовании прокси-сервера можно принудительно направить через него трафик Flash с помощью Proxifier или другой аналогичной программы. Если при анонимной работе не требуется наличие Flash-плагина, рекомендуется его отключать [24].

2) Утечка IP через WebRTC может происходить даже при использовании VPN. Чаще всего WebRTC не требуется для работы сайта, и его отключение в браузере не вызывает проблем, но есть и способы подмены раскрываемого IP.

3) Утечка DNS приводит к явному несоответствию IP-адреса и используемого DNS-сервера, а также косвенно раскрывает наименование интернет-провайдера. Использование публичных DNS-серверов (например, Google) не считается подозрительным. В случае, если VPN-клиент не обеспечивает стабильную защиту от такой утечки, целесообразно использовать DNSCrypt, по возможности выбрав адрес DNS той страны, которой соответствует подменный IP-адрес. Даже если невозможно обеспечить соответствие, это предохранит от утечки оригинального DNS.

4) Несоответствие браузерных данных об ОС и характерных **особенностей TCP** для этой ОС. Разные системы по-разному формируют TCP-пакеты, утилита p0f позволяет точно определить ОС и приблизительно её версию. Однако при использовании прокси-сервера будет определена ОС, на которой работает прокси, так как именно он генерирует пакеты. В итоге несовпадение этих данных с User-agent браузера означает либо подмену User-agent, либо использование прокси-сервера [25].

5) Принадлежность IP-адреса к сети Tor очевидно указывает на использование Tor, так как адреса всех выходных узлов известны. Использование VPN через TOR — один из путей решения проблемы.

6) Несовпадение часового пояса: IP-адрес имеет определённую геолокацию, что позволяет соотносить его с часовым поясом. Несоответствие системному времени означает подмену IP. Практически все анонимайзеры не подменяют часовой пояс в браузере, за исключением некоторых браузерных расширений. Обычно требуется изменять системные настройки времени.

7) Заголовки HTTP Proxy. Прокси-серверы, не относящиеся к анонимным, передают IP-адрес клиента за прокси. X_FORWARDED_FOR, FORWARDED_FOR, X_FORWARDED, HTTP_FORWARDED, HTTP_CLIENT_IP, HTTP_FORWARDED_FOR_IP, HTTP_VIA, FORWARDED_FOR_IP, HTTP_PROXY_CONNECTION — могут содержать реальный IP. С другой стороны, существует тактика намеренной имитации использования прокси, когда в пустой заголовок подставляется случайный IP-

адрес. Это создаёт впечатление, что основной IP является адресом прокси-сервера. Так работает, например, плагин Dolus.

8) Открытые порты, характерные для прокси, веб-прокси, VPN. Предпочтительно использование нестандартных портов, по возможности — с авторизацией.

9) Так называемый VPN fingerprint — обнаружение использования VPN по характерным значениям MTU/MSS и некоторым другим признакам, особенно актуально для OpenVPN [25].

10) Подозрительное название хоста: если по конечному IP разрешается имя хоста, оно не должно содержать слова наподобие vpn, hide, proxy и т.п. При настройке собственного VPN или прокси-сервера следует избегать «говорящих» имён, но предпочтительно полное отсутствие имени, доступного для внешних обратных DNS-запросов.

11) Определение туннеля по двустороннему пингу. Запустив пинг к клиентскому IP со стороны сервера, можно узнать приблизительную длину маршрута. То же самое можно сделать со стороны браузера через XMLHTTPRequest. Полученную разницу в петле более 30 мс можно интерпретировать как туннель. Способ срабатывает не во всех случаях [24].

12) Язык браузера, нехарактерный для страны, определяемой по IP. Может указывать на использование анонимайзера, но возможны исключения. Если присутствует только английский язык, то параметр считается нейтральным.

13) Принадлежность IP хостинг-провайдеру: обычно указывает на использование VPS.

1.4.6. Атаки пересечения и подтверждения в анонимных сетях

Атаки подтверждения (частный случай атак пересечения) основаны на том, что у противника есть предположение, какого рода сетевой ресурс посещает данный пользователь через анонимную сеть. Ему нужно лишь подтвердить или отвергнуть эту гипотезу. Для этого противнику нужно снять данные трафика с точки входа пользователя в анонимную сеть и точки выхода из неё к этому

ресурсу (или на самом ресурсе). В сетях с малой задержкой передачи данных будут наблюдаться явные корреляции по числу пакетов, по времени их отправки и другим параметрам, что позволит вычислить пользователя за один сеанс с вероятностью выше 90%, в то время как вероятность ошибки может быть меньше тысячных долей процента. Если противник применит активные методы — например, сам будет вносить задержки в трафик или повреждать пакеты, то для полного раскрытия пользователя иногда достаточно одного пакета данных.

Эти атаки несколько затруднены против скрытых ресурсов Tor и замкнутых файлообменных сетей типа Freenet, так как противнику неизвестно, откуда снимать трафик, даже если он знает, к какому ресурсу хочет обратиться пользователь. Тем не менее, похожие атаки такого рода бывают достаточно эффективны и в этих случаях.

Другой вариант атак пересечения (когда также заранее неизвестна по крайней мере одна из двух точек, откуда нужно снимать трафик) — противнику неизвестен ресурс, к которому хочет обратится пользователь, но он контролирует некоторое количество узлов анонимной сети. Если трафик пользователя случайно пройдёт через эти узлы в начальной и конечной точке, достаточно корреляции статистических параметров трафика (т.е. без необходимости его расшифровки) между входящим узлом (или между точкой входа в анонимную сеть у провайдера пользователя и конечным узлом цепочки), чтобы провести атаку пересечения и посмотреть, к какому ресурсу обращается пользователь с последнего узла цепочки. При этом количество узлов между первым и последним узлом цепочки не играет особой роли против большинства такого рода атак и является аргументом о бесполезности увеличения длины цепочек больше трёх узлов. Такой вариант атак существенно ограничивает анонимность пользователя в сетях типа Tor.

Следует помнить, что анонимные сети или защищают от анализа трафика (Tor) или обеспечивают цензурозащищённость информации (Freenet), но все такого рода сети плохо защищены против атак подтверждения получения информации, заведомо известной противнику, или иной возможности

статистических атак пересечения. Построение сетей с соблюдением условий такого рода — сложная теоретическая задача. В дизайне существующих анонимных сетей атаками пересечения и подтверждения в большинстве случаев пренебрегают или ограничиваются минимальными мерами защиты, так как защита от противника такого уровня слишком сложна, хотя и в меньшей степени, чем от условного «глобального наблюдателя». Разного рода атаки на нахождение корреляций практически на 100% эффективны и тривиально просты против одиночных шифрующих прокси и VPN, которые иногда используются для получения невысокого уровня «анонимности» [26].

Вывод: современные технологии отслеживания далеко выходят за рамки традиционных способов наподобие cookie-файлов, и борьба с ними становится достаточно сложной задачей. Сокрытие личности как таковое может показаться относительно простым, но в реальности содержит много неочевидных нюансов. Идентифицирующие данные необходимо не просто скрывать, но и регулярно изменять, так как статичный «псевдоним» подвержен отслеживанию не меньше, чем реальная личность. Наибольшую сложность может представлять подмена цифровых отпечатков с сохранением их полной правдоподобности.

2 Методы обеспечения анонимности в Интернете

2.1. Основные категории средств анонимизации

1) **Прокси-серверы** – есть несколько видов со своими особенностями, но обычно для анонимизации используются SOCKS5. В настоящее время не могут считаться надёжными, так как сами по себе не обеспечивают шифрование трафика, а также сравнительно легко поддаются деанонимизации даже при построении цепочки прокси: последовательное изучение логов на каждом сервере позволяет определить реальный IP при любой длине цепочки. Предпочтительно использование в сочетании с VPN.

2) **VPN-сервисы** – также существует несколько протоколов, сервисы чаще всего являются платными, обеспечивают высокую надёжность шифрования канала. Но, как и в случае с прокси-сервером, основной проблемой становится вопрос доверия к провайдеру сервиса. Подавляющее большинство VPN-провайдеров заявляют об отсутствии ведения логов, на самом деле это невозможно проверить, чаще всего логгирование ведётся. Также VPN имеет следующий недостаток: при внезапном разрыве VPN-подключения весь трафик пойдёт в интернет напрямую, что приводит к раскрытию реального IP. Проблема решается дополнительной настройкой правил файрвола.

3) **SSH-туннели**, изначально создавались (и применяются до сих пор) для других целей, но используются и «для анонимности». Частично схожи с VPN в отношении шифрования трафика, но имеют другие принципы работы и потенциально более низкую скорость. В отличие от VPN, не направляют по умолчанию весь трафик в туннель (хотя для этого существуют специальные программы), а используются наподобие локального прокси-сервера.

4) **Dedicated-серверы** – используются как удалённое рабочее место либо как платформа для запуска собственного VPN-сервера. Нередко используют виртуализацию (VPS), при которой на одном физическом хосте располагается несколько виртуальных серверов, что затрудняет отслеживание подключений к конкретному серверу [15].

5) Анонимная сеть **Tor**. Некоторое время считалась наиболее надёжным средством обеспечения анонимности в Интернете, в дальнейшем имели место случаи деанонимизации пользователей. Трафик на многих выходных узлах прослушивается, к тому же выход в сеть с IP-адреса, принадлежащего Tor, сам по себе расценивается как подозрительный.

6) **JonDonym**, или JAP (Java Anonymous Proxy). Направляет трафик через цепочку серверов, пользователь может сам выбирать используемые «каскады». Присутствует бесплатный и премиум-доступ. Браузер JonDoFox в ранних версиях являлся сборкой Firefox с набором дополнений, а в настоящее время это модифицированный Tor Browser.

7) **I2P** – анонимная, децентрализованная сеть, работающая поверх интернета, не использующая IP-адресацию. Превосходит Tor по надёжности шифрования передаваемых данных. Иногда позиционируется как альтернатива Tor, но на самом деле малопригодна для анонимизации доступа во внешний интернет (изначально не была предназначена для этого) из-за нестабильного и медленного подключения, особенно при отсутствии публичного IP-адреса.

8) Виртуальные машины – решают ряд дополнительных задач безопасности при анонимной работе, используются в комбинации с другими средствами. Гарантированно направить весь трафик виртуальной машины в канал VPN или Tor обычно легче, чем сделать это с трафиком основной системы. Браузер внутри виртуальной машины не имеет доступа к данным об аппаратном обеспечении физического хоста. Рекомендуется использовать в гостевой системе оформление, заметно отличающееся от основной, чтобы случайно не перепутать окна. Особенно важно визуальное отличие браузеров. Не допускается установка программного обеспечения с лицензией, связанной с реальными данными пользователя, во избежание утечки этих данных в анонимный канал [27].

9) Так называемые «антидетекты» – сборки браузеров с встроенной подменой различных идентификаторов. Часто создаются для нелегальной деятельности (нацелены на обход систем антифрода), имеют высокую стоимость и не выкладываются в свободный доступ. Встречаются и бесплатные решения с

различной степенью эффективности. Задача анонимизации трафика обычно остаётся на усмотрение пользователя. Термин «антидетект» также применяют к виртуальным машинам, модифицированным для правдоподобной маскировки под реальный ПК.

10) Иные средства анонимизации — слабо популярные, недостаточно проверенные или не обеспечивающие надёжную анонимность инструменты. Также сюда относятся программы и браузерные расширения, предназначенные для защиты браузера от отслеживания. Они дополняют систему анонимизации в тех аспектах, которые не обеспечиваются средствами, перечисленными выше.

2.2. TOR

The Onion Router — наиболее значимое и популярное средство для обеспечения анонимности в Интернете. Это свободное и открытое ПО, работающее по принципу так называемой луковой маршрутизации: все данные, попадающие в сеть TOR, проходят через три узла сети, выбираемых случайным образом, а перед отправкой последовательно шифруются ключами выбранных узлов. Когда первый узел получает пакет, он расшифровывает «верхний» слой шифра (отсюда аналогия с чисткой луковицы) и узнаёт, куда отправить пакет дальше. Аналогично поступают второй и третий сервер. Наиболее уязвимым местом в такой цепочке становятся выходные узлы (exit nodes), на которых трафик окончательно расшифровывается и направляется к целевому ресурсу. На выходных узлах трафик может прослушиваться, и об этом следует помнить в тех случаях, когда соединение с ресурсом происходит по небезопасному протоколу — например, посещается сайт, не поддерживающий HTTPS [28].

Фактически, TOR является сетью шифрующих прокси-серверов, или виртуальных туннелей, поддерживаемых преимущественно добровольцами. На 2017 год, эта сеть имеет около 7000 узлов, из которых 11% являются выходными узлами [29]. Таким образом, число возможных маршрутов очень велико, к тому же TOR обеспечивает смену маршрута каждые 10 минут. Входные узлы (entry nodes) обеспечивают защиту от перехвата и подделки данных на пути между входным узлом и клиентом. Кроме того, существуют мосты (bridges) —

ретрансляторы, адреса которых не публикуются в общем каталоге, а предоставляются по клиентскому запросу [30]. Мосты обеспечивают доступ к сети в тех случаях, когда интернет-провайдер блокирует известные входные узлы TOR, а также выполняют обфускацию (маскировку) трафика, что препятствует его идентификации и блокировке системами DPI. Разработано несколько типов мостов, в настоящее время наиболее эффективным считается obfs4.

Вероятно, для многих пользователей знакомство с Tor ограничивается работой в Tor Browser. Данная сборка состоит из приложения Tor и модифицированной версии браузера Firefox. Современные версии являются сравнительно надёжным и при этом доступным инструментом для противодействия отслеживанию и сохранения анонимности. Многие улучшения Tor Browser постепенно внедряются в обычный Firefox (проект Tor Uplift). Однако следует чётко различать Tor Browser и собственно Tor, который может быть запущен и без браузера. Ранее широко применялось приложение Vidalia – графический интерфейс для управления узлом Tor, но его разработка была прекращена. Существует также AdvOR (Advanced Onion Router), позволяющий принудительно направлять трафик приложений через Tor и настраивать различные параметры работы узла. Вообще говоря, обычный Tor Browser также позволяет использовать Tor в качестве прокси-сервера для различных приложений. Пока Tor запущен, он предоставляет локальный интерфейс SOCKS5, параметры которого можно увидеть в настройках прокси-сервера Tor Browser. Для приложений, не поддерживающих работу через прокси, возможно использование программы Proxifier или вышеупомянутого AdvOR. Важное ограничение: Tor поддерживает только TCP-трафик, но не UDP. В случае, когда необходимо функционирование UDP, потребуется дополнительное тунеллирование UDP-трафика через VPN.

Основной недостаток Tor Browser — в том, что факт его использования легко определяется со стороны посещаемого ресурса. Прежде всего, IP-адреса выходных узлов Tor известны, и некоторые сайты ограничивают доступ с таких

адресов, так как Tor нередко используется злоумышленниками. Также Tor Browser имеет характерные цифровые отпечатки (fingerprints). Механизмы борьбы с отслеживанием, используемые данным браузером, делают все экземпляры Tor Browser неотличимыми друг от друга (или, во всяком случае, стремятся к этому), поэтому отследить конкретного пользователя очень сложно, однако нетрудно распознать, что он использует Tor Browser. Разумеется, это не относится к внутренним сайтам сети Tor, onion-ресурсам, которые непосредственно предназначены для посещения через Tor.

Категорически не рекомендуется использовать Tor для BitTorrent. Это не только является угрозой для анонимности, но и создаёт излишнюю нагрузку на сеть Tor. Перечислим и некоторые другие вещи, которые не следует делать [31]. Нельзя заходить через Tor в аккаунты, связанные с реальной личностью, и также нельзя заходить без анонимизации в созданные через Tor аккаунты. Если учётная запись хотя бы раз использовалась с реального IP, она больше не является анонимной. Не следует забывать о социальных методах деанонимизации: нельзя раскрывать идентифицирующие данные при анонимном общении или публикациях. Нежелательно использовать одну и ту же цифровую личность слишком долго — чем дольше используется один псевдоним, тем больше накапливается профилирующей информации о нём. Не рекомендуется оставаться авторизованным в каком-либо аккаунте дольше, чем необходимо. Нельзя подключаться к ресурсу одновременно анонимно и неанонимно, так как это позволяет обнаружить корреляции между двумя соединениями. К скачиваемым файлам, особенно исполняемым, нужно относиться с максимальной осторожностью. Кроме того, нежелательно устанавливать какие-либо дополнения в Tor Browser и вообще изменять его стандартную конфигурацию.

Сеть Tor считается относительно надёжным средством анонимизации, но случаи раскрытия личности пользователей неоднократно имели место. Прежде всего отметим: деанонимизация далеко не всегда связана с уязвимостью самого Tor, часто используются методы социальной инженерии, и сам пользователь

может совершать ошибки. Тем не менее, «уязвимости нулевого дня» в Firefox (на котором основан Tor Browser) успешно эксплуатировались ФБР уже как минимум дважды [32]. Кроме того, некоторые методы отслеживания браузера, так называемый fingerprinting, оказывались пригодными для Tor Browser, хотя к настоящему времени разработчики значительно усилили его защиту [21]. Также сеть Tor периодически сталкивалась с проблемой вредоносных узлов, осуществлявших перехват и даже инфицирование трафика, и это относится не только к выходным ретрансляторам — в 2016 году исследователи обнаружили 110 директорий скрытых сервисов (HSDir), отслеживающих запросы к onion-ресурсам и используемых для поиска уязвимостей данных ресурсов [33]. Вредоносные узлы в Tor продолжают время от времени выявляться и блокироваться сетью.

Уязвимость Tor к атакам, анализирующим трафик, известна давно. Оригинальная проектная документация указывает на уязвимость системы перед «глобальным пассивным злоумышленником», способным прослушивать весь трафик входных и выходных узлов. Сопоставив оба потока трафика, подобный злоумышленник может деанонимизировать каждого пользователя. В реальности это возможно в меньших масштабах, поскольку ни одна организация не способна контролировать полностью всю сеть Tor, однако наличие даже двух контролируемых узлов (входного и выходного) уже даёт шанс идентифицировать некоторую, пусть и ничтожно малую, часть пользователей, чей трафик пройдёт через оба узла [34]. Tor изначально не был спроектирован для противостояния масштабным атакам, когда злоумышленник имеет множество точек присутствия внутри сети. Здесь уместно вспомнить сеть I2P, созданную с учётом того, что каждый узел может прослушиваться.

Итак, в настоящее время Tor остаётся сравнительно эффективным свободным инструментом для обеспечения анонимности и противодействия отслеживанию (в Tor Browser), продолжает активно разрабатываться и получать новые механизмы защиты. Однако его использование связано с некоторыми неудобствами и не является достаточным для надёжной анонимизации.

Целесообразно рассматривать Tor как основу для построения более сложных комбинаций.

2.3. Виртуальная частная сеть

Технология Virtual Private Network, предназначенная для защищённой передачи данных посредством шифрованного туннеля между двумя узлами, на сегодняшний день стала популярным способом анонимизации и часто воспринимается Интернет-пользователями как альтернатива Tor. Фактически это неверно — сохранение анонимности здесь полностью опирается на доверие к VPN-провайдеру, за исключением случаев, когда пользователь настраивает свой собственный VPN-сервер. Корректнее утверждать, что VPN обеспечивает приватность данных, например, позволяет скрыть от интернет-провайдера историю активности пользователя. При этом скорость соединения у платных VPN обычно намного выше, чем в Tor.

2.3.1. Протоколы

Существует несколько наиболее распространённых протоколов VPN:

- **PPTP**. Быстрый, легко настраиваемый, но сравнительно небезопасный и устаревший. Point-to-Point Tunneling Protocol был изобретён Microsoft и долгое время являлся стандартным протоколом для VPN. Для обеспечения безопасности он опирается на различные методы аутентификации. Хотя PPTP обычно используется со 128-битным шифрованием, в 1999 году был найден ряд уязвимостей. Наиболее серьёзной оказалась уязвимость протокола аутентификации MSCHAP v.2, и с её использованием PPTP был взломан в течение 2 дней. И хотя Microsoft исправила эту ошибку за счёт использования протокола аутентификации PEAP вместо MSCHAP, она сама рекомендовала к использованию для VPN протоколы L2TP или SSTP [35].
- **L2TP/IPsec**. Протокол туннелирования уровня 2, в отличие от других протоколов VPN, не шифрует и не защищает данные. Поэтому обычно используются дополнительные протоколы, в частности IPSec, с помощью которого данные шифруются ещё до передачи. Все современные устройства и

системы, совместимые с VPN, имеют встроенный протокол L2TP/IPSec. Установка и настройка совершаются легко и не занимают много времени, однако может возникнуть проблема с использованием порта UDP 500, который блокируется файрволами NAT. Так что, если протокол используется с брандмауэром, может потребоваться переадресация портов. Не известно о каких-либо крупных уязвимостях IPSec, и при правильном применении он обеспечивает надёжную защиту данных. Тем не менее, Эдвард Сноуден отмечал, что и этот протокол не так безопасен. Джон Гилмор, основатель и специалист по безопасности Electric Frontier Roundation, заявляет, что Агентство национальной безопасности США намеренно ослабляет протокол. Более того, двукратное инкапсулирование данных делает протокол не столь эффективным, как, например, решения на основе SSL, и поэтому он работает медленнее других протоколов.

- **OpenVPN** — сравнительно новая технология с открытым кодом, которая использует библиотеку OpenSSL и протоколы SSLv3/TLSv1 вместе с множеством других технологий для обеспечения надёжного VPN-решения. Одним из главных преимуществ является то, что OpenVPN очень гибок в настройках. Этот протокол может быть настроен на работу на любом порту, в том числе на 443 TCP-порту, что позволяет маскировать трафик внутри OpenVPN под обычный HTTPS, поэтому его трудно заблокировать. Ещё одно преимущество — библиотеки OpenSSL поддерживают множество криптографических алгоритмов (например, AES, Blowfish, 3DES, CAST-128, Camelia и другие). Как правило, VPN-провайдеры используют только AES и Blowfish.

Скорость OpenVPN зависит от уровня шифрования, но обычно она выше, чем у IPSec. И хотя OpenVPN сейчас используется большинством VPN-провайдеров, он не поддерживается по умолчанию на каких-либо платформах. Однако соответствующие сторонние приложения уже разработаны не только для ПК, но даже для Android и iOS. С этим связана другая проблема OpenVPN – гибкость может сделать его неудобным в настройке. В частности, при

использовании типовой программной реализации OpenVPN (например, стандартный открытый клиент под Windows) необходимо не только скачать и установить клиент, но и загрузить конфигурационные файлы. Многие VPN-провайдеры решают эту проблему путём использования преднастроенных VPN-клиентов.

С учётом всех факторов и информации, представленной Э. Сноуденом, можно считать, что протокол OpenVPN является самым безопасным на данный момент. Также предполагается, что он защищён от вмешательства Агентства национальной безопасности США, так как использует экспериментальные методы шифрования. Естественно, никто не знает всех возможностей АНБ, но скорее всего, OpenVPN — единственный по-настоящему безопасный протокол на сегодня [35].

- **SSTP**. Протокол безопасного туннелирования сокетов (Secure Socket Tunneling Protocol) был представлен Microsoft в Windows Vista SP1, и, хотя он теперь доступен на Linux, RouterOS и SEIL, он по-прежнему используется в значительной степени только Windows-системами. SSTP использует SSL v.3 и, следовательно, предлагает аналогичные преимущества, что и OpenVPN (например, возможность использовать TCP-порт 443 для обхода NAT), а так как он интегрирован в Windows, он проще в использовании и более стабилен, чем OpenVPN. Однако SSTP не имеет открытого исходного кода, и все права на него принадлежат Microsoft, поэтому OpenVPN использовать предпочтительно.
- **IKEv2** (протокол обмена ключами, версия 2) разработан Cisco и Microsoft, встроен в Windows 7 и последующие версии. Протокол допускает модификации с открытым исходным кодом, в частности для Linux и других платформ, также поддерживаются устройства Blackberry. Он хорошо подходит для установки автоматического VPN-подключения, если интернет-соединение периодически разрывается. Пользователи мобильных устройств могут воспользоваться им как протоколом для беспроводных сетей по умолчанию, он очень гибок и позволяет легко переключать сети. Хотя IKEv2 доступен на меньшем количестве платформ по сравнению с, например, IPSec, он считается достаточно хорошим протоколом

с точки зрения стабильности, безопасности и скорости работы. Недостаток — закрытый исходный код.

- **SoftEther VPN** — мультипротокольный VPN-сервер под лицензией GPLv2, разрабатывается с 2013 года, обладает широким спектром возможностей. Имеет собственный протокол SSL-VPN, который неотличим от обычного HTTPS-трафика. Заявлена поддержка L2TP/IPsec, MS-SSTP, OpenVPN, L2TPv3 и EtherIP, причём для L2TP указана строгая совместимость со встроенными клиентами в iOS и Android. Сам сервер имеет версии под Windows, Linux, OS X, FreeBSD и Solaris. Работает быстрее, чем OpenVPN, не требует наличия TUN/TAP, имеет встроенный NAT и DHCP. Протокол SSL-VPN может работать через TCP, причём поддерживаются множественные TCP-сессии, UDP и даже ICMP [36].

2.3.2. Проблемы выбора VPN-провайдера

Итак, при выборе протокола следует остановиться на OpenVPN, а если речь идёт о настройке собственного VPN-сервера, есть смысл использовать SoftEther VPN. Некоторые из бесплатных публичных серверов VPN Gate также предоставляют доступ по протоколу SoftEther (SSL-VPN). Заметим, что многие VPN-провайдеры предлагают собственные клиентские приложения для подключения — это может быть удобно, но потенциально небезопасно. Протокол OpenVPN подразумевает использование открытого клиента и конфигурационного файла, который и должен быть предоставлен провайдером. С другой стороны, приложение провайдера может иметь полезные функции: так называемый kill switch (предотвращение утечки трафика в обход VPN при обрыве подключения), защиту от утечек DNS. Впрочем, надёжность их работы необходимо тщательно протестировать.

К вопросу выбора VPN-провайдера следует подходить очень внимательно и ответственно. Бесплатные VPN часто вызывают недоверие, поскольку неясно, кто и с какой целью спонсирует сервис — возможно, вся деятельность пользователей отслеживается. Показательный пример: в 2017 году правозащитная группа Center for Democracy and Technology (Центр демократии

и технологий, CDT) уличила популярный сервис Hotspot Shield в нарушении собственной политики конфиденциальности. Исследователи обнаружили, что Hotspot Shield отслеживает поведение пользователей в интернете, перенаправляет интернет-трафик, продаёт данные своих пользователей третьим сторонам, а также раскрывает конфиденциальные данные, в том числе названия беспроводных сетей, MAC-адреса и идентификаторы IMEI устройств. Кроме того, приложение внедряло код Javascript для рекламных целей. Как показал реверс-инжиниринг исходного кода приложения, Hotspot Shield использовал более пяти различных сторонних библиотек для отслеживания пользователей.
В некоторых случаях сервис перенаправлял трафик на сайты партнёров, в том числе рекламных компаний, для получения прибыли.

Крупные платные VPN-сервисы, как правило, более серьёзно относятся к сохранению конфиденциальности. Однако не следует доверять заявлениям об отсутствии ведения логов, чаще всего логгирование активности производится, но многое зависит от объёма собираемых данных, времени их хранения и возможности предоставления их по запросу уполномоченных организаций. Полезно задать технической поддержке сервиса вопрос, возможна ли блокировка учётной записи в случае вредоносной активности пользователя. Если ответ сводится к тому, что доступ будет блокирован только при поступлении жалоб (abuses), то активность действительно не отслеживается. Также большое значение имеет возможность анонимной оплаты сервиса. Раскрытие платёжных данных пользователя VPN-провайдеру явно противоречит сохранению анонимности. Если сервис позиционируется как обеспечивающий анонимность, он обязан принимать криптовалюту. Заметим, что обычно принимается только Bitcoin, однако он не обеспечивает надёжной анонимности, если не использовать миксеры. Предпочтительными были бы такие криптовалюты, как Monero или Dash, более ориентированные на анонимизацию транзакций, но практически нет VPN-сервисов, которые бы принимали их к оплате.

Следует выбирать иностранного VPN-провайдера в юрисдикции той страны, которая не поддерживает дипломатические отношения со страной

пользователя, либо страны с либеральным законодательством, где получение логов сервера бывает затруднительно даже для местной полиции. Это же относится к использованию двух VPN (не DoubleVPN, а разных провайдеров) — желательно выбрать сервера в странах, не сотрудничающих друг с другом [37]. Кроме того, следует избегать стран «альянса Five Eyes» — основных участников соглашения UKUS SIGINT. Вообще выбор надёжного VPN-провайдера является сложной задачей даже для опытного пользователя. В 2016 году был запущен сайт thatoneprivacysite.net, где приведено детальное сравнение свыше ста VPN-сервисов по множеству параметров. Таблица не даёт однозначного ответа «какой из VPN лучший», но лидерами можно назвать Proxy.sh, расположенный на Сейшелах, шведские oVPN.se и IPredator, гибралтарский IVPN и исландский CryptoStorm. Хорошей репутацией также обладают Private Internet Access, NordVPN, Mullvad, AirVPN. Также есть небольшое число провайдеров, размещающих свою рекламу на ресурсах «теневой» направленности, по сути открыто предлагающих свои услуги потенциальным злоумышленникам. Отношение к таким провайдерам обычно противоречивое. Теоретически, такое поведение должно означать, что данный провайдер принципиально не сотрудничает с правоохранительными органами и обеспечит любому пользователю надёжную анонимность. Реальная же ситуация может быть прямо противоположной. При отсутствии веских причин для доверия к такому VPN, предпочтительно воздержаться от его использования.

Что касается различных DoubleVPN, TripleVPN, QuadVPN, то в большей степени это маркетинговый ход, чем повышение защищённости, поскольку все серверы цепочки принадлежат одному VPN-провайдеру, и их количество не препятствует ведению журнала активности пользователя и возможности раскрытия этих данных провайдером. Тем не менее, замена обычного VPN на DoubleVPN снижает вероятность деанонимизации. Следует учитывать, что это не двухслойное шифрование — в отличие от Tor, здесь трафик на промежуточном сервере расшифровывается. Но возможен и Parallel VPN — способ подключения через два параллельных VPN-канала, при котором трафик

шифруется дважды (канал в канале). Это несколько снижает скорость, но решает проблему незащищённости трафика на промежуточном узле.

Итог: VPN не следует рассматривать как надёжное средство обеспечения анонимности, но при правильном выборе провайдера и корректной настройке может быть достигнут высокий уровень конфиденциальности.

2.4. Использование VPS

Виртуальный частный сервер, применительно к анонимизации, используется для настройки собственного VPN, SSH или прокси-сервера, а иногда и узла Tor, если это позволяет VPS-хостер. Стоимость аренды VPS может оказаться ниже, чем покупка VPN. При этом административный доступ к серверу позволяет полностью отключить ведение логов и в целом настроить VPN-сервер под собственные нужды при наличии соответствующих навыков. Недостатком такого решения считается то, что пользователь на сервере всего один, и его значительно легче отследить, чем при использовании крупных платных и бесплатных VPN. С другой стороны, виртуальных серверов на физическом сервере несколько, поэтому для внешнего наблюдателя будет по-прежнему сложно сопоставить исходящие подключения с этого сервера с конкретным пользователем. При выборе провайдера руководствоваться можно теми же соображениями, что и для VPN. Как минимум, сервер не должен попадать под юрисдикцию спецслужб той страны, где находится пользователь, или стран, находящихся с ней в сотрудничестве.

Провайдеров VPS существует очень много, и значительная часть зарубежных компаний принимает к оплате Bitcoin. Однако, если предполагается сохранение анонимности при регистрации, проблемы могут возникнуть уже на этом этапе. Многие VPS-хостеры не разрешают анонимную регистрацию. В случае присутствия антифрод-системы следует учесть несколько базовых факторов: IP-адрес не должен быть адресом Tor или общедоступного прокси-сервера; личные данные должны быть правдоподобными, не нужно вводить случайные комбинации символов вместо Ф.И.О; адрес также правдоподобный, страна должна соответствовать IP-адресу; телефон — принадлежащий указанной

стране [38]. Вообще, при любой анонимной регистрации, когда требуется указать персональные данные, желательно создавать максимально правдоподобную личность-псевдоним, а не привлекать внимание вводом бессмысленных данных. И, естественно, если в дальнейшем планируется подключаться к VPS с реального IP-адреса, то анонимная покупка не имеет смысла.

При выборе сервера нужно обратить внимание на лимит трафика и пропускную способность. Ёмкость жёсткого диска практически не важна, но оперативной памяти рекомендуется не менее 512 мегабайт. Для разворачивания VPN-сервера необходима поддержка TUN/TAP (не нужна для SoftEther). В зависимости от конкретного хостера и типа виртуализации может потребоваться запрос к техподдержке, чтобы включить TUN-адаптер. Доступ к серверу предоставляется обычно по SSH. Его следует настроить на авторизацию по сертификату, чтобы обезопасить сервер от взлома пароля SSH. Затем, вероятно, потребуется настройка правил файрвола, и затем уже производится установка и конфигурирование основного ПО. Собственный сервер позволяет настроить VPN так, чтобы его использование нельзя было определить по MTU или характерным портам. Кроме того, существует возможность защитить сервисы от обнаружения злоумышленниками, используя так называемый port knocking. Это неявная форма разрешения доступа к некоему сервису, при условии прохождения предварительно заданной последовательности соединений с различными портами целевого сервера. Специальное ПО на стороне сервера отслеживает все входящие соединения, и, если фиксируется характерная «цепочка подключений» соответствующих ранее заданному «эталонному стуку» — временно открывает доступ к закрытому порту и, соответственно, скрытому сервису на нём [39].

2.5. Операционные системы для анонимной работы

Существует ряд дистрибутивов Linux, специально нацеленных на обеспечение анонимности и безопасности. Как правило, такие сборки основаны на Debian, используют сеть Tor и различные дополнительные средства защиты.

Если не рассматривать системы, разработка которых была прекращена, то на данный момент выделяются следующие проекты:

- Whonix
- Tails
- Kodachi
- MOFO Linux
- Subgraph OS
- heads

Рассмотрим подробнее два первых пункта этого списка.

2.5.1. Whonix

ОС Whonix — система для анонимной работы, основанная на Debian и состоящая из двух виртуальных машин, одна из которых является шлюзом, отправляющим весь трафик в сеть Tor, а другая – изолированной рабочей станцией, подключающейся только к шлюзу. Существует также вариант физического разделения шлюза и рабочей станции. Whonix реализует в себе механизм так называемого изолирующего прокси-сервера. Рабочая станция не получает внешний IP-адрес в Интернете, и это позволяет нейтрализовать множество уязвимостей, например, даже если вредоносное ПО получит root-доступ к рабочей станции, у него не будет возможности узнать реальный IP-адрес [40].

Whonix, как утверждают разработчики, успешно прошла множество тестов на утечки. Даже такие приложения, как Skype, BitTorrent, Flash, Java, известные своими особенностями выходить в открытый Интернет в обход Tor, были успешно протестированы на предмет отсутствия утечки компрометирующих данных. ОС Whonix реализует следующие механизмы анонимизации:

- весь трафик любых приложений идёт через сеть Tor;
- для защиты от профилирования трафика Whonix реализует концепцию изоляции потоков. Предустановленные в Whonix приложения настроены на использование отдельного Socks-порта, а так как каждый Socks-порт

использует отдельную цепочку узлов в сети Tor, то профилирование невозможно;

- обеспечивается безопасный хостинг сервисов Tor Hidden services. Даже если злоумышленник взломает web-сервер, он не сможет украсть закрытый ключ Hidden-сервиса, так как ключ хранится на Whonix-шлюзе;
- Whonix защищён от DNS-утечек, так как в своей архитектуре использует принцип изолированного прокси. Все DNS-запросы перенаправляются на DnsPort Tor;
- Whonix поддерживает obfuscated bridges — мосты Tor;
- применяются технологии «Protocol Leak Protection and Fingerprinting Protection», снижающие риск идентификации по цифровому отпечатку браузера или системы путём использования наиболее общих значений, например, имя пользователя – user, временная зона – UTC и т.д.;
- есть возможность туннелировать другие анонимные сети: Freenet, I2P, JAP, Retroshare через Tor, или работать с каждой такой сетью напрямую;
- важно отметить, что в Whonix протестированы, документированы и успешно работают все схемы комбинирования VPN/SSH/Proxy с Tor [41];
- Whonix – полностью открытый проект, использующий свободное ПО.

Установка Whonix возможна несколькими способами. Запуск виртуальных машин в VirtualBox — наиболее простой способ. Более надёжным считается использование Qubes-Whonix, когда в качестве хостовой операционной системы используется Qubes OS, а Whonix-Gateway устанавливается через встроенные средства виртуализации. Система Qubes OS использует гипервизор Xen для реализации подхода «безопасность через изоляцию». Также существует возможность запуска Whonix с виртуализацией KVM с помощью qemu-kvm, и последний вариант — физическая изоляция, установка двух компонентов Whonix на две физических машины. При этом рекомендуется устанавливать шлюз (Gateway) непосредственно на «железо» ПК, а рабочую станцию (Workstation) — в виртуальную машину. Отметим, что разработчики после проведённых исследований признали Qubes-Whonix более безопасной, чем

физическую изоляцию [42]. Впрочем, в Xen также возможны уязвимости. Ещё одна особенность Whonix — возможность подключения через Gateway практически любой виртуальной машины вместо Whonix-Workstation.

В настоящее время установка Whonix под Windows максимально упростилась ввиду появления автоматического установщика, который самостоятельно скачивает и импортирует в VirtualBox образы виртуальных машин, а затем позволяет запустить их нажатием одной кнопки. Тестирование выявило проблему: инсталлятор устанавливает отдельный экземпляр VirtualBox, даже если VirtualBox уже присутствовал в системе. В результате возникает конфликт, и оба экземпляра оказываются неработоспособны. В такой ситуации следует деинсталлировать оригинальный VirtualBox, а затем переустановить его в каталог, который был создан установщиком Whonix.

2.5.2. TAILS

The Amnesic Incognito Live System получила известность как «система, которую использовал Эдвард Сноуден» и «самая анонимная ОС». На самом деле сложно сказать, что Tails лучше (или хуже), чем Whonix, поскольку их концепции существенно различаются. Tails является Live-дистрибутивом для загрузки с Flash-накопителя и не оставляет следов на компьютере, где использовалась. Как и Whonix, Tails основана на Debian. Все исходящие соединения осуществляются через сеть Tor, а попытки неанонимных соединений блокируются [43]. Tor Browser работает в защищённом режиме (AppArmor). В то же время Tails имеет «Небезопасный браузер» (обычный Firefox), позволяющий посещать сайты напрямую, без Tor. В целом Tails может показаться менее безопасной, чем Whonix, так как имеет доступ к физической системе, MAC-адресу, реальному IP, в то время как Whonix-Workstation изолирован в виртуальной машине. С другой стороны, в случае Whonix возможны уязвимости как в двух её компонентах, так и в VirtualBox и в операционной системе хоста. В принципе запуск Tails в виртуальной машине также возможен, но потребуется использовать пакет virt-manager в Debian.

Кроме Tor Browser, в Tails предустановлен набор ПО, в частности:

- Pidgin – Jabber+OTR
- Electrum – лёгкий клиент для Bitcoin
- KeePassX – менеджер (хранитель) паролей
- GPG – система асимметричного шифрования
- MAT – удаление метаданных из различных типов файлов
- Программы для редактирования документов, фото, аудио, видео и т.д.
- Thunderbird – почтовый клиент
- Легко поставить Psi или Psi+ (Jabber с поддержкой GPG)

Процедура установки Tails из-под Windows несколько своеобразна, для неё потребуются два Flash-накопителя. Сначала установочный образ Tails записывается на первый носитель (объёмом в 2 Гб) — это «промежуточная» Tails, ограниченно пригодная для работы (при установке из Linux процедура более проста, и промежуточный носитель не требуется). Затем следует загрузить ПК с этого носителя. Нередко на этом этапе возникает проблема, BIOS не может корректно загрузить образ. В таком случае рекомендуется перезаписать Tails на носитель, используя программу Rufus вместо рекомендуемого Universal USB Installer. Обычно после этого загрузка проходит успешно. Далее подключается второй накопитель, и на него производится установка «основной» Tails. Для этого следует выбрать в меню Приложения → Tails → Tails Installer → Install by cloning. После успешного завершения установки второй носитель готов к работе, а первый более не требуется. Можно завершить работу системы.

Производим загрузку со второго накопителя. Теперь, чтобы иметь возможность сохранять какие-либо данные в системе, следует создать постоянный раздел — криптоконтейнер LUKS. Выбираем в меню Application → Tails → Configure Persistence и задаём пароль, желательно криптостойкий. Есть возможность выбрать, какие данные будут сохраняться. Всё, что не сохранено в постоянном разделе, очищается после перезагрузки Tails. Отметим, что у Tor Browser есть возможность чтения и записи только в 2 папки, они есть в закладках проводника: *Tor Browser* и *Tor Browser (Persistent)*. Скачивание и выгрузка файлов возможны только в/из них. При наличии действительно важных данных

следует периодически делать их резервную копию на другой носитель, поскольку шанс внезапного выхода из строя Flash-накопителя намного выше, чем жёсткого диска.

Использование VPN в Tails не рекомендовано разработчиками, поэтому такая возможность по умолчанию отсутствует, и настройка VPN требует вмешательства в правила iptables. Считается, что цепочка «VPN через Tor» вредит анонимности, об этом сказано в официальной документации Tor. Дело в том, что важным преимуществом Tor является частая смена маршрутов трафика, а при подключении к VPN-серверу через Tor фактически создаётся постоянный маршрут, фиксированное место назначения. Тем не менее, реализовать такую цепочку позволяет Whonix. Для Tails возможна схема «Tor через VPN», если использовать роутер с прошивкой dd-wrt и подключиться к VPN с роутера.

При необходимости более надёжного сокрытия шифрованных данных целесообразно использовать TrueCrypt (или VeraCrypt). В настоящее время создатели Tails рекомендуют использовать cryptsetup, основанный на LUKS. Эта программа позволяет создавать скрытые разделы, однако такой раздел скрыт не до конца. Существует возможность обнаружить заголовок скрытого раздела, что позволяет установить его наличие. Заголовок же скрытого раздела TrueCrypt неотличим от случайных данных, и, насколько известно, обнаружить его невозможно (убедительная отрицаемость) [44].

При запуске Tails синхронизирует системные часы. Если при этом обнаруживается существенное расхождение времени, Tor Browser прекращает работу и перезапускается. С точки зрения внешнего наблюдателя, такое поведение может быть использовано для выявления пользователей Tails, главным образом потому, что синхронизация происходит при каждом запуске системы.

2.5.3. Сравнение Whonix и Tails

Обе системы основаны на Debian и используют Tor Browser. В целом, Whonix больше предназначена для установки на регулярно используемый ПК, в

то время как Tails – скорее «походный» инструмент, позволяющий анонимно выйти в Интернет с чужого ПК. Ниже представлены некоторые из отличий.

Таблица 1 – сравнение дистрибутивов

	Whonix	Tails
Тип системы	Образы виртуальных машин либо установка на ПК или USB-диск	Live-дистрибутив для загрузки с DVD или USB-носителя
Запуск в VirtualBox	Да	Допускается
Защита от утечек IP	Полная, кроме случая взлома Whonix-Gateway	Утечка возможна при ошибках системного ПО или заражении вирусом
Защита от атаки «холодной загрузки»	Нет	Да
Поддержка VPN	Да, документировано	Не предусмотрена
Скрытие MAC-адреса хоста в локальной сети	Нет	Да
Может служить шлюзом в сеть Tor для любой ОС	Да	Нет
Возможность посещать сайты напрямую, без Tor	Нет, но можно через браузер основной ОС	Через отдельный браузер (Firefox)

2.6. Специфика анонимного поведения

Анонимная работа в Интернете редко ограничивается просмотром веб-страниц, она может включать в себя регистрацию на каких-либо сайтах, публикацию текстов, общение на форумах, связь по электронной почте или в Jabber и т.д. без утраты анонимности. В таких ситуациях техническая анонимность становится недостаточной, возникает необходимость не допустить утечки информации от самого себя. Далеко не всем пользователям могут потребоваться подобные меры безопасности. Прежде всего при создании альтернативной личности следует помнить, что она не должна пересекаться с реальной даже косвенно.

- Оценить степень доверия к ресурсу, на котором регистрируется профиль.
- По возможности использовать временный e-mail адрес (Dropmail, 10MinuteMail) или постоянный, но специально созданный в анонимном сеансе.

- Не раскрывать дату рождения либо указать неверные данные.
- В случаях, когда необходимо указать имя и фамилию, не следует делать их излишне экзотическими или абсурдными, чтобы не привлекать дополнительного внимания.
- Иногда целесообразно указать реальный город проживания, чтобы придать профилю больше правдоподобности. Иначе в процессе общения может быть замечено, что аноним практически не знает город, в котором якобы проживает. Если же нет необходимости указывать город, то и делать это не нужно. По возможности — вообще не раскрывать географические данные, включая часовой пояс.
- «Мульти-ник»: следует использовать разные никнеймы в разных местах, если нет явного желания идентифицировать себя как одну и ту же личность.
- «Кросс-постинг»: полный запрет на одинаковые тексты и ссылки на них из-под разных профилей [45].
- Стиль речи может говорить об уровне образования, проф.принадлежности и т.п.
- Характерные речевые обороты, «коронные фразы», повторяющиеся ошибки в речи. Может указать на связь двух профилей или даже на реальную личность.
- При регистрации в анонимных сетях — не использовать свои никнеймы из «обычного» Интернета.
- Обязательно удалять метаданные из отправляемых файлов, например, EXIF из фотографий, имя пользователя из документов. К полученным файлам от неизвестных лиц следует относиться с особой осторожностью [27]. Например, картинки, полученные из непроверенного источника, могут содержать стеганографическую метку. Если планируется где-либо публиковать их с другого профиля, есть смысл перекодировать их с потерями.
- Время публикации сообщений может локализовать основное времяпрепровождение.

- В анонимном сеансе работы нельзя посещать аккаунты, связанные с реальной личностью, особенно в соцсетях. Даже если профиль не содержит настоящих данных, но был создан при неанонимном подключении, он уже небезопасен. И наоборот, при обычной работе без анонимизации — не входить в анонимный аккаунт.
- В некоторых случаях, особенно на малопосещаемых ресурсах, общность нескольких анонимных подключений становится заметна из простого логического соображения: если за короткий промежуток времени зашли несколько неизвестных пользователей с редким отпечатком браузера — скорее всего, пользователь один [16].
- При копировании текста с веб-сайта стоит проверить его на наличие скрытых (непечатаемых) символов [46].

Вывод: существует значительное количество программного обеспечения, ориентированного на обеспечение анонимности и приватности. Современные средства позволяют достичь высокого уровня безопасности, однако она всегда зависима от человеческого фактора. Наиболее мощным инструментом сокрытия личности является Tor и анонимные операционные системы на его основе. VPN-сервисы менее безопасны, но более удобны в использовании. Подключение к VPN через Tor имеет как преимущества, так и недостатки.

3 Проектирование программного комплекта

3.1. Исходные данные и постановка задачи

Поскольку подразумевается, что итоговый набор ПО предназначен для широкого круга пользователей (потребность в анонимности может возникнуть у любых, а не только «продвинутых»), будем предполагать, что исходная система не анонимна: интернет-провайдеру известна личность пользователя, ПК используется для повседневной работы, и скорее всего под ОС Windows. Допускается, что решение не будет полностью бесплатным, так как будет задействован надёжный VPN-сервис или предварительно настроенный VPS.

Сформулируем требования к реализации:

- Скрыть от посещаемых сайтов все данные, связанные с исходной системой и браузером, используемым для не-анонимной активности;
- Обеспечить шифрование трафика, проходящего через оборудование (DPI-системы, СОРМ-3 и т.д.) интернет-провайдера;
- Обеспечить возможность многократной смены цифровых отпечатков;
- Исключить возможность утечки реального IP в анонимном браузере;
- Сайт не должен обнаруживать, что средства анонимизации используются;
- Системы анализа трафика не должны опознавать наличие VPN или Tor;
- Решение должно быть пригодно для предоставления пользователю в уже готовом виде, с несложной процедурой установки и быстрой настройкой.

Очевидно, что в реальности пользователь может отказаться от готового решения, поскольку не имеет оснований доверять разработчику. Кроме того, полностью скрыть все данные о реальной личности обычно невозможно в силу человеческого фактора. Естественно, что пользователь из России будет посещать в основном русскоязычные сайты, переключаться на русский язык отображения страниц, писать комментарии и, в конце концов, общаться на родном языке. Но следует принять во внимание, что такие сайты будут составлять лишь меньшую часть от всего объёма посещаемых ресурсов.

Не все названные требования являются обязательными. Например, если интернет-провайдер не блокирует трафик Tor или OpenVPN, то нет и прямой

необходимости маскировать его, но пользователь может предпочитать делать это «на всякий случай». Также, далеко не все сайты как-либо проверяют наличие средств анонимизации и тем более оценивают правдоподобность отпечатков. В решении, которое будет описываться далее, делается попытка реализовать все вышеуказанные требования.

3.2. Выбор ПО и необходимой конфигурации

3.2.1. Веб-браузер

Ввиду поставленной цели — максимально скрыть факт анонимизации — использование Tor Browser оказывается нежелательным, поскольку он легко обнаруживается и потенциально привлекает внимание. Предполагается, что будет реализована цепочка «VPN через Tor», при которой на выходе имеется IP-адрес VPN-сервера, не вызывающий подозрений, в отличие от адресов Tor. Добиться этого в Tor Browser сложно — он направляет трафик исключительно в Tor и не принимает альтернативных настроек прокси-сервера. В то же время, как упоминалось выше, Tor Browser имеет характерные цифровые отпечатки. Следовательно, в нашем случае необходимо использовать обычный Firefox, но для этого потребуется значительно изменить его конфигурацию. Варианты с Chromium-браузерами не рассматриваются, так как для анонимной работы практически всегда рекомендуется Firefox — этому способствует и репутация Mozilla, активно выступающей за сохранение приватности, и большая гибкость настроек браузера.

В **приложении Г** приведены некоторые параметры, которые доступны через служебную страницу about:config (некоторые отсутствуют по умолчанию, но работают, если их создать) [47]. Кроме них, существует ещё множество параметров, так или иначе пригодных для усиления защиты. Основная цель такой настройки – предотвращение утечки различных второстепенных данных, с учётом того, что все основные функции браузера должны работать как обычно. К примеру, отключение различных опций телеметрии – не более чем способ повысить конфиденциальность, однако отключение WebRTC – характерный

признак борьбы с утечкой реального IP при использовании некоторых средств анонимизации, а подобных признаков следует избегать.

В обычном меню настроек Firefox активируем пункт «Всегда работать в режиме приватного просмотра». Хотя режим инкогнито не обеспечивает анонимность, он является наиболее простым и эффективным средством борьбы с Evercookie, так как любые сохранённые идентификаторы будут удалены после закрытия окна браузера независимо от способа их хранения. Теоретически, можно отключить использование кэша и локального хранилища, однако на практике это может вызвать некоторые проблемы. На вкладке «Приватность» рекомендуется запретить приём cookies со сторонних сайтов. В дополнительных настройках – полностью отключить отправку телеметрии.

В настоящее время Firefox содержит некоторые опции противодействия «фингерпринтингу», заимствованные из Tor Browser. Соответствующий режим активируется опцией privacy.resistfingerprinting. Однако, данный режим мы использовать не будем, поскольку некоторые цифровые отпечатки в нём идентичны отпечаткам Tor Browser, например, Canvas fingerprint. Также он подменяет часовой пояс на UTC без возможности выбора, а в нашем случае часовой пояс должен соответствовать геолокации используемого IP-адреса.

Кроме изменения настроек Firefox, потребуется использовать некоторые браузерные дополнения для подмены отпечатков и блокировки отслеживания.

- CanvasBlocker – подменяет отпечаток Canvas fingerprint. Имеет опцию полной блокировки запроса canvas readout и разные режимы подмены, а также поддерживает белый и чёрный списки. Отпечаток генерируется случайным образом при каждом обновлении страницы, что исключает возможность отслеживания пользователя по данному отпечатку.
- NoScript – расширение, позволяющее блокировать исполнение JavaScript, Java, Flash и других потенциально опасных компонентов HTML-страниц. Также предоставляет защиту от XSS-атак.
- uBlock Origin – расширение для фильтрации контента. Позволяет блокировать не только рекламу, но и различные отслеживающие элементы

(списки фильтров в категории «Приватность» следует активировать). В некоторых случаях защищает даже от фингерпринтинга: например, если сайт использует стандартный скрипт fingerprint2.js, загрузка скрипта будет блокирована, так как он входит в список фильтрации. Имеет опцию предотвращения утечки локального IP через WebRTC. Также послужит заменой Safe Browsing благодаря спискам вредоносных доменов.

- Decentraleyes – защищает от отслеживания со стороны крупных CDN (сетей доставки контента) путём предоставления локальных ресурсов и блокирования сетевых запросов к CDN. Может рассматриваться как дополнение к фильтрам. Не вызывает проблем с функциональностью сайтов.
- Privacy Badger – средство блокировки отслеживающих элементов, создан Фондом электронных рубежей (EFF), способен к «самообучению».
- HTTPS Everywhere – ещё одно дополнение от EFF, принудительно использует https-соединение для сайтов, которые это поддерживают.
- Smart Referer – подменяет http referer, позволяет отправлять referer только в пределах одного сайта (рекомендованный режим) либо удалять referer вообще (возможны проблемы). Поддерживает добавление исключений.
- AudioContext Fingerprint Defender – искажает отпечатки AudioContext путём добавления случайного шума.
- ScriptSafe – содержит множество функций анти-отслеживания, частично повторяет функционал NoScript, uBlock и других дополнений, но имеет и некоторые уникальные опции: предотвращение манипуляций с буфером обмена, добавление случайных малых задержек между нажатиями клавиш.
- User-agent Switcher – подмена User-agent, в том числе через JavaScript.

Следует также упомянуть дополнение RAS (Random Agent Spoofer), полезное для более ранних версий Firefox. Это инструмент для подмены профиля браузера (User-agent и ряд сопутствующих параметров) с широким списком возможностей (впрочем, многие его настройки просто управляют штатными параметрами конфигурации Firefox). Для некоторых функций использует внедрение скрипта (script injection), поддерживает анонимизацию параметра

window.name, подмену разрешения экрана, часового пояса (в протестированной версии опция Time Zone Spoofing отсутствовала по неясной причине). Разработка данного расширения прекращена из-за трудностей миграции на новый стандарт расширений Firefox WebExtension. Это означает, что с Firefox 57 и выше Random Agent Spoofer несовместим.

Завершая рассмотрение браузера Firefox, отметим недавнюю инициативу по интеграции Tor в Firefox и, в дальнейшем, полному слиянию Tor Browser и Firefox в единый браузер (проект Fusion), который сможет работать в различных режимах. Это станет логическим продолжением текущего проекта Tor Uplift. Планируется и дальнейшее усиление функций борьбы с «фингерпринтингом» браузера, а также повышение удобства их использования.

3.2.2. Архитектура системы

Для надёжной защиты от возможных утечек и для изоляции браузера от основной системы было решено использовать виртуальную машину. Поскольку концепция Whonix — две ВМ, одна из которых служит интернет-шлюзом, соединённые внутренней сетью — работает очень эффективно, она и будет применена в данном случае. Whonix позволяет подключать к своему шлюзу не только оригинальную Whonix-Workstation, но и любую другую ВМ. Несмотря на то, что для анонимной работы традиционно используется Linux, выбор сделан в пользу Windows – такая машина будет выглядеть намного более «обычной», так как подавляющее большинство ПК работает под Windows. Попытки маскировать Linux-версию браузера под Windows-версию потенциально ненадёжны и потому нежелательны. Отметим, что современная Windows 10 содержит большое количество функций, направленных на сбор и отсылку данных о пользователе и явно неподходящих для анонимной работы. Даже применяя все возможные рекомендации и программы для отключения «сбора телеметрии», невозможно гарантировать надёжное обеспечение приватности. Поэтому будет установлена Windows 7, из которой также потребуется удалить несколько обновлений с функционалом отправки телеметрии. На сегодняшний день данная система всё ещё широко используется, и её наличие не будет выглядеть подозрительно.

Шлюз Whonix-Gateway обеспечит анонимизацию трафика средствами сети Tor, но необходимо скрыть факт использования Tor как от посещаемых сайтов, так и от интернет-провайдера (если в этом есть необходимость). IP-адрес не должен быть адресом узла Tor, поэтому дополнительно используется VPN. Возможны два варианта — персональный VPN-сервер, запущенный на VPS, или использование какого-либо VPN-сервиса. Первый вариант позволяет настроить VPN для максимальной защищённости (отсутствие ведения логов, применение надёжных криптографических алгоритмов, различные меры для скрытия факта использования VPN), однако имеет очень существенный недостаток — сервер только один, и возможность многократно менять IP-адрес отсутствует. Любой коммерческий VPN-сервис предоставляет на выбор целый ряд серверов, часто они расположены в различных странах, и пользователь может переключаться между ними в любой момент. С другой стороны, далеко не все VPN-провайдеры настраивают свои серверы так, чтобы сайты не могли распознать наличие VPN. В практической части данной работы будет продемонстрирован пример запуска собственного VPN-сервера и приведена его конфигурация.

При настройке VPN-сервера предусмотрено следующее: используется протокол TCP и порт 443 (другой вариант – нестандартный порт, нехарактерный для VPN и прокси-серверов). Все DNS-запросы направляются через VPN. Адреса DNS взяты из списка OpenNIC и относятся к той же стране, где расположен выбранный VPS. Сервер блокирует внешние ICMP-запросы, поэтому метод «двустороннего пинга» для определения туннеля не работает. Значение MTU принудительно устанавливается в 1500, сжатие трафика (характерный признак OpenVPN) отключено. Задействована опция шифрования управляющего канала в сочетании с HMAC-аутентификацией (tls-crypt) в OpenVPN.

Для маскировки трафика Tor (и на случай возможной блокировки доступа к сети Tor интернет-провайдером) будет задействован obfs4 – так называемый «подключаемый транспорт», дополнительный компонент Tor, специально предназначенный для противодействия анализу трафика DPI-системами. Кроме того, целесообразно исключить из использования узлы Tor, находящиеся в

стране пребывания пользователя, в нашем случае это российские узлы. Данная возможность встроена в приложение Tor и легко настраивается. Все изменения конфигурации Tor потребуется выполнить на Whonix-Gateway. За исключением этих действий, вмешиваться в настройки на шлюзе не рекомендуется.

На основной виртуальной машине, кроме браузера и VPN-клиента, по желанию пользователя может быть установлено дополнительное ПО. Например, GPG4Win для шифрования текста и файлов, Exif Purge для удаления данных EXIF из фотографий, Tox или Jabber-клиент для безопасного обмена сообщениями (естественно, если собеседник согласен пользоваться тем же приложением). Вопрос об установке антивируса является дискуссионным. С одной стороны, коммерческий продукт – например, ESET Internet Security – обеспечил был намного лучшую защиту от различных угроз, чем фильтр uBlock со списком Malware Domains. Однако это требует покупки лицензии, и тогда антивирус будет отсылать через анонимный канал идентифицирующие данные. В реальности, скорее всего, пользователь будет периодически искать пробные ключи в Интернете либо выберет бесплатный антивирус. С другой стороны, архитектура системы такова, что рабочая виртуальная машина в принципе не имеет доступа к реальному IP и файловой системе физической машины. Кроме того, наличие заранее сделанного снимка состояния ВМ (snapshot) позволит сбросить её к незаражённому состоянию. Единственной, хотя и маловероятной угрозой остаётся заражение вирусом, эксплуатирующим некую уязвимость в VirtualBox, которая позволила бы вирусу «выйти» за пределы ВМ.

3.2.3. Итоговые возможности подмены данных

Цифровые отпечатки Firefox подменяются при помощи вышеупомянутых браузерных дополнений, некоторых возможностей самого Firefox, а также изменением параметров виртуальной машины. Отдельные параметры можно подменить и с помощью JavaScript, подключая пользовательские скрипты через дополнение Tampermonkey, но это срабатывает не во всех случаях. Например, разрешение экрана предпочтительнее изменять для самой ВМ через настройки VirtualBox. User-agent оставляем без изменений либо подменяем только версию

браузера. Язык браузера – английский по умолчанию, допускается установить русскую локализацию интерфейса, но при этом удалить русский из списка языков, на которых запрашиваются веб-страницы (это влияет на заголовок HTTP Accept-Language). Flash-плагин устанавливать нежелательно. Часовой пояс изменяется в системе и должен соответствовать геолокации используемого VPN-сервера (учитывая также летнее/зимнее время).

«Отпечаток шрифтов» имеет две разновидности:

- отрисовка нескольких символов Юникода в разных начертаниях и измерение размеров полученных символов;
- выявление установленных шрифтов с помощью механизма CSS Fallback, причём напрямую получить весь список шрифтов нельзя, но можно проверять наличие каждого конкретного шрифта из заранее подготовленной базы.

В первом случае отпечаток можно исказить обычным изменением масштаба страницы (это же касается и отпечатка getClientRects), но очевидно, что это не удастся делать многократно. С другой стороны, ценность данного отпечатка сравнительно невысокая. Для борьбы со вторым методом Firefox имеет встроенную функцию «белого списка» шрифтов, а также режим блокировки всех шрифтов, задаваемых веб-страницей (вместо них используется небольшой набор стандартных шрифтов браузера). Отметим, что в случае установки и запуска плагина Flash сайт сможет получить доступ ко всему списку шрифтов, установленных в системе.

Дополнение CanvasBlocker подменяет отпечаток Canvas и частично WebGL. Браузер Firefox позволяет переопределить значения строк Renderer и Vendor для API WebGL, однако в целом отпечаток WebGL остаётся наиболее сложным. Правдоподобная подмена всех параметров для WebGL 2 может быть реализована только при полноценной эмуляции видеокарты в виртуальной машине. На данный момент известен один экспериментальный проект с такой возможностью – модифицированный VirtualBox от Д. Момота (Vektor T13), но его совместимость с Whonix пока ещё плохо проверена, и сложно гарантировать

стабильность, а также имеются проблемы с цифровыми подписями драйверов. В обычном VirtualBox функциональность WebGL будет зависеть от того, включено ли 3D-ускорение графики в виртуальной машине и установлены ли «дополнения гостевой ОС». И наконец, подмена отпечатка AudioContext выполняется с помощью AudioContext Fingerprint Defender, также можно переключать частоту дискретизации в настройках динамиков.

Итоговая схема реализации имеет вид, представленный на рисунке:

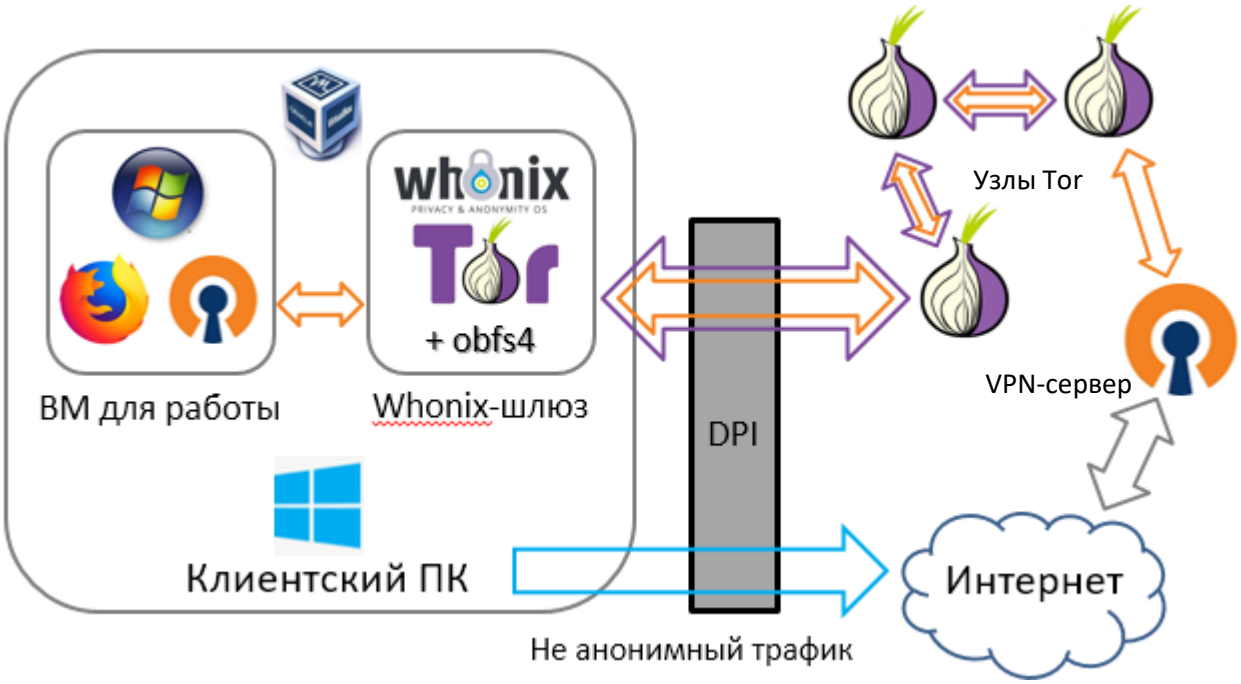

Рисунок 1 – компоненты системы

Под обозначением DPI здесь подразумевается любое оборудование анализа и записи трафика (в том числе, системы СОРМ-3), установленное у интернет-провайдера. Схема не исключает возможности одновременного посещения какого-либо сайта из виртуальной машины и из основной системы, но даже в этом случае со стороны сайта было бы очень сложно распознать, что посетитель один и тот же. Заметим, что при данной схеме нет необходимости маскировать трафик OpenVPN, поскольку он находится «внутри» канала Tor с обфускацией. В то же время VPN обеспечит защиту трафика от возможного прослушивания на выходных узлах сети Tor.

4 Запуск и тестирование

4.1. Настройка сервера

4.1.1. Предварительный этап

VPS (Virtual Private Server) – услуга, в рамках которой пользователю предоставляется так называемый «виртуальный выделенный сервер». В плане управления операционной системой она по большей части соответствует физическому выделенному серверу. В частности, имеется root-доступ, собственные IP-адреса, порты, правила фильтрования и таблицы маршрутизации. Владелец VPS может удалять, добавлять, изменять любые файлы, включая файлы в корневой и других служебных директориях, а также устанавливать собственные приложения или настраивать/изменять любое доступное ему прикладное программное обеспечение [48]. Тип виртуализации сервера может быть любым, однако Xen и KVM (полная виртуализация) считаются более надёжными и удобными, чем OpenVZ (общее ядро ОС).

Соответственно, мы будем использовать VPS, чтобы установить и настроить на нём VPN-сервер. Трафик между пользователем и VPN-сервером надёжно зашифрован и тем самым защищён от прослушивания. Между сервером и конечным ресурсом трафик не шифруется средствами VPN, но может быть зашифрован протоколом TLS, если посещаемый сайт работает по безопасному соединению HTTPS. Из этого следует важное замечание: сервер, на котором размещается VPS, всё же способен отслеживать историю подключений к внешним ресурсам, и даже прослушивать трафик незащищённых соединений.

Для тестового запуска VPN в рамках данной работы (и для личного использования в дальнейшем) был арендован недорогой виртуальный сервер у VPS-провайдера HostSailor. Операционная система – Debian 9 x64, гипервизор – Xen, сервер расположен в Нидерландах. Для удалённого доступа к серверу по протоколу SSH использовался клиент PuTTY, а также программа WinSCP для удобной работы с файлами на сервере.

Прежде чем приступать собственно к установке VPN, следует обезопасить сервер от возможного несанкционированного доступа. Авторизация

по паролю – не самый безопасный метод для SSH, поэтому прежде всего был настроен вход по сертификату Ed25519, а парольная авторизация отключена. Ed25519 – это схема сигнатур эллиптической кривой, которая обеспечивает лучшую защиту, чем ECDSA и RSA, и хорошую производительность ввиду небольшой длины ключа. В программа PuTTYgen генерируется пара ключей и задаётся пароль для закрытого ключа, затем публичный ключ копируется на сервер и добавляется в список авторизованных ключей.

4.1.2. Установка и настройка OpenVPN и Easy-RSA

Убедимся, что поддержка TUN/TAP на VPS включена, для этого в консоли введём команду cat /dev/net/tun. Вывод «File descriptor in bad state» является нормальным. Если же получим «No such file or directory», то адаптер TUN/TAP не включен [38]. В зависимости от провайдера, потребуется включить эту функцию через панель управления сервером на сайте, либо сделать запрос к техподдержке. На Xen VPS у Hostsailor адаптер был включен изначально.

Для установки пакета OpenVPN в Debian выполняем команды:

```
apt update
apt install openvpn
```

Создадим папку для ключей и перейдём в неё:

```
mkdir /etc/openvpn/keys
cd /etc/openvpn/keys
```

Все операции по созданию ключей и сертификатов можно выполнить с помощью утилиты openssl, но проще воспользоваться специально созданной для этого программой Easy-RSA, которая использует openssl для выполнения действий с ключами и сертификатами. Ранее Easy-RSA поставлялась вместе с OpenVPN, но теперь это отдельный проект. Скачиваем её, извлекаем и создаём 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
```

Теперь в WinSCP также заходим в папку /etc/openvpn/keys/easy-rsa-master/easyrsa3 и в ней открываем файл vars. Находим следующие строки:

```
#set_var EASYRSA_REQ_COUNTRY    «US»
#set_var EASYRSA_REQ_PROVINCE   «California»
#set_var EASYRSA_REQ_CITY       «San Francisco»
#set_var EASYRSA_REQ_ORG        «Copyleft Certificate Co»
#set_var EASYRSA_REQ_EMAIL      «me@example.net»
#set_var EASYRSA_REQ_OU         «My Organizational Unit»
```

Это параметры, наличие которых обязательно для генерации ключа. Значения в кавычках можно заменить на любые по своему усмотрению, они в данном случае ни на что не влияют. Затем эти строки необходимо раскомментировать (убрать символ # в начале строк). Также раскомментируем параметры, задающие длину ключа:

```
#set_var EASYRSA_KEY_SIZE    2048
#set_var EASYRSA_DIGEST    «sha256»
```

Чтобы повысить стойкость шифрования RSA, увеличим длину ключей до наибольшей – заменим 2048 на 4096, а sha256 на sha512. Однако, вместо RSA можно использовать более современную криптографию на эллиптических кривых [49], что даст экспоненциальное возрастание криптостойкости при меньшей длине ключа. Например, популярным сегодня ключам RSA с длиной 1024-2048 бит соответствует всего лишь 160-224 битный ключ ECC. Кроме высокой надёжности шифрования, это повышает производительность. Также в этом случае не требуется генерировать файл ключа Диффи-Хеллмана. Выбор между RSA и эллиптическими кривыми необходимо сделать до начала работы с EasyRSA для создания ключей. В файле конфигурации vars нам потребуется указать следующие параметры:

```
set_var EASYRSA_ALGO     ec
set_var EASYRSA_CURVE    secp521r1
```

Список поддерживаемых кривых достаточно обширен, и среди них сложно выбрать наиболее надёжную. В 2013 году отдельные высказывания представителей АНБ вызвали опасения, что некоторые, а возможно, и все виды

криптографии на основе эллиптических кривых, используемые органами по стандартизации в США, были намеренно ослаблены, чтобы упростить для АНБ задачу их взлома. Доказательств, что это возможно для кривых, используемых для подписания и обмена ключами, не существует, и некоторые специалисты считают это маловероятным. В ходе работы первоначально была выбрана менее распространённая кривая secp256k1, которую, в частности, использует система Bitcoin и которая была сгенерирована канадской компанией Certicom, а не Национальным институтом стандартов и технологии США (как другие кривые). Предполагается, что данная кривая предоставляет меньше возможностей скрыть «бэкдор» [50]. К сожалению, начиная с версии 2.4.5 OpenVPN не работает с этой кривой (точнее, она не поддерживается обновлённой библиотекой OpenSSL 1.1), поэтому пришлось остановиться на secp521r1.

4.1.3. Генерирование сертификатов

Нам необходимо создать так называемую PKI – инфраструктуру публичных ключей. 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;
6. (Опционально) Создать список отзыва сертификатов;
7. (Усиление безопасности) Создать ключ аутентификации TLS.

Выполняем команду инициализации:

```
./easyrsa init-pki
```

Итак, создадим свой удостоверяющий центр (CA). На самом деле, из соображений безопасности, это следовало бы делать на другом компьютере, изолированном от сети, чтобы исключить возможность компрометации ключа [51]. Сейчас, для упрощения процедуры, мы создаём CA на нашем VPN-сервере, для этого достаточно ввести команду:

```
./easyrsa build-ca
```

Как и при генерации ключей SSH, здесь потребуется защитить ключ надёжным паролем. Также будет запрошено «Common Name», можно просто нажать Enter. Получаем файлы: ca.crt (корневой сертификат, открытый, будет передаваться клиентам) и ca.key (закрытый ключ, который не должен быть скомпрометирован).

Теперь создадим 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. Создаём запрос на сертификат:

```
./easyrsa gen-req server nopass
```

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

```
./easyrsa sign-req server server
```

Подтверждаем операцию и вводим пароль закрытого ключа УЦ. Получим подписанный открытый ключ сервера – server.crt. Полный путь к нему получится таким: /etc/openvpn/keys/easyrsa3/pki/issued/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. Процесс займёт некоторое время:

```
./easyrsa gen-dh
```

На выходе получаем файл dh.pem. В данном же случае был выбран алгоритм эллиптической криптографии, который не требует создания этого файла. Также можно создать список отозванных сертификатов на случай утери какого-либо устройства с OpenVPN-клиентом. Процедура отзыва сделает утерянный ключ недействительным. Сейчас просто создаём сам список:

```
./easyrsa gen-crl
```

Наконец, скопируем ключи в папку OpenVPN и перейдём в эту папку:

```
cp pki/ca.crt /etc/openvpn/
cp pki/dh.pem /etc/openvpn/
cp pki/crl.pem /etc/openvpn/
cp pki/issued/server.crt /etc/openvpn/
cp pki/private/server.key /etc/openvpn/
cd /etc/openvpn
```

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. Однако современные версии OpenVPN имеют более совершенный механизм защиты, активируемый опцией tls-crypt. Это включает в себя не только функционал tls-auth, но и шифрование всех пакетов управляющего канала, что затрудняет опознавание трафика OpenVPN. Ключ используется такой же, поэтому настройка сводится к замене директивы tls-auth на tls-crypt в файлах конфигурации.

Теперь с помощью WinSCP изменим права доступа у файлов: ca.crt, crl.pem, dh.pem, server.crt – выставляем для всех 0644. На файлах server.key и ta.key должны быть права 0600. 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
```

Параметр nopass применяется по усмотрению пользователя. Если защитить ключ паролем, это повысит безопасность, но придётся вводить пароль при каждом подключении к VPN. В данном же случае для подключения достаточно иметь закрытый ключ. Имя client_name – произвольное, например, home_pc. 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 Б**.

4.1.4. Дополнительная настройка и запуск сервера

Поскольку сервер служит одновременно и DNS-резолвером, требуется установить DNSMasq (команда apt install dnsmasq). В файл конфигурации /etc/ dnsmasq.conf добавляем строки:

```
server=185.208.208.141
server=146.185.176.36
interface=tun0
```

В данном случае здесь указаны адреса использованных DNS от OpenNIC, а также сетевой интерфейс TUN, запросы с которого будет обрабатывать DNSmasq. В системном файле /etc/resolv.conf следует также указать аналогичные адреса DNS и удалить оттуда адреса Google DNS, если они по умолчанию присутствовали.

Для перенаправления трафика из сети VPN во внешний интернет обычно используется механизмы NAT и IP forwarding. В файл /etc/sysctl.conf добавляем (или раскомментируем уже имеющиеся) строки:

```
net.ipv4.ip_forward = 1
net.ipv6.conf.all.forwarding=1
```

Для применения настроек выполняем команду sysctl -p /etc/sysctl.conf. Теперь добавляем правила файрвола iptables:

```
iptables -t nat -A POSTROUTING -s 10.8.0.0/24 -j SNAT --to-source 185.141.27.70
iptables -A INPUT -i eth0 -p icmp -j DROP
```

Здесь 10.8.0.0/24 – подсеть, используемая для VPN, а 185.141.27.70 – публичный статический адрес данного VPS. Второе правило блокирует ICMP из внешней сети, как уже упоминалось – это мера борьбы с распознаванием туннеля.

Перезапуск DNSMasq, запуск и проверка работоспособности OpenVPN:

```
systemctl restart dnsmasq
systemctl start openvpn@server
systemctl status openvpn@server
```

Этап настройки VPN-сервера завершён, но для подключения к VPN требуется создать файл конфигурации клиента.

4.2. Настройка рабочего места

На клиентский ПК устанавливается VirtualBox, образы двух виртуальных машин Whonix скачиваются с официального сайта и импортируются в VirtualBox. В описываемой схеме используется только Whonix-Gateway, но целесообразно скачать и Whonix-Workstation для тех случаев, когда более важна повышенная защищённость, чем удобство и незаметность. Создаётся ещё одна виртуальная машина, в которой устанавливается Windows 7 (предпочтительный вариант – заранее создать образ ВМ с установленной системой и остальным ПО,

а затем импортировать его у клиента сразу в готовом виде). Применяется программа Destroy Windows Spying для удаления средств сбора телеметрии. В настройках виртуальной машины указывается внутренняя сеть Whonix. Также рекомендуется выставить число ядер процессора более одного, этот параметр доступен через браузер (свойство navigator.hardwareConcurrency), а одно ядро слишком явно указывает на наличие ВМ. В сетевых настройках самой системы следует задать параметры для подключения к Whonix-Gateway:

IP-адрес – 10.152.152.50
Маска подсети – 255.255.192.0
Шлюз – 10.152.152.10
DNS – 10.152.152.10

На Whonix-Gateway редактируется файл настроек Tor для включения obfs4 и запрета использования российских узлов. Содержимое файла:

```
DisableNetwork 0
UseBridges 1
ClientTransportPlugin obfs2, obfs3, obfs4 exec /usr/bin/obfs4proxy
bridge obfs4 <адрес моста> # 2–3 адреса, каждый в отдельной строке
ExcludeNodes {ru}, {??} # ?? – узлы с неизвестной геолокацией
```

В ходе тестирования были использованы следующие адреса мостов (на момент написания они остаются актуальными):

```
bridge obfs4 194.135.88.138:443 9F0BC3AA3CC72F17DC7789D7ABC7A763038F82CB
cert=lINVQVt8EQS5q9DWz3S+RHLosgiRVXueHlMfY3qtas1qHhGXvg7MOu6jECDZ0mbrS7tQLA iat-mode=0
bridge obfs4 185.79.93.126:59815 1594A9B832D4E0BD946A5988B364F1687814EC5D
cert=3DlWyDr4IwpZlxQbDX+7obB/EZr+eQavtnFbqaQsLym01MgIIsXPIl5E3ftp4ILYK/G+OQ iat-mode=0
bridge obfs4 144.76.182.167:43981 77644CB35D66304974B84855A580155053365935
cert=yI120MhitxPLUcJFhDgspTy+sHOm4VlSAXLegRjYsu9qEd2yR59YNq3tvDnkRiGY/+rQFQ iat-mode=0
```

В систему устанавливается OpenVPN-клиент и браузер Firefox. Файл конфигурации для клиента приведён в **приложении В** (некоторые параметры OpenVPN для сервера и клиента позаимствованы у сервиса RootVPN). При отключенном VPN весь трафик идёт через Tor, что позволяет посещать onion-сайты в Firefox (сначала необходимо в about:config отключить параметр network.dns.blockDotOnion). Важное замечание: не следует устанавливать Tor Browser в данной машине, так как это приведёт к цепочке «Tor через Tor» –

встроенный Tor-клиент браузера будет работать через Tor-шлюз. Это не только снижает быстродействие, но и потенциально небезопасно из-за возможного появления самопересекающегося маршрута и сокращению эффективной длины цепочки до одного-двух узлов. Если необходимо использовать Tor Browser, можно запустить его в основной системе либо внутри Whonix-Workstation.

В Firefox устанавливается набор дополнений, упомянутых в разделе 3, и применяются необходимые настройки. Полный список возможных параметров конфигурации достаточно обширен и не имеет единственного правильного варианта. «Белый список шрифтов» применяется следующим образом: на одном из сайтов (например, BrowserLeaks) выявляем список шрифтов, опознаваемых в текущей конфигурации. Создаём строковый параметр font.system.whitelist на странице about:config в Firefox. Содержимое параметра заполняем полученным списком шрифтов. Теперь «отпечаток шрифтов» будет изменяться при удалении некоторых шрифтов из списка. Отметим, что разные сайты проверяют наличие разного набора шрифтов, поэтому удаление (или добавление в систему) некого шрифта не гарантирует изменение полученного списка на конкретном сайте. Параметр WebGL Renderer под VirtualBox содержит слова Software Adapter, это выдаёт наличие виртуализации, поэтому требуется подменить строку значением, взятым с какого-либо реального ПК. Пример:

webgl.renderer-string-override = ANGLE (Intel(R) HD Graphics 620 Direct3D11 vs_5_0 ps_5_0)

Подмену User-agent удобно выполнять с помощью User-agent Switcher, однако несоответствие ОС или движка браузера может быть обнаружено по косвенным признакам, поэтому желательно подменять только версию браузера. У дополнения CanvasBlocker рекомендуется выбрать режим «fake at input», так как он более сложен для обнаружения. Системные часы следует периодически синхронизировать. Кроме того, в Firefox 60 точность таймера снижена до 2 мс по умолчанию и до 100 мс в режиме ResistFingerprinting.

Очистка данных (cookies, Local Storage и др.) происходит при перезапуске Firefox, а также при использовании функции «Забыть» или ручном удалении

данных для конкретного сайта (в Firefox 63 разработчики планируют упростить эту процедуру). Кроме того, дополнение Firefox Multi-Account Containers позволяет открыть один и тот же сайт в нескольких изолированных вкладках, каждая из которых не имеет доступа к данным других вкладок.

4.3. Тестирование полученной сборки

4.3.1. Проверяемые факторы и используемые веб-сайты

Необходимо убедиться, что подмена всех цифровых отпечатков надёжно работает, а посещаемые сайты не распознают наличие средств анонимизации. В виртуальной машине с Windows было выполнено подключение к настроенному VPN через Whonix-Gateway, использован Firefox 60 (последняя стабильная версия на момент тестирования). При работе не было замечено проблем с подключением OpenVPN по протоколу TCP через цепочку Tor и obfs4. Часовой пояс в системе был изменён до запуска браузера.

Для проверки VPN на предмет «необнаружимости» использовались следующие интернет-ресурсы:

https://2ip.ru/privacy – определяет наличие VPN или прокси-сервера по характерным особенностям. Следует отметить, что при полном отсутствии средств анонимизации данный сайт также выдаст «хороший» результат.

https://whoer.net — также проверяет признаки наличия анонимайзера, но некоторые параметры отличаются от 2ip.ru: отличие языка браузера, неполная подмена User-agent, присутствие IP в «чёрных списках». Дополнительно отображает различные данные о браузере и выводит некоторые рекомендации по повышению безопасности.

http://witch.valdikss.org.ru/ — определяет операционную систему по специфическим особенностям TCP и сопоставляет с User-agent браузера. Проверяет значение MTU для обнаружения OpenVPN.

https://www.perfect-privacy.com/dns-leaktest/ — наиболее надёжный сервис для определения используемых DNS-серверов, позволяет проверить отсутствие утечек (желательно повторить тест несколько раз).

Основные сайты для определения цифровых отпечатков:

https://browserleaks.com/ — позволяет получить отпечатки Canvas, WebGL 2.0, шрифтов (Font fingerprinting), прямоугольных блоков (метод getClientRects), показывает различную информацию, доступную через JavaScript, проверяет функции WebRTC. Определяет степень «уникальности» отпечатка Canvas и его соответствие известным браузерам.

https://audiofingerprint.openwpm.com/ — отпечаток AudioContext API.

https://browserprint.info — комплексный отпечаток по ряду параметров, включая шрифты, Canvas, AudioContext, размер экрана и другие.

https://panopticlick.eff.org/ — один из первых сайтов, демонстрировавших технологию цифрового отпечатка браузера, имеет сходство с BrowserPrint, но набор параметров немного меньше.

4.3.2. Данные об основной системе без анонимизации

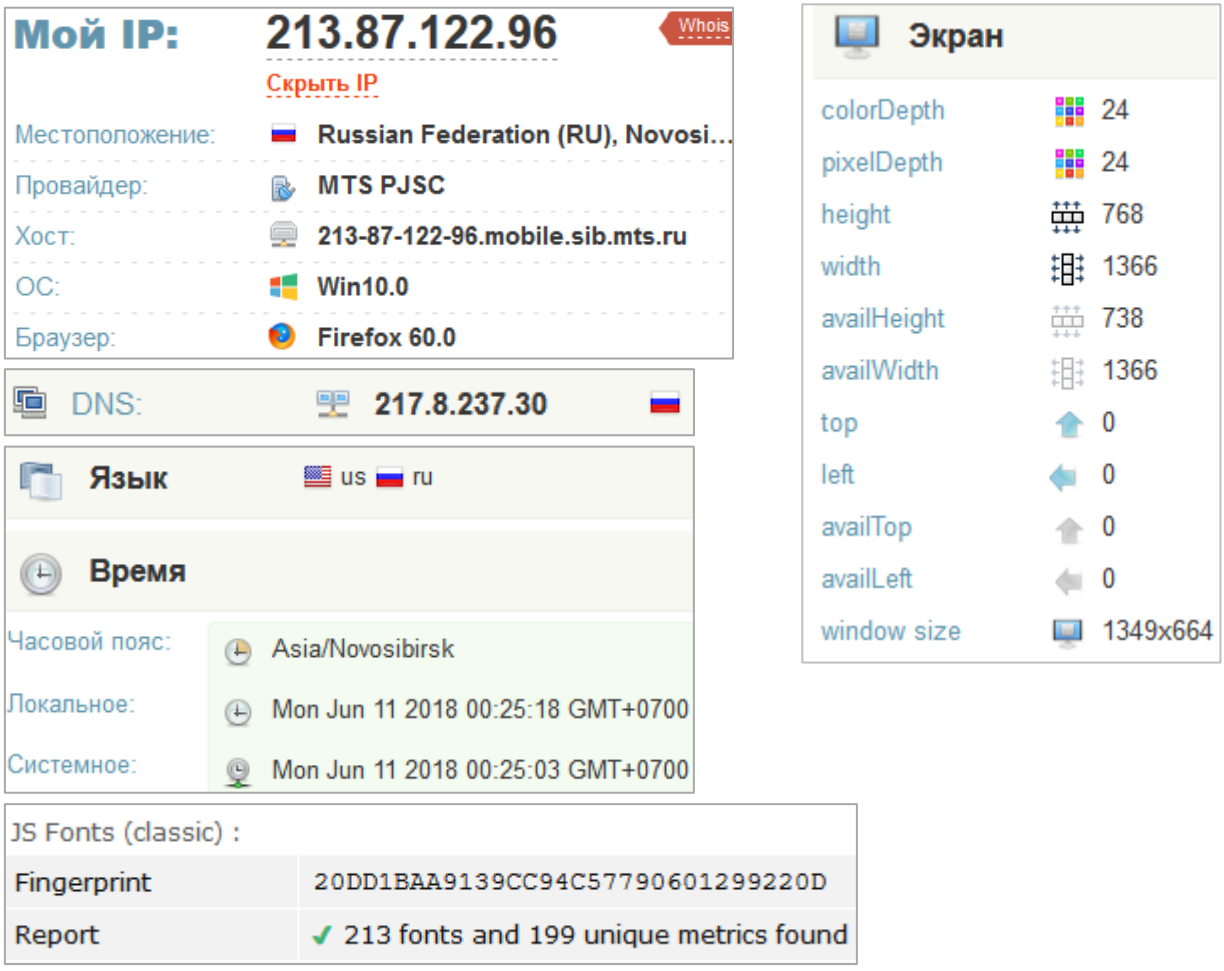

Рисунок 2 – информация из браузера, установленного на ПК

Цифровые отпечатки Canvas, WebGL, AudioContext из основной системы не имеют значения, так как в виртуальной машине они будут другими даже без применения дополнительных средств для их подмены. Задача – удостовериться в наличии возможности менять их многократно.

Проверки на обнаружение средств анонимизации показали практически идеальные результаты, однако следует понимать, что некоторые сайты могут использовать более полные базы IP-адресов хостингов и VPN-провайдеров.

Метод проверки	Результат
Заголовки HTTP proxy	нет
Открытые порты HTTP proxy	нет
Открытые порты web proxy	нет
Открытые порты VPN	нет
Подозрительное название хоста	нет
Разница во временных зонах (браузера и IP)	IP: 2018-05-29 07:56 (Europe/Amsterdam) браузер: 2018-05-29 7:56
Принадлежность IP к сети Tor	нет
Режим браузера Turbo	нет
Принадлежность IP хостинг провайдеру	нет
Определение web proxy (JS метод)	нет
Утечка IP через Flash	нет
Определение туннеля (двусторонний пинг)	высокая анонимизация (не можем проверить)
Утечка DNS	нет данных об используемых DNS
VPN fingerprint	нет
Утечка IP через WebRTC	нет

Рисунок 2 – проверка на сайте 2ip.ru

Важно отметить, что данный ресурс не смог определить DNS-адреса и факт принадлежности IP к хостинг-провайдеру HostSailor. Это является недостатком сайта, а не достоинством VPN-сервера. Так, например, сайт ipqualityscore.com

опознал IP-адрес как принадлежащий HostSailor и соответственно присвоил ему статус «подозрительного». Вероятность такого распознавания существует при использовании практически любых VPN-сервисов и VPS-хостингов, однако она существенно ниже, чем для адресов сети Tor.

Для наглядного сравнения приведём результат данной проверки для VPN-провайдера ProtonVPN (в режиме бесплатного доступа):

Метод проверки	Результат	
Заголовки HTTP proxy	нет	👍
Открытые порты HTTP proxy	нет	👍
Открытые порты web proxy	нет	👍
Открытые порты VPN	500/udp, IPSec	👎
Подозрительное название хоста	нет	👍
Разница во временных зонах (браузера и IP)	IP: 2018-04-10 10:17 (Asia/Tokyo) браузер: 2018-04-10 8:17	👎
Принадлежность IP к сети Tor	нет	👍
Режим браузера Turbo	нет	👍
Принадлежность IP хостинг провайдеру	нет	👍
Определение web proxy (JS метод)	нет	👍
Утечка IP через Flash	нет	👍
Определение туннеля (двусторонний пинг)	обнаружен	👎
Утечка DNS	нет данных об используемых DNS	👍
VPN fingerprint	MTU 1365	👎
Утечка IP через WebRTC	нет	👍

Рисунок 3 – пример неудовлетворительного результата

Очевидно, что здесь не был выставлен соответствующий часовой пояс, однако остальные три параметра зависят именно от настроек сервера.

Тестирование на сайте Whoer показало, что утечка реального IP через WebRTC не происходит, но есть утечка внутрисетевого адреса (10.8.0.2), которая

косвенно указывает на наличие VPN. После включения в uBlock соответствующей опции (Prevent WebRTC from leaking local IP addresses) данная утечка блокируется. Альтернативный способ: установить параметр media.peerconnection.ice.proxy_only = true в конфигурации Firefox. Результат аналогичен действию uBlock. После этого данный сайт не выявляет никаких признаков использования анонимайзера:

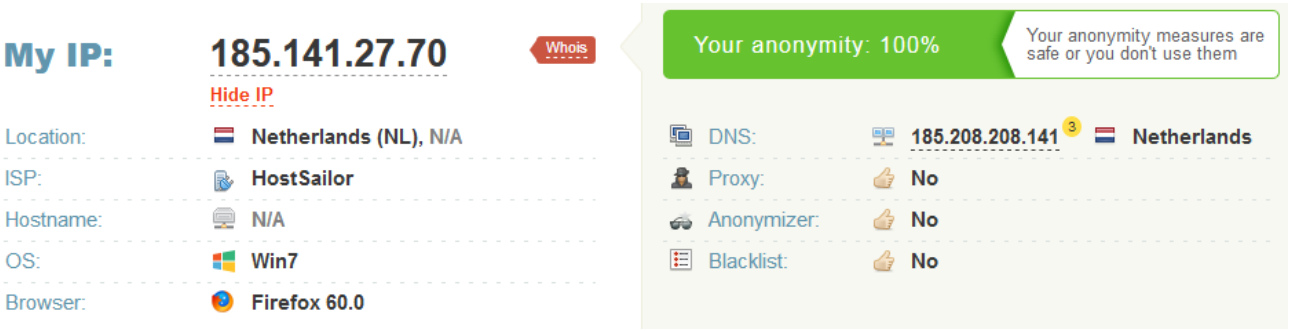

Рисунок 4 – тест на сайте Whoer.net

Проверка MTU показывает нейтральное значение 1500 и, соответственно, не обнаруживает присутствия VPN:

```
First seen     = 2018/06/05 14:54:39
Last update    = 2018/06/05 14:57:15
Total flows    = 6
Detected OS    = Windows 7 or 8
HTTP software  = Firefox 10.x or newer (ID seems legit)
MTU            = 1500
Network link   = Ethernet or modem
Language       = English
Distance       = 7

PTR test       = Probably home user
Fingerprint and OS match. No proxy detected (this test
No OpenVPN detected.
```

Рисунок 5 – ответ сайта witch.valdikss.org.ru

Утечек посторонних адресов DNS обнаружено не было, определяются только те адреса, которые используются сервером и относятся к Нидерландам.

IP	HOSTNAME	ISP	COUNTRY
146.185.176.36		RIPE-ERX-146-185-0-0	NL
82.196.9.45		Digital Ocean, Inc.	NL
185.208.208.141		Hostio Solutions B.V.	NL

Рисунок 6 – проверка адресов DNS

Один из вариантов цифрового отпечатка браузера приведён ниже.

Browser Characteristic	bits of identifying information	one in x browsers have this value	value
Limited supercookie test	0.39	1.31	DOM localStorage: Yes, DOM sessionStorage: Yes, IE userData: No
Hash of canvas fingerprint	20.65	1645312.0	c2c4645b2004347687b0ee050fafbbcc
Screen Size and Color Depth	17.48	182812.44	1280x680x24
Browser Plugin Details	1.23	2.35	undefined
Time Zone	2.56	5.91	-120
DNT Header Enabled?	0.78	1.72	True
HTTP_ACCEPT Headers	2.01	4.02	text/html, */*; q=0.01 gzip, deflate, br en-US,en;q=0.5
Hash of WebGL fingerprint	19.65	822656.0	593985985e588db7b927e4e70057819f
Language	0.92	1.89	en-US
System Fonts	19.65	822656.0	Arial, Arial Black, Calibri, Cambria, Cambria Math, Comic Sans MS, Consolas, Courier, Courier New, Georgia, Helvetica, Impact, Lucida Console, Lucida Sans Unicode, Microsoft Sans Serif, MS Gothic, MS PGothic, MS Sans Serif, MS Serif, Palatino Linotype, Segoe Print, Segoe Script, Segoe UI, Segoe UI Light, Segoe UI Semibold, Tahoma, Times, Times New Roman, Trebuchet MS, Verdana, Wingdings 2, Wingdings 3 (via javascript)
Platform	3.04	8.24	Win64
User Agent	8.13	279.39	Mozilla/5.0 (Windows NT 6.1; Win64; x64; rv:60.0) Gecko/20100101 Firefox/60.0
Touch Support	0.59	1.51	Max touchpoints: 0; TouchEvent supported: false; onTouchStart supported: false
Are Cookies Enabled?	0.22	1.16	Yes

Рисунок 7 – цифровой отпечаток браузера с Panopticlick.eff.org

Отпечаток Canvas на сайте BrowserLeaks имеет следующий формат:

Signature	✓ E2BAD04C
Uniqueness	100% (0 of 258561 user agents have the same signature)
Image File Details :	BrowserLeaks.com <canvas> 1.0
File Size	3849 bytes
Number of Colors	259
PNG Hash	C93AB3EAB4750C3D6523AE4EF07DA53E

Рисунок 8 – случайный Canvas Fingerprint с CanvasBlocker

Сравним это с оригинальным отпечатком и с подменой через встроенную функцию Firefox ResistFingerprinting:

1)

Signature	✓ B305455D
Uniqueness	99.97% (88 of 258561 user agents have the same signature)

2)

Signature	✓ 5BEB984A
Uniqueness	100% (0 of 258561 user agents have the same signature)

3)

Signature	✓ A4E1854E
Uniqueness	× False (Tor Browser signature)

Рисунок 9 – отпечатки HTML5 Canvas

1 – Отпечаток без использования подмены

2 – Случайный отпечаток при включенном CanvasBlocker

3 – Статическая подмена с опцией ResistFingerprinting

Данный сайт не обнаруживает присутствия CanvasBlocker в режиме «fake at input», как и других подозрительных признаков, кроме uBlock:

Network Filters Detection :	
HTTP Proxy	✓ not detected
Tor Browser Detection :	
TOR Relay IP	✓ not detected
Tor Browser Ports	✓ not detected
HTML5 Canvas Protection	✓ not detected
WebGL Blocking (NoScript)	✓ not detected
CSS Fonts Protection	✓ not detected
Adblock Detection :	
AB Type	! Adblock for Mozilla Firefox

Рисунок 9 – проверка на сайте BrowserLeaks

Аналогично рассмотрим отпечатки WebGL. Замечено, что в виртуальной машине доступна только ограниченная функциональность WebGL 1.0, несмотря на включенное 3D-ускорение графики в настройках данной ВМ.

Debug Renderer Info :	
Unmasked Vendor	! Google Inc.
Unmasked Renderer	! ANGLE (Software Adapter Direct3D11 vs_5_0 ps_5_0)
WebGL Fingerprint :	
WebGL Report Hash	C6FCC26C0E17D793BC09415795D74264
WebGL Image Hash	42F3ECF80B0132497576DC52941323D9

Рисунок 10 – исходный отпечаток WebGL в VirtualBox

Debug Renderer Info :

Unmasked Vendor	! Google Inc.
Unmasked Renderer	! ANGLE (Intel(R) HD Graphics 620 Direct3D11 vs_5_0 ps_5_0)

WebGL Fingerprint :

WebGL Report Hash	D77B1800B2862B40C1B1DF5E71F4E53F
WebGL Image Hash	550CE9AC46F5293812F64F779CDE4ED2

Рисунок 11 – отпечаток после подмены

Теперь установим параметр webgl.enable-debug-renderer-info=false :

Debug Renderer Info :

Unmasked Vendor	n/a
Unmasked Renderer	n/a

WebGL Fingerprint :

WebGL Report Hash	FD2F31E5AC14E11D570EB122A99F666E
WebGL Image Hash	F429E49DA8C387231B91D42248DA37BE

Рисунок 12 – подмена отпечатка и сокрытие данных

CanvasBlocker влияет только на значение Image Hash, изменяя его случайным образом. Report Hash зависит от содержимого строк Vendor и Renderer, которые переопределяются через параметры Firefox (webgl.renderer-string-override).

Отпечатки шрифтов:

JS Fonts (unicode) :

Fingerprint	31C1E5E1
Report	✓ Unicode Glyphs Measurement

JS Fonts (classic) :

Fingerprint	18030F5F86EF0D63BD0529C03796C538
Report	✓ 129 fonts and 118 unique metrics found

Рисунок 13 – отпечаток шрифтов до подмены

JS Fonts (unicode) :

Fingerprint	3C86EEB5
Report	✓ Unicode Glyphs Measurement

JS Fonts (classic) :

Fingerprint	D796B6DDCAAA2DFA3B6AA14B3B83D220
Report	✓ 111 fonts and 101 unique metrics found

Рисунок 14 – отпечаток шрифтов после подмены

Примеры Audio Fingerprint были получены на сайте vektort13.pro ввиду более компактного представления, чем на openwpm.com.

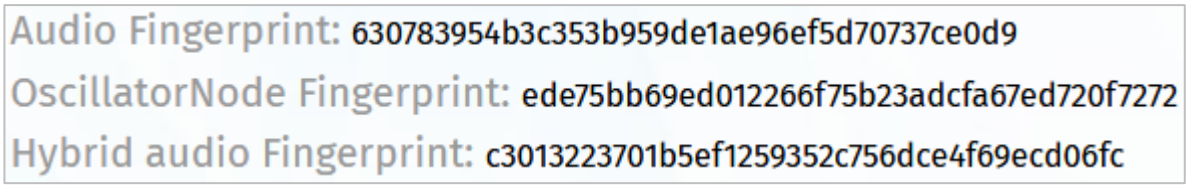

Рисунок 15 – исходные отпечатки AudioContext

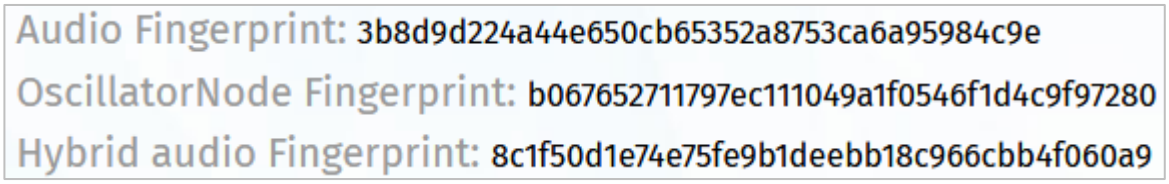

Рисунок 16 – случайные отпечатки AudioContext

В ходе тестирования была подтверждена возможность смены цифровых отпечатков неограниченное число раз (Canvas, WebGl Image, Audio Fingerprint) или, как минимум, неоднократной подмены (шрифты, User-agent, разрешение экрана, WebGL Render, ClientRects и др).

Вывод: предложенная конфигурация ПО обеспечивает эффективное противодействие различным современным методам отслеживания, надёжную изоляцию анонимного браузера от не-анонимной системы, защиту от раскрытия реальных данных о системе, не нарушая при этом функциональность браузера. Успешно проверена также правильность настройки OpenVPN в отношении его маскировки. В то же время необходимо учитывать, что подключение VPN через Tor является менее надёжным с точки зрения анонимности, чем использование только Tor, равно как и ОС Windows обычно не рекомендуется для анонимной работы, в отличие от специальных Linux-дистрибутивов.

ЗАДАНИЕ ДЛЯ РАЗДЕЛА
«ФИНАНСОВЫЙ МЕНЕДЖМЕНТ, РЕСУРСОЭФФЕКТИВНОСТЬ И РЕСУРСОСБЕРЕЖЕНИЕ»

Студенту:

Группа	**ФИО**
8ВМ6Б	Айду Михаилу Александровичу

Школа	ИШИТР	**Отделение**	ОИТ
Уровень образования	Магистратура	**Направление/специальность**	09.04.01 «Информатика и вычислительная техника»

Исходные данные к разделу «Финансовый менеджмент, ресурсоэффективность и ресурсосбережение»	
1. Стоимость ресурсов научного исследования (НИ): материально-технических, энергетических, финансовых, информационных и человеческих	Оклады участников проекта, нормы рабочего времени, ставки налоговых отчислений во внебюджетные фонды, районный коэффициент по г. Томску.
2. Нормы и нормативы расходования ресурсов	
3. Используемая система налогообложения, ставки налогов, отчислений, дисконтирования и кредитования	
Перечень вопросов, подлежащих исследованию, проектированию и разработке	
1. Оценка коммерческого и инновационного потенциала НТИ	Анализ потенциальных потребителей результатов работы, проработка анализа конкурентных технических разработок
2. Разработка устава научно-технического проекта	Проработка целей и результатов исследования, определение участников разработки
3. Планирование процесса управления НТИ: структура и график проведения, бюджет, риски и организация закупок	Планирование этапов работ, построение графика проведения работ, расчёт бюджета проведения работ
4. Определение ресурсной, финансовой, экономической эффективности	Оценка эффективности проекта
Перечень графического материала	
1. Оценка конкурентоспособности технических решений. *2. Матрица SWOT.* *3. Диаграмма Ганта.* *4. График проведения и бюджет НТИ.*	

Дата выдачи задания для раздела по линейному графику	

Задание выдал консультант:

Должность	**ФИО**	**Учёная степень, звание**	**Подпись**	**Дата**
Старший преподаватель ШИП	Шаповалова Наталья Владимировна.	-		

Задание принял к исполнению студент:

Группа	**ФИО**	**Подпись**	**Дата**
8ВМ6Б	Айд Михаил Александрович		

5 Финансовый менеджмент, ресурсоэффективность и ресурсосбережение

5.1. Предпроектный анализ

5.1.1. Потенциальные потребители результатов исследования

Для анализа потребителей результатов необходимо рассмотреть целевой рынок и провести его сегментирование.

Результатом выполнения магистерской диссертации является программный комплекс, служащий относительно удобным и эффективным инструментом для обеспечения анонимности и защиты от отслеживания при работе в интернете.

Целевым рынком, на котором будет реализовываться в будущем разработка, является широкий круг пользователей в различных областях деятельности, так или иначе заинтересованных в сохранении приватности или анонимности при посещении веб-сайтов. Потенциальными потребителями являются в первую очередь частные лица – обычные пользователи, по каким-либо причинам желающие пользоваться интернет-ресурсами анонимно, при этом не испытывая значительных неудобств, или просто стремящиеся к защите неприкосновенности частной жизни. В перспективе, подобную систему могут использовать различные активисты, информаторы, журналисты, а также лица, занимающиеся конкурентной разведкой и другие категории пользователей, проявляющих интерес к средствам анонимизации.

5.1.2. Анализ конкурентных технических решений с позиции ресурсоэффективности и ресурсосбережения

Анализ конкурентных технических решений позволяет провести оценку сравнительной эффективности разработки и определить направления для её будущего повышения.

Данный анализ производится с помощью оценочной карты, представленной в таблице 2. Для её построения была рассмотрена конкурентная разработка – Whonix (К1).

Таблица 2 – Оценочная карта для сравнения конкурентных технических решений (разработок)

Критерии оценки	Вес критерия	Баллы		Конкуренто-способность	
		$Б_ф$	$Б_{к1}$	$К_ф$	$К_{к1}$
Технические критерии оценки ресурсоэффективности					
1. Повышение производительности труда пользователя	0,3	5	4	1,5	1,2
2. Удобство в эксплуатации	0,1	4	3	0,4	0,3
3. Функциональная помощь	0,1	5	3	0,5	0,3
4. Качество интеллектуального интерфейса	0,1	4	3	0,4	0,3
Экономические критерии оценки эффективности					
1. Конкурентоспособность продукта	0,1	4	3	0,4	0,3
2. Цена	0,1	4	3	0,4	0,3
3. Послепродажное обслуживание	0,2	5	1	1	0,2
Итого	1	31	20	4,6	2,9

Критерии для сравнения и оценки ресурсоэффективности и ресурсосбережения, приведённые в таблице 1, подбираются, исходя из выбранных объектов сравнения с учётом их технических и экономических особенностей разработки, создания и эксплуатации.

Позиция разработки и конкурентов оценивается по каждому показателю экспертным путём по пятибалльной шкале, где 1 – наиболее слабая позиция, а 5 – наиболее сильная. Веса показателей, определяемые экспертным путём, в сумме должны составлять 1.

Анализ конкурентных технических решений определяется по формуле:

$$K = \sum В_i \cdot Б_i \ , \qquad (1)$$

где К – конкурентоспособность научной разработки или конкурента;

$В_i$ – вес показателя (в долях единицы);

$Б_i$ – балл i-го показателя.

Исходя из полученных результатов, можно сделать вывод об оптимальном уровне конкурентоспособности программного продукта. Уязвимость конкурентного продукта связана со средним уровнем

функциональности, а также с невозможностью внесения дополнительного функционала после продажи продукта.

5.1.3. SWOT-анализ

SWOT – Strengths (сильные стороны), Weaknesses (слабые стороны), Opportunities (возможности) и Threats (угрозы) – представляет собой комплексный анализ научно-исследовательского проекта.

Первый этап заключается в описании сильных и слабых сторон проекта, в выявлении возможностей и угроз для реализации проекта, которые проявились или могут появиться в его внешней среде.

Второй этап состоит в выявлении соответствия сильных и слабых сторон научно-исследовательского проекта внешним условиям окружающей среды. В рамках данного этапа необходимо построить интерактивную матрицу проекта. Каждый фактор помечается либо знаком «+» (означает сильное соответствие сильных сторон возможностям), либо знаком «-» (что означает слабое соответствие); «0» – если есть сомнения в том, поставить «+» или «-». Интерактивная матрица проекта представлена в таблице 3.

В рамках третьего этапа составлена итоговая матрица SWOT-анализа, представленная в таблице 3.

Таблица 3 – Итоговая матрица SWOT-анализа

	Сильные стороны научно-исследовательского проекта: С1. Повышение производительности и эффективности работы пользователей. С2. Оптимизация различных задач.	Слабые стороны научно-исследовательского проекта: Сл1. Необходимость дополнительного обучения кадров для работы с программным продуктом. Сл2. Большой набор требований к продукту со стороны потребителей.
Возможности: В1. Появление новых сфер применения программного продукта. В2. Интерес крупных частных предприятий. В3. Повышение стоимости конкурентных разработок	Новые сферы применения увеличат финансирование разработки. Интерес предприятий поможет понять конечные требования к продукту.	Новые сферы применения технологии помогут найти область с легко выполнимыми требованиями.
Угрозы: У1. Отсутствие спроса на разрабатываемую систему у производства. У2. Появление более эффективных и удобных альтернатив.	Повышенная производительность работы пользователей, за счёт оптимизации решения различных задач могут стать важным аргументом для перехода к новой системе.	Главной угрозой является отсутствие спроса, что решается поиском новых сфер применения и демонстрацией достоинств программного продукта.

Исходя из результатов SWOT-анализа, можно сделать вывод о том, что при разработке системы большое внимание должно уделяться задаче оптимизации и повышения производительности работы, поскольку благодаря таким сильным сторонам системы обеспечивается защита от угроз, а также открываются возможности по расширению такой системы.

5.1.4. Оценка готовности проекта к коммерциализации

Для того, чтобы оценить готовность научной разработки к коммерциализации, необходимо заполнить специальную форму, содержащую показатели о степени проработанности проекта с позиции коммерциализации и компетенциям разработчика научного проекта. Оценка готовности проекта к коммерциализации приведена в таблице 4.

Таблица 4 – Бланк оценки степени готовности научного проекта к коммерциализации.

п/п	Наименование	Степень проработанности научного проекта	Уровень имеющихся знаний у разработчика
1	Определён имеющийся научно-технический задел	5	4
2	Определены перспективные направления коммерциализации научно-технического задела	3	3
3	Определены отрасли и технологии (товары, услуги) для предложения на рынке	4	3
4	Имеется команда для коммерциализации научной разработки	5	5
5	Проработан механизм реализации научного проекта	4	4
	ИТОГО БАЛЛОВ	21	19

Оценка готовности научного проекта к коммерциализации (или уровень имеющихся знаний у разработчика) определяется по формуле:

$$Б_{сум} = \sum Б_i \ , \qquad (2)$$

где $Б_{сум}$ – суммарное количество баллов по каждому направлению;

$Б_i$ – балл по i-му показателю.

Исходя из результатов таблицы 3, значение $Б_{сум}$ составило 40, что соответствует средней перспективности проекта. Анализируя показатели проработанности проекта, можно сделать вывод о том, что слабой стороной проекта является маркетинговая сторона вопроса, следовательно, для реализации проекта необходимо привлечь специалистов в сфере маркетинга, продумать вопросы финансирования со стороны предприятия.

В качестве метода для коммерциализации программного продукта был рассмотрен инжиниринг. Выбор данного метода обуславливается, поскольку данная система предполагает предоставление заказчику комплекс инженерно-технических услуг и вводом такой системы в эксплуатацию.

5.2. Инициализация проекта

5.2.1. Цели и результаты проекта

Группа процессов инициации состоит из процессов, которые выполняются для определения нового проекта или новой фазы существующего. В рамках процессов инициации определяются изначальные цели и содержание и фиксируются изначальные финансовые ресурсы. Определяются внутренние и внешние заинтересованные стороны проекта, которые будут взаимодействовать и влиять на общий результат научного проекта. Данная информация закрепляется в уставе проекта.

Ниже, в таблицах 5-6 представлены необходимые данные, которые входят в устав проекта.

Таблица 5 – Заинтересованные стороны проекта

Заинтересованные стороны проекта	Ожидания заинтересованных сторон
Отделение информационных технологий НИ ТПУ	Разработка системы для эффективной подмены идентифицирующих данных при посещении веб-сайтов, без ущерба удобству работы.

Таблица 6 – Цели и результат проекта

Цели проекта:	Разработка системы обеспечения анонимности и защиты от отслеживания при работе в Интернете.
Ожидаемые результаты проекта:	• Высокий уровень безопасности, надёжное обеспечение анонимности и приватности • Оптимизация работы пользователей с программным продуктом, невысокие требования к опыту • Повышение эффективности имеющихся средств для защиты от отслеживания
Критерии приёмки результата проекта:	Разработка запланированного функционала для нормальной работы пользователей.
Требования к результату проекта:	Удобный интерфейс и функционал для пользователей продукта. Автоматизация всего процесса подмены данных.

5.2.2 Организационная структура проекта

На этапе организационной структуры работы проекта решались следующие вопросы: определить, кто будет входить в рабочую группу данного проекта, определить роль каждого участника в данном проекте, а также прописать функции, выполняемые каждым из участников и их трудозатраты в проекте. Данная информация представлена в таблице 7.

Таблица 7 – Рабочая группа проекта

№ п/п	ФИО, основное место работы, должность	Роль в проекте	Функции	Трудо-затраты, час
1	Шерстнёв Владислав Станиславович, ТПУ, отделение ИТ, доцент, к.т.н.	Руководитель	Координация деятельности проекта	246
2	Айд Михаил Александрович, ТПУ, отделение ИТ, магистрант	Исполнитель	Разработка программного продукта	810
Итого				1 056

5.2.3. Ограничения и допущения проекта

Факторы, которые могут послужить ограничением степени свободы участников команды проекта, а также параметры проекта, которые не будут реализованы в рамках данного проекта представлены в таблице 8.

Таблица 8 – Ограничения проекта

Фактор	Ограничения/допущения
Бюджет проекта	Не определён
Источник финансирования	Собственные средства
Сроки проекта	12.01.2018 – 01.06.2018
Дата утверждения плана управления проектом	12.01.2018
Дата завершения проекта	01.06.2018

5.3 Планирование управления научно-техническим проектом

5.3.1 План проекта

В рамках планирования выпускной квалификационной работы построен календарный график работы (таблица 9).

Таблица 9 – Календарный план проекта

Код работы (из ИСР)	Название		Длительность, дни	Дата начала работ	Дата окончания работ	Состав участников (ФИО ответственных исполнителей)
1	Получение задания на разработку системы		1	12.01	13.01	Руководитель, Исполнитель
2	Ознакомление с методами отслеживания и технологиями противодействия		14	14.01	28.01	Исполнитель, Руководитель
3	Проектирование автоматизированной системы		14	29.01	12.02	Исполнитель
4	Разработка автоматизированной системы		48	13.02	01.04	Исполнитель
5	Тестирование программного продукта		3	02.04	05.04	Исполнитель, Руководитель
6	Исправление и корректировка ошибок, выявленных в процессе тестирования		14	06.04	20.04	Исполнитель
7	Разработка дополнительного функционала		18	21.04	08.05	Исполнитель
8	Оформление пояснительной записки		21	09.05	29.05	Исполнитель
9	Корректировка пояснительной записки		2	30.05	01.06	Исполнитель, Руководитель
Итого:		Исполнитель	135			
		Руководитель	20			

Календарный план-график проекта с помощью диаграммы Ганта представлен в таблице 10.

Код работы (из ИСР)	Вид работ	Исполнители	$T_к$, кал, дн.	Продолжительность выполнения работ															
				янв		фев			март			апр			май			июнь		
				2	3	1	2	3	1	2	3	1	2	3	1	2	3	1		
1	Получение задания на разработку системы	Р, И	1	Р И																
2	Ознакомление с методами отслеживания и технологиями противодействия	Р, И	14		Р И															
3	Проектирование автоматизированной системы	И	14			И														
4	Разработка автоматизированной системы	И	48				И	И	И	И	И									
5	Тестирование программного продукта	Р, И	3									Р И								
6	Исправление и корректировка ошибок, выявленных в процессе тестирования	И	14										И							
7	Разработка дополнительного функционала	И	18											И	И					
8	Оформление пояснительной записки	Р, И	21													И	И			
9	Корректировка пояснительной записки	Р, И	2															Р И		

Р – Руководитель

И – Исполнитель

Календарный план-график проекта с помощью диаграммы Ганта представлен в таблице 10.

Таблица 10 – Календарный план-график проекта

Код работы (из ИСР	Вид работ	Исполнители	$T_к$, кал, дн.	Продолжительность выполнения работ														
				янв.		фев.			март			апр.			май			июн	
				2	3	1	2	3	1	2	3	1	2	3	1	2	3	1
1	Получение задания на разработку системы	Руководитель, Исполнитель	1															
2	Ознакомление с методами отслеживания и технологиями противодействия	Исполнитель, Руководитель	14															
3	Проектирование автоматизированной системы	Исполнитель	14															
4	Разработка автоматизированной системы	Исполнитель	48															
5	Тестирование программного продукта	Исполнитель, Руководитель	3															
6	Исправление и корректировка ошибок, выявленных в процессе тестирования	Исполнитель	14															
7	Разработка дополнительного функционала	Исполнитель	18															
8	Оформление пояснительной записки	Исполнитель, Руководитель	23															

- исполнитель - руководитель

5.4 Бюджет научного исследования

5.4.1 Сырье, материалы, покупные изделия и полуфабрикаты

При планировании бюджета научного исследования должно быть обеспечено полное и достоверное отражение всех видов планируемых расходов, необходимых для его выполнения.

Разработка данного программного продукта не предполагает больших затрат на приобретение специальных материалов или оборудование. Основными затратами выступает покупка канцелярских принадлежностей. Результаты по данной статье были занесены в таблицу 11.

Таблица 11 – Сырье, материалы, комплектующие изделия и покупные полуфабрикаты

Наименование	Марка, размер	Кол-во	Цена за единицу, руб.	Сумма, руб.
Бумага форматная белая для офисной техники	Paperline Gold, A4	500 листов	0,5	280
Шариковая ручка синяя	PILOT, 0,7 мм	2 шт	58	116
Всего за материалы				396
Транспортно-заготовительные расходы (3-5%)				16
Итого				412

$$С_м = 412 \text{ руб.}$$

5.4.2 Основная заработная плата

Статья включает основную заработную плату работников, непосредственно занятых выполнением проекта, (включая премии, доплаты) и дополнительную заработную плату.

$$С_{зп} = З_{осн} + З_{доп}, \quad (3)$$

$$С_{зп} = З_{осн} + З_{доп},$$

где $З_{осн}$ – основная заработная плата;

$З_{доп}$ – дополнительная заработная плата.

Основная заработная плата ($З_{осн}$) руководителя (лаборанта, инженера) от предприятия (при наличии руководителя от предприятия) рассчитывается по следующей формуле:

$$З_{осн} = З_{дн} \cdot Т_{раб}, \quad (4)$$

где $З_{осн}$ – основная заработная плата одного работника;

$Т_{раб}$ – продолжительность работ, выполняемых научно-техническим работником, раб.дн.

Среднедневная заработная плата рассчитывается по формуле:

$$З_{дп} = \frac{З_{м} \cdot М}{F_{д}}, \quad (5)$$

где $З_{м}$ – месячный должностной оклад работника, руб.;

М – количество месяцев работы без отпуска в течение года:

при отпуске в 24 раб. дня М = 11,2 месяца, 5-дневная неделя;

при отпуске в 48 раб. дней М = 10,4 месяца, 6-дневная неделя;

$F_{д}$ – действительный годовой фонд рабочего времени научно-технического персонала, раб.дн. (таблица 11).

Месячный должностной оклад работника вычисляется по формуле:

$$З_{м} = З_{б} \cdot (k_{пр} + k_{д}) \cdot k_{р}, \quad (6)$$

где $З_{б}$ – базовый оклад, руб.;

$k_{пр}$ – премиальный коэффициент:

$k_{д}$ – коэффициент доплат и надбавок;

$k_{р}$ – районный коэффициент, равный 1,3 (для Томск).

На настоящем этапе сформирована команда из ключевых специалистов во главе с руководителем, имеющим опыт реализации подобных проектов. Расчёт стоимости их услуг представлен в таблице ниже:

Таблица 12 – Баланс рабочего времени

Показатели рабочего времени	Руководитель	Магистрант
Календарное число дней	365	365

Количество нерабочих дней • выходные дни • праздничные дни	 52 14	 52 14
Потери рабочего времени • отпуск • невыходы по болезни	 48 0	 48 0
Действительный годовой фонд рабочего времени	251	251

Расчёт основной заработной платы исполнителей системы выбирается на основе системы оплаты труда в ТПУ (для руководителя). Для исполнителя (магистра) также предусматривается расчёт оплаты труда исходя из системы оплаты труда в ТПУ.

Таблица 13 – Расчёт основной заработной платы

Исполнители	$З_б$, руб.	$k_р$	$З_м$, руб.	$З_{дн}$, руб.	$Т_р$, раб.дн.	$З_{осн}$, руб.
Руководитель	33 664	1,3	43 763,2	1 813,3	20	36 265,91
Магистрант	9 489	1,3	12 335,7	550,4	135	74 306.7
Итого						110 572,61

$$З_{осн} = 110\,572{,}61 \text{ руб.}$$

5.4.3 Отчисления на социальные нужды

При начислении зарплаты работникам ежемесячно производится оплата страховых отчислений в пенсионный фонд, медицинского и социального страхования. На сегодняшний день общая ставка для всех перечисленных отчислений в России составляет 30%. В таблице 13 перечислены отчисления на каждого из работников.

Таблица 14 – Отчисления на социальные нужды

Исполнитель по категориям	Зар.плата,руб.	Страх. отчисления, руб.
Руководитель	36 265,91	10 879,77
Магистрант	74 306,7	22 292,01
Итого:	110 572,61	33 171,78

$$С_{внеоб} = 33\,171{,}78 \text{ руб.}$$

5.4.4 Оплата работ, выполняемая сторонними организациями и предприятиями

В ходе реализации проекта были использованы услуги Internet. Для оказания подобного рода услуг, был заключён договор со сторонней организацией.

Договором установлена ежемесячная плата за услуги пользования 4G-Интернетом, составляющая 800 руб./мес.

Общее количество рабочих дней равно 135 (≈ 5 мес.).

Для экспериментов был также арендован виртуальный сервер у хостинг-провайдера, плата за который составляет $4/мес. (253 руб./мес.). Он использовался 2 месяца.

Таким образом, затраты на использования услуг, которые оказываются сторонними организациями составляют:

$$С_{контр} = 800 \cdot 5 + 253 \cdot 2 = 4506 \text{ руб.}$$

5.4.5 Затраты на электроэнергию

Затраты по данной статье включают затраты на электроэнергию компьютера в процессе разработки программного продукта.

Цена электричества составляет 3,30 руб./кВт·час.

Мощность ноутбука примерно составляет 0,05 кВт.

Рабочий день составляет 6 часов. Общее количество рабочих дней равно 135.

Исходя из данных потребления электроэнергии, затраты составят:

$$С_{электр} = 3{,}30 \cdot 0{,}05 \cdot 6 \cdot 135 = 133{,}65 \text{ руб.}$$

5.4.6 Итоговый бюджет

Итоговый бюджет системы состоит из затрат на сырье, заработную плату и накладных расходов. Накладные расходы составляют 16% от предыдущих статей.

$$С_{накл} = (412 + 110\,572{,}61 + 33\,171{,}78 + 4\,506 + 133{,}65) \cdot 0{,}16 = 23\,807{,}37 \text{ руб.}$$

$$С_{проекта} = С_{м} + З_{осн} + С_{внеб} + С_{контр} + С_{электр} + С_{накл} \quad (7)$$

$$С_{проекта} = 412 + 110\,572{,}61 + 33\,171{,}78 + 4\,506 + 133{,}65 + 23\,807{,}37$$

$$С_{проекта} = 172\,603{,}41 \text{ руб.}$$

5.5 Оценка сравнительной эффективности исследования

Результат внедрения данной системы позволит заказчику повысить уровень безопасности при анонимной работе, в первую очередь, благодаря снижению влияния человеческого фактора. Разработанная система изолирует браузер в виртуальной машине, трафик которой направляется только в сеть TOR, что исключает возможность

случайных утечек реальных данных. Данная проблема является особо актуальной в процессе использования большинства популярных решений.

Главное преимущество данной системы – максимальное снижение вероятности того, что посещаемый веб-сайт распознает наличие средств анонимизации. Работая в системе Whonix, пользователи часто сталкиваются с ограничением доступа на многих ресурсах, владельцы которых считают анонимную деятельность потенциально вредоносной. Разработанная система не исключает полностью такую возможность, но вызывает подобные проблемы существенно реже, чем Tor Browser и популярные VPN-сервисы. Таким образом, удобство анонимной работы значительно повышается.

Выводы по разделу

В ходе выполнения магистерской диссертации производилась разработка программного обеспечения для противодействия отслеживанию и обеспечения анонимности пользователей Интернета. Анализ конкурентоспособности показал, что получаемый на выходе продукт обладает значимыми конкурентными преимуществами, благодаря которым обеспечивается защита от угроз, который были выделены в SWOT-анализе.

На разработку данного проекта потребовалось 1 056 ч., для подробного описания трудозатрат был представлен календарный план проекта. Итоговый бюджет проекта, исходя из расчётов всех затрат, составил около 320 тыс. руб.

В заключении стоит отметить, что в результате внедрения данной системы процесс анонимного использования веб-сайтов становится существенно проще и удобнее, благодаря уменьшению риска распознавания анонимизации, повышению эффективности борьбы с отслеживанием и снижению влияния человеческого фактора. Данные улучшения позволят снизить затраты времени на некоторые виды работ пользователей, что позволит направить сохранённое время на решение других задач.

ЗАДАНИЕ ДЛЯ РАЗДЕЛА
«СОЦИАЛЬНАЯ ОТВЕТСТВЕННОСТЬ»

Студенту:

Группа	ФИО
8ВМ6Б	Айду Михаилу Александровичу

Школа	ИШИТР	Отделение	ОИТ
Уровень образования	магистратура	Направление/специальность	09.04.01 «Информатика и вычислительная техника»

Исходные данные к разделу «Социальная ответственность»:	
1. Характеристика объекта исследования (вещество, материал, прибор, алгоритм, методика, рабочая зона) и области его применения	Рабочее место оператора ПЭВМ. Проект является комплексом программного обеспечения для безопасной и анонимной работы в Интернете, потенциально предназначен для широкого круга пользователей и различных областей деятельности.
Перечень вопросов, подлежащих исследованию, проектированию и разработке:	
1. Производственная безопасность	Вредные факторы: - Физические (микроклимат; повышенный уровень шума; недостаточная освещённость; воздействие ЭМП). - Психофизиологические (монотонность труда). Опасные факторы: - Поражение электрическим током; статическое электричество.
2. Экологическая безопасность:	Бытовые отходы. Отходы в случае поломки ПЭВМ. Люминесцентные лампы
3. Безопасность в чрезвычайных ситуациях:	Техногенные ЧС. Пожар.
4. Правовые и организационные вопросы обеспечения безопасности:	Право на условия труда, отвечающие требованиям безопасности и санитарным нормам. (Трудовой кодекс РФ) Использование оборудования и мебели в соответствии с антропометрическими факторами. (СанПиН 2.2.2/2.4.1340-03)

Дата выдачи задания для раздела по линейному графику	01.03.2018

Задание выдал консультант:

Должность	ФИО	Учёная степень, звание	Подпись	Дата
Ассистент	Авдеева Ирина Ивановна			

Задание принял к исполнению студент:

Группа	ФИО	Подпись	Дата
8ВМ6Б	Айд Михаил Александрович		

6 Социальная ответственность

6.1. Введение

Разработанный в рамках магистерской диссертации проект является комплектом программного обеспечения, подобранного и настроенного для обеспечения анонимности и защиты от отслеживания при работе с ресурсами Интернета. Разработка решения производилась при помощи компьютера. Потенциальными пользователями данного программного обеспечения является широкий круг интернет-пользователей, область деятельности которых может быть различной. Независимо от конкретного применения, взаимодействие с предоставленными программами в любом случае производится с помощью программных и аппаратных средств ПЭВМ, а также с помощью периферийных устройств, подключенных к ПЭВМ.

Данный раздел посвящён анализу вредных и опасных факторов производственной среды для операторов ПЭВМ, которые будут использовать полученное решение с той или иной целью.

6.2. Производственная безопасность

Для обеспечения производственной безопасности необходимо проанализировать воздействие на человека вредных и опасных производственных факторов, которые могут возникать при разработке или эксплуатации проекта.

Производственный фактор считается вредным, если воздействие этого фактора на работника может привести к его заболеванию. Производственный фактор считается опасным, если его воздействие на работника может привести к его травме [35].

Все производственные факторы классифицируются по группам элементов: физические, химические, биологические и психофизические. Для данной работы целесообразно рассмотреть физические и психофизические вредные и опасные факторы производства, характерные как для рабочей зоны программиста, как разработчика рассматриваемой в данной работе системы, так

и для рабочей зоны пользователя готового продукта – оператора ПЭВМ. Выявленные факторы представлены в таблице 15.

Таблица 15 – Вредные и опасные производственные факторы при выполнении работ за ПЭВМ [36]

Источник фактора, наименование видов работ	Факторы (по ГОСТ 12.0.003-74)		Нормативные документы
	Вредные	Опасные	
1) Работа за ПЭВМ	1) Микроклимат; 2) Повышенный уровень электромагнитных излучений 3) Недостаточная освещённость рабочей зоны. 4) Монотонный режим работы 5) Шум	1) Опасность поражения электрическим током	1) СанПиН 2.2.4.548-96; 2) СанПиН 2.2.2/2.4.1340-03; 3) СанПиН 2.2.4.3359-16 4) СП 52.13330.2016; 5) ГОСТ Р 12.1.019-2009 ССБТ; 6) СНиП 21-01-97.

6.2.1. Вредные производственные факторы

6.2.1.1. Повышенная или пониженная температура воздуха рабочей среды

Данный фактор является вредным производственным фактором и является фактором микроклимата рабочей среды, параметры которого регулируются СанПиН 2.2.4.548-96. Он больше характерен для рабочей среды программиста-разработчика системы. К параметрам, характеризующим микроклимат в производственных помещениях, относятся:

- Температура воздуха (t, °C);
- Температура поверхностей (t, °C);
- Относительная влажность воздуха (φ, %);
- Скорость движения воздуха (υ, м/с);

- Интенсивность теплового облучения (I, Вт/м^2).

В производственных помещениях для работы с ПЭВМ происходит постоянное выделение тепла самой вычислительной техникой, вспомогательными приборами и средствами освещения. Поскольку оператор расположен в непосредственной близости с источниками выделения тепла, то данный фактор (в случае плохой вентиляции и кондиционирования), является одним из важнейших вредных факторов производственной среды оператора ПЭВМ, а высокая температура воздуха способствует быстрому перегреву организма и быстрой утомляемости [37].

Влажность оказывает большое влияние на терморегуляцию организма. Так, например, высокие показатели относительной влажности (более 85 %) затрудняют терморегуляцию снижая возможность испарения пота, низкие показатели влажности (менее 20 %) вызывают пересыхание слизистых оболочек человека [38].

Санитарные нормы устанавливают оптимальные и допустимые значения величин показателей микроклимата рабочих мест для различных категорий работ в тёплый и холодный периоды года. Для программиста или оператора ПЭВМ категория работ является лёгкой (1а), т.к. работа проводится сидя, без систематических физических нагрузок. Оптимальные параметры микроклимата в офисных помещениях приведены в таблице 16.

Таблица 16 – Оптимальные параметры микроклимата производственных помещений оператора ПЭВМ

Период года	Температура воздуха, ºС	Температура поверхностей, ºС	Относительная влажность, %	Скорость движения воздуха, м/с
Холодный	22–24	21–25	60–40	0,1
Тёплый	23–25	22–26	60–40	0,1

Холодный период года – среднесуточная температура воздуха 10 ºС и ниже, тёплый период года – среднесуточная температура воздуха выше 10 ºС.

В таблице 17 приведены допустимые показатели микроклимата для офисных помещений.

Таблица 17 – Допустимые показатели микроклимата производственных помещений оператора ПЭВМ [39]

Период года	Температура воздуха, ºС		Температура поверхностей, ºС	Относительная влажность, воздуха, %	Скорость движения воздуха, м/с, для диапазона температур воздуха	
	ниже оптимальных величин	выше оптимальных величин			ниже оптимальных величин, не более	выше оптимальных величин, не более
Холодный	20,0–21,9	24,1–25,0	19–26	15–75	0,1	0,1
Тёплый	21,0–22,9	25,1–28,0	20–29	15–75	0,1	0,2

6.2.1.2. Повышенный уровень электромагнитных излучений

Уровень электромагнитных излучений на рабочем месте оператора ПЭВМ является вредным фактором производственной среды, величины параметров которого определяются СанПиН 2.2.2/2.4.1340-03. Основными источниками электромагнитных излучений в помещениях для работы операторов ПЭВМ являются дисплеи компьютеров и мобильных устройств, сеть электропроводки, системный блок, устройства бесперебойного питания, блоки питания.

Излучения, применительно к дисплеям современных ПЭВМ, можно разделить на следующие классы:

- Переменные электрические поля (5 Гц – 400 кГц);
- Переменные магнитные поля (5 Гц – 400 кГц).

Воздействие данных излучений на организм человека носит необратимый характер и зависит от напряжённости полей, потока энергии, частоты колебаний, размера облучаемого тела. При воздействии полей, имеющих напряжённость выше предельно допустимого уровня, развиваются нарушения нервной системы, кровеносной сердечно-сосудистой системы, органов пищеварения и половой системы [40].

В таблице 18 приведены допустимые уровни параметров электромагнитных полей.

Таблица 18 – Временные допустимые уровни электромагнитных полей, создаваемых ПЭВМ на рабочих местах [41]

Наименование параметров		Допустимые значения
Напряжённость электрического поля	в диапазоне частот 5 Гц - 2 кГц	25 В/м
	в диапазоне частот 2 кГц - 400 кГц	2,5 В/м
Плотность магнитного потока	в диапазоне частот 5 Гц - 2 кГц	250 нТл
	в диапазоне частот 2 кГц - 400 кГц	25 нТл
Напряжённость электростатического поля		15 кВ/м

6.2.1.3. Недостаточная освещённость рабочей зоны

Недостаточная освещённость рабочей зоны является вредным производственным фактором, возникающим при работе с ПЭВМ, уровни которого регламентируются СП 52.13330.2011.

Причиной недостаточной освещённости являются недостаточность естественного освещения, недостаточность искусственного освещения, пониженная контрастность.

Работа с компьютером подразумевает постоянный зрительный контакт с дисплеем ПЭВМ и занимает от 80 % рабочего времени. Недостаточность освещения снижает производительность труда, увеличивает утомляемость и количество допускаемых ошибок, а также может привести к появлению профессиональных болезней зрения.

Разряд зрительных работ программиста и оператора ПЭВМ относится к разряду III и подразряду г (работы высокой точности). В таблице 19 представлены нормативные показатели искусственного освещения при работах заданной точности.

Таблица 19 – Требования к освещению помещений промышленных предприятий для операторов ПЭВМ [42]

Характеристика	Наименьший или эквивален	Разряд зрител	Подразряд зрител	Контраст объек	Характеристика фона	Искусственное освещение
						Освещённость, лк

зрительной работы	тный размер объекта различения, мм	ьной работы	ьной работы	та с фоном		При системе комбинированного освещения		При системе общего освещения
						всего	В том числе от общего	
Высокой точности	От 0,3 до 0,5	III	г	Средний, большой	Светлый, средний	400	200	200

6.2.1.4. Повышенный уровень шума на рабочем месте

Уровни звукового давления в октавных полосах со среднегеометрическими частотами 31,5; 63; 125; 250; 500; 1 000; 2 000; 4 000; 8 000 Гц не являются нормируемыми параметрами; рассматриваются как справочные параметры, которые могут использоваться для подбора СИЗ, разработки мер профилактики, решения экспертных вопросов связи заболевания с профессией и так далее; могут измеряться и отражаться в протоколе измерения. (Согласно СанПиН 2.2.4.3359–16). Нормируемыми показателями шума на рабочих местах являются:

а) эквивалентный уровень звука А за рабочую смену,

б) максимальные уровни звука А, измеренные с временными коррекциями S и I,

в) пиковый уровень звука С.

Превышение любого нормируемого параметра считается превышением ПДУ. Нормативным эквивалентным уровнем звука на рабочих местах, согласно СН 2.2.4/2.1.8.562-96, является 50 дБА для программиста. Для пользователей – в зависимости от конкретного рабочего места, но не более 75 дБА (работа, требующая сосредоточенности). Максимальные уровни звука А, измеренные с временными коррекциями S и I — не более 110 дБА и 125 дБА соответственно. Пиковый уровень звука С не более 137 дБС. Работы в условиях воздействия эквивалентного уровня шума выше 85 дБА не допускаются.

Таблица 20 — Эквивалентные уровни звука на рабочих местах для трудовой деятельности разных категорий напряжённости и тяжести, дБА, СанПиН 2.2.4.3359–16.

Предельно допустимые эквивалентные уровни звука, дБА			
Категории напряжённости трудового процесса	Категории тяжести трудового процесса		
	Лёгкая и средняя физическая нагрузка	Тяжёлый труд 1 степени	Тяжёлый труд 2 степени
Напряжённость лёгкой и средней степени	80	75	75
Напряжённый труд 1 степени	70	65	65
Напряжённый труд 2 степени	60	-	-
Напряжённый труд 3 степени	50	-	-

6.2.1.5. Монотонный режим работы

При работе с ПЭВМ основным фактором, влияющим на нервную систему программиста или пользователя, является большое количество информации, которое он должен воспринимать. Во многих случаях это становится сложной задачей и значительно влияет на сознание и психофизическое состояние из-за монотонности работы. Поэтому меры, позволяющие снизить воздействие этого вредного производственного фактора, которые регулируются СанПиН 2.2.2/2.4.1340-03, являются важными в работе оператора ПЭВМ. Они позволяют увеличить производительность труда и предотвратить появление профессиональных болезней.

Организация работы с ПЭВМ осуществляется в зависимости от вида и категории трудовой деятельности. Виды трудовой деятельности разделяются на 3 группы: группа А – работа по считыванию информации с экрана с предварительным запросом; группа Б – работа по вводу информации; группа В – творческая работа в режиме диалога с ПЭВМ. Работа программиста-разработчика рассматриваемой в данной работе системы относится к группам А и Б, в то время, как деятельность врача-специалиста, который будет использовать систему в профессиональной деятельности, относится к группе В. Категории туровой деятельности различаются по степени тяжести выполняемых работ. Для

снижения воздействия рассматриваемого вредного фактора предусмотрены регламентированные перерывы для каждой группы работ – таблица 21.

Таблица 21 – Суммарное время регламентированных перерывов в зависимости от продолжительности работы, вида категории трудовой деятельности с ПЭВМ [41]

Категория работы с ПЭВМ	Уровень нагрузки за рабочую смену при видах работ с ПЭВМ			Суммарное время регламентированных перерывов, мин.	
	группа А, количество знаков	группа Б, количество знаков	группа В, ч	при 8-часовой смене	при 12-часовой смене
I	до 20 000	до 15 000	до 2	50	80
II	до 40 000	до 30 000	до 4	70	110
III	до 60 000	до 40 000	до 6	90	140

6.2.2. Опасные производственные факторы

6.2.2.1. Опасность поражения электрическим током

Поражение электрическим током является опасным производственным фактором и, поскольку оператор ПЭВМ имеет дело с электрооборудованием, то вопросам электробезопасности на его рабочем месте должно уделяться много внимания. Нормы электробезопасности на рабочем месте регламентируются СанПиН 2.2.2/2.4.1340-03, вопросы требований к защите от поражения электрическим током освещены в ГОСТ Р 12.1.019-2009 ССБТ.

Электробезопасность – система организационных и технических мероприятий и средств, обеспечивающих защиту людей от вредного и опасного воздействия электрического тока, электрической дуги, электромагнитного поля и статического электричества.

Опасность поражения электрическим током усугубляется тем, что человек не в состоянии без специальных приборов обнаружить напряжение дистанционно.

Помещение, где расположено рабочее место оператора ПЭВМ, относится к помещениям без повышенной опасности ввиду отсутствия следующих факторов: сырость, токопроводящая пыль, токопроводящие полы, высокая температура, возможность одновременного прикосновения человека к имеющим

соединение с землёй металлоконструкциям зданий, технологическим аппаратам, механизмам и металлическим корпусам электрооборудования.

Для оператора ПЭВМ при работе с электрическим оборудованием обязательны следующие меры предосторожности:

- Перед началом работы нужно убедиться, что выключатели и розетка закреплены и не имеют оголённых токоведущих частей;
- При обнаружении неисправности оборудования и приборов необходимо, не делая никаких самостоятельных исправлений, сообщить человеку, ответственному за оборудование [41, 43].

6.2.3. Мероприятия и рекомендации по устранению и минимизации

Для поддержания нормальных значений параметров микроклимата на рабочих местах они оснащаются системами отопления, вентиляции и кондиционирования воздуха. Также, в некоторых случаях, целесообразно обеспечить питьевое водоснабжение. В помещениях для работы с ПЭВМ производится ежедневная влажная уборка, а также систематическое проветривание после каждого часа работы [39].

Для защиты операторов ПЭВМ от негативного воздействия электромагнитных полей в первую очередь необходимо, чтобы используемая техника удовлетворяла нормам и правилам сертификации. При работе с ПЭВМ установлены регламентированные перерывы, а также иногда предусмотрено использование экранов и фильтров в целях защиты оператора [41].

Для создания и поддержания благоприятных условий освещения для операторов ПЭВМ, их рабочие места соответствуют санитарно-эпидемиологическим правилам СанПиН 2.2.2/2.4.1340-03. Рабочее помещение имеет естественное и искусственное освещение, соответствующее показателям, представленным в таблице 15. Для рассеивания естественного освещения используются жалюзи на окнах рабочих помещений. В качестве источников искусственного освещения использованы люминесцентные лампы, а также лампы накаливания – для местного освещения [42].

Для предупреждения преждевременной утомляемости пользователей ПЭВМ организовывается рабочая смена путём чередования работ с использованием ПЭВМ и без него. В случаях, когда характер работы требует постоянного взаимодействия с компьютером (работа программиста-разработчика) с напряжением внимания и сосредоточенности, при исключении возможности периодического переключения на другие виды трудовой деятельности, не связанные с ПЭВМ, организуются перерывы на 10–15 мин. через каждые 45–60 мин. работы. При высоком уровне напряжённости работы предусмотрена возможность психологической разгрузки в специально оборудованных помещениях [41].

К мероприятиям по предотвращению возможности поражения электрическим током относятся:

- При производстве монтажных работ используется только исправный инструмент, аттестованный службой КИПиА;
- С целью защиты от поражения электрическим током, возникающим между корпусом приборов и инструментом при пробое сетевого напряжения на корпус, корпуса приборов и инструментов заземлены;
- При включенном сетевом напряжении запрещены работы на задней панели;
- Все работы по устранению неисправностей производит квалифицированный персонал;
- Необходимо постоянно следить за исправностью электропроводки [41, 43].

6.3. Экологическая безопасность

В данном разделе рассматривается воздействие на окружающую среду деятельности по разработке проекта, а также самого продукта в результате его реализации на производстве.

Разработка программного обеспечения и работа за ПЭВМ не являются экологически опасными работами, потому объект, на котором производилась разработка продукта, а также объекты, на которых будет производиться его

использование операторами ПЭВМ относятся к предприятиям пятого класса, размер селитебной зоны для которых равен 50 м [45].

Программный продукт, разработанный непосредственно в ходе выполнения магистерской диссертации, не наносит вреда окружающей среде. Аппаратные средства, необходимые для разработки и эксплуатации программного комплекса, могут наносить вред окружающей среде.

Современные ПЭВМ производят практически без использования вредных веществ, опасных для человека и окружающей среды. Исключением являются аккумуляторные батареи компьютеров и мобильных устройств. В аккумуляторах содержатся тяжёлые металлы, кислоты и щелочи, которые могут наносить ущерб окружающей среде, попадая в гидросферу и литосферу, если они были неправильно утилизированы. Для утилизации аккумуляторов необходимо обращаться в специальные организации, специализировано занимающиеся приёмом, утилизацией и переработкой аккумуляторных батарей [46].

Люминесцентные лампы, применяющиеся для искусственного освещения рабочих мест, также требуют особой утилизации, т.к. в них присутствует от 10 до 70 мг ртути, которая относится к чрезвычайно-опасным химическим веществам и может стать причиной отравления живых существ, а также загрязнения атмосферы, гидросферы и литосферы. Сроки службы таких ламп составляют около 5-ти лет, после чего их необходимо сдавать на переработку в специальных пунктах приёма. Юридические лица обязаны сдавать лампы на переработку и вести паспорт для данного вида отходов [46-48].

6.4. Безопасность в чрезвычайных ситуациях

В рабочей среде оператора ПЭВМ возможно возникновение следующих чрезвычайных ситуаций техногенного характера:

- Пожары и взрывы в зданиях и на коммуникациях;
- Внезапное обрушение зданий.

Среди возможных стихийных бедствий можно выделить метеорологические (ураганы, ливни, заморозки), гидрологические (наводнения, паводки, подтопления), природные пожары.

К чрезвычайным ситуациям биолого-социального характера можно отнести эпидемии, эпизоотии, эпифитотии.

Экологические чрезвычайные ситуации могут быть вызваны изменениями состояния, литосферы, гидросферы, атмосферы и биосферы в результате деятельности человека [38].

Наиболее характерной для объекта, где размещаются рабочие помещения, оборудованные ПЭВМ, чрезвычайной ситуацией является пожар.

Помещение для работы операторов ПЭВМ по системе классификации категорий помещений по взрывопожарной и пожарной опасности относится к категории Д (из 5-ти категорий А, Б, В1-В4, Г, Д), т.к. относится к помещениям с негорючими веществами и материалами в холодном состоянии [49].

Каждый сотрудник организации ознакомлен с инструкцией по пожарной безопасности, проходит инструктаж по технике безопасности и обязан строго соблюдать его.

Запрещается использовать электроприборы в условиях, не соответствующих требованиям инструкций изготовителей, или имеющие неисправности, которые в соответствии с инструкцией по эксплуатации могут привести к пожару, а также эксплуатировать электропровода и кабели с повреждённой или потерявшей защитные свойства изоляцией. Электроустановки и бытовые электроприборы в помещениях по окончании рабочего времени должны быть обесточены (вилки должны быть вынуты из розеток). Под напряжением должны оставаться дежурное освещение и пожарная сигнализация. Недопустимо хранение легковоспламеняющихся, горючих и взрывчатых веществ, использование открытого огня в помещениях офиса.

Перед уходом из служебного помещения работник обязан провести его осмотр, закрыть окна, и убедиться в том, что в помещении отсутствуют источники возможного возгорания, все электроприборы отключены и выключено освещение. С периодичностью не реже одного раза в три года проводятся замеры сопротивления изоляции токоведущих частей силового и осветительного оборудования.

Повышение устойчивости достигается за счёт проведения соответствующих организационно-технических мероприятий, подготовки персонала к работе в ЧС [38].

Работник при обнаружении пожара или признаков горения (задымление, запах гари, повышение температуры и т.п.) должен:

- Немедленно прекратить работу и вызвать пожарную охрану по телефону «01», сообщив при этом адрес, место возникновения пожара и свою фамилию;
- Принять по возможности меры по эвакуации людей и материальных ценностей;
- Отключить от сети закреплённое за ним электрооборудование;
- Приступить к тушению пожара имеющимися средствами пожаротушения;
- Сообщить непосредственному или вышестоящему начальнику и оповестить окружающих сотрудников;
- При общем сигнале опасности покинуть здание согласно «Плану эвакуации людей при пожаре и других ЧС».

Для тушения пожара применять ручные углекислотные огнетушители (типа ОУ-2, ОУ-5), находящиеся в помещениях офиса, и пожарный кран внутреннего противопожарного водопровода. Они предназначены для тушения начальных возгораний различных веществ и материалов, за исключением веществ, горение которых происходит без доступа воздуха. Огнетушители должны постоянно содержаться в исправном состоянии и быть готовыми к действию. Категорически запрещается тушить возгорания в помещениях офиса при помощи химических пенных огнетушителей (типа ОХП-10) [50].

6.5. Правовые и организационные вопросы обеспечения безопасности

6.5.1. Правовые нормы трудового законодательства для рабочей зоны оператора ПЭВМ

Регулирование отношений между работником и работодателем, касающихся оплаты труда, трудового распорядка, особенности регулирования

труда женщин, детей, людей с ограниченными способностями и проч., осуществляется законодательством РФ, а именно трудовым кодексом РФ.

Продолжительность рабочего дня не должна быть меньше указанного времени в договоре, но не больше 40 часов в неделю. Для работников до 16 лет – не более 24 часов в неделю, от 16 до 18 лет и инвалидов I и II группы – не более 35 часов.

Возможно установление неполного рабочего дня для беременной женщины; одного из родителей (опекуна, попечителя), имеющего ребёнка в возрасте до четырнадцати лет (ребёнка-инвалида в возрасте до восемнадцати лет). Оплата труда при этом производится пропорционально отработанному времени, без ограничений оплачиваемого отпуска, исчисления трудового стажа и других прав.

При работе в ночное время продолжительность рабочей смены сокращается на один час. К работе в ночную смену не допускаются беременные женщины; работники, не достигшие возраста 18 лет; женщины, имеющие детей в возрасте до трёх лет, инвалиды, работники, имеющие детей-инвалидов, а также работники, осуществляющие уход за больными членами их семей в соответствии с медицинским заключением, матери и отцы-одиночки детей до пяти лет.

Организация обязана предоставлять ежегодный отпуск продолжительностью 28 календарных дней. Дополнительные отпуска предоставляются работникам, занятым на работах с вредными или опасными условиями труда, работникам имеющими особый характер работы, работникам с ненормированным рабочим днём и работающим в условиях Крайнего Севера и приравненных к нему местностях.

В течение рабочего дня работнику должен быть предоставлен перерыв для отдыха и питания продолжительностью не более двух часов и не менее 30 минут, который в рабочее время не включается. Всем работникам предоставляются выходные дни, работа в выходные дни осуществляется только с письменного согласия работника.

Организация-работодатель выплачивает заработную плату работникам. Возможно удержание заработной платы только в случаях, установленных ТК РФ ст. 137. В случае задержки заработной платы более чем на 15 дней, работник имеет право приостановить работу, письменно уведомив работодателя.

Законодательством РФ запрещена дискриминация по любым признакам и принудительный труд [51].

6.5.2. Организационные мероприятия при компоновке рабочей зоны

К мероприятиям, относящимся к компоновке рабочей зоны относятся работы по организации рабочего места пользователя, позволяющие наилучшим образом организовать деятельность работника, делая его работу максимально удобной и безопасной.

Как разработка, так и использование программного комплекса подразумевает работу с ПК. В связи с этим, требуется рассмотрение санитарных норм работы с ЭВМ и организации соответствующего рабочего места.

Для взрослых пользователей для организации рабочего места с ПЭВМ предъявляются следующие требования по СанПиН 2.2.2/2.4.1340-03:

- Высота рабочей поверхности стола для взрослых пользователей должна регулироваться в пределах 680–800 мм; при отсутствии такой возможности высота рабочей поверхности стола должна составлять 725 мм.
- Модульными размерами рабочей поверхности стола для ПЭВМ, на основании которых должны рассчитываться конструктивные размеры, следует считать: ширину 800, 1000, 1200 и 1400 мм, глубину 800 и 1000 мм при нерегулируемой его высоте, равной 725 мм.
- Рабочий стол имеет пространство для ног высотой не менее 600 мм, шириной - не менее 500 мм, глубиной на уровне колен - не менее 450 мм и на уровне вытянутых ног — не менее 650 мм.
- Конструкция рабочего стула обеспечивает:
  - ширину и глубину поверхности сиденья не менее 400 мм;
  - поверхность сиденья с закруглённым передним краем;

- регулировку высоты поверхности сиденья в пределах 400–550 мм и углам наклона вперёд до 15 град. и назад до 5 град.;

- высоту опорной поверхности спинки 300 +/- 20 мм, ширину - не менее 380 мм и радиус кривизны горизонтальной плоскости 400 мм;

- угол наклона спинки в вертикальной плоскости в пределах +/- 30 градусов;

- регулировку расстояния спинки от переднего края сиденья в пределах 260–400 мм;

- стационарные или съёмные подлокотники длиной не менее 250 мм и шириной 50–70 мм;

- регулировку подлокотников по высоте над сиденьем в пределах 230 +/- 30 мм и внутреннего расстояния между подлокотниками в пределах 350–500 мм.

- Рабочее место пользователя ПЭВМ оборудуется подставкой для ног, имеющей ширину не менее 300 мм, глубину не менее 400 мм; регулировку по высоте в пределах до 150 мм и по углу наклона опорной поверхности подставки до 20 град. Поверхность подставки рифлёная и имеет по переднему краю бортик высотой 10 мм.

- Клавиатура располагается на поверхности стола на расстоянии 100–300 мм от края, обращённого к пользователю, или на специальной, регулируемой по высоте рабочей поверхности, отделённой от основной столешницы.

Вывод

В данном разделе были рассмотрены следующие части:

- Производственная безопасность.
- Экологическая безопасность.
- Безопасность в чрезвычайных ситуациях.
- Правовые и организационные вопросы обеспечения безопасности.

По производственной безопасности был проведён анализ выявленных вредных факторов при разработке и эксплуатации проектируемого решения, в результате было установлено, что все пункты, которые включены в данную

часть, соответствуют нормативным документам. Приведены меры по снижению вреда, оказывающие негативное воздействие на человека в процессе работы.

Касательно экологической безопасности были рассмотрены вопросы утилизации отходов оргтехники, макулатуры. В ходе работы установлено, что из самых распространённых источников загрязнения наиболее серьёзным являются вышедшие из эксплуатации люминесцентные лампы, так как в них содержится ртуть. Они также подлежат соответствующей утилизации.

При рассмотрении безопасности в чрезвычайных ситуациях было выявлено что наиболее типичной ЧС для помещения, в котором производится выполнение работы, является пожар. Правовые и организационные вопросы обеспечения безопасности включают в себя требования к организации рабочих мест пользователей в соответствии с СанПиНом, а также организации самого труда согласно Трудовому кодексу РФ.

Заключение

В ходе работы над ВКР был произведён масштабный поиск различной информации о современных методах идентификации пользователей и отслеживания их активности в Интернете. Это само по себе было одной из задач данной работы – сбор и анализ разрозненных фактов из самых различных источников с целью систематизировать эту информацию и перейти от неофициального обсуждения «анонимности» к научному исследованию. Были выполнены этапы аналитического обзора, проектирования и экспериментов. В результате была получена конфигурация программного комплекта, сочетающая ряд положительных качеств. В значительной степени была подтверждена первоначальная гипотеза о том, что высокий уровень защиты достигается без ущерба функциональности браузера.

Спроектированная система имеет и очевидные недостатки, наиболее существенных из которых – высокие системные требования. Виртуальная машина с Windows 7 занимает значительный объём места на жёстком диске и в оперативной памяти, при том что браузер Firefox (впрочем, как и Chrome) сам по себе потребляет сравнительно много памяти, что приводит к необходимости выделять виртуальной машине много системных ресурсов, а это, соответственно, вызывает нехватку памяти в основной системе. В результате, быстродействие виртуальной машины – неудовлетворительное. Далеко не каждый пользователь будет иметь достаточно мощный ПК с большим запасом оперативной памяти.

Используемая цепочка «VPN через Tor», при всех её преимуществах, может быть признана анонимной только при условии, что клиенту удалось сохранить анонимность при регистрации и особенно при оплате VPN-сервиса или VPS-хостинга. Для этого, очевидно, он уже должен обладать надёжным инструментом анонимизации – следовательно, такой клиент может просто не нуждаться в дополнительных мерах защиты.

Список используемых источников

1. Anonymity Bibliography / The Free Haven Project, 2018. – URL: https://www.freehaven.net/anonbib/full/date.html. Дата обращения: 7.06.2018.
2. Самозащита от слежки / Electronic Frontier Foundation. – URL: https://ssd.eff.org/ru. Дата обращения: 7.06.2018.
3. Проект SAFE. Базовые принципы информационной безопасности / Роскомсвобода. – URL: https://safe.roskomsvoboda.org. Дата обращения: 06.06.2018.
4. Козлюк А. У вас есть право на анонимность. Часть 1 / Хабр, 19 мая 2017. – URL: https://habr.com/company/digitalrightscenter/blog/329050. Дата обращения: 10.06.2018.
5. Макаренко Г. Freedom House перевёл Россию в разряд стран с несвободным интернетом : Общество // РБК, 28.10.2015. URL: http://www.rbc.ru/society/28/10/2015/5630abef9a7947d5ad2e5543 (дата обращения: 16.02.2017).
6. Колисниченко Д.Н. Анонимность и безопасность в Интернете. — СПб.: БХВ-Петербург, 2012. — 240 с.
7. Do not confuse Anonymity with Pseudonymity : DoNot // Whonix Wiki. URL: https://www.whonix.org/wiki/DoNot (дата обращения: 8.02.2017).
8. Голованов В. ООН причислила шифрование и анонимность в интернете к правам человека / Geektimes, 29.05.2015. URL: https://geektimes.ru/post/251202/ (дата обращения: 17.02.2017).
9. Петренко С. Почему приватность важна, даже если вам нечего скрывать / БлоGнот, 18.06.2012. URL: https://blognot.co/011002 (дата обращения: 17.02.2017).
10. Лопаницын А. Анонимности нет / Хабрахабр, 27.04.2015. URL: https://habrahabr.ru/post/254217/ (дата обращения: 04.02.2017).
11. Гленн Гринвальд. Почему важна неприкосновенность частной жизни : TED Talk // TED.com, октябрь 2014. URL: https://www.ted.com/talks/glenn_greenwald_why_privacy_matters/transcript (дата обращения: 08.02.2017).
12. Tor (The Onion Router) - как стать анонимным в интернете / Новые информационные технологии, февраль 2013. URL: http://pro-spo.ru/inet/1902-tor-the-onion-router (дата обращения: 17.02.2017).
13. Electronic Frontier Foundation. Введение в моделирование угроз / Самозащита от слежки. URL: https://ssd.eff.org/ru/module/введение-в-моделирование-угроз (дата обращения: 09.02.2017).
14. Alex Efros. «Немножко анонимен» / Хабрахабр, 26.08.2013. URL: https://habrahabr.ru/post/191448/ (дата обращения: 15.02.2017).
15. Как сохранить анонимность в сети: полное руководство / Cryptoworld, 18.01.2016. URL: https://cryptoworld.su/как-сохранить-анонимность-в-сети-полн/ (дата обращения: 31.01.2017)
16. Цатурян Т.Ш. Обзор способов распознавания посетителей веб-ресурсов // Молодежный научно-технический вестник № 01, янв. 2014 : электронный журнал.
17. Жуков А. Фингерпринтинг браузера. Как отслеживают пользователей в Сети / Журнал «Хакер», 30.01.2015. URL: https://xakep.ru/2015/01/30/user-web-tracking-howto/ (дата обращения: 18.02.2017).

18. Meet the online tracking device that is virtually impossible to block / ProPublica, 21.07.2014. URL: https://www.propublica.org/article/meet-the-online-tracking-device-that-is-virtually-impossible-to-block (дата обращения: 18.02.2017).
19. Васильев В. Browser Fingerprint – анонимная идентификация браузеров / Хабрахабр, 6.02.2017. URL: https://habrahabr.ru/company/oleg-bunin/blog/321294/ (дата обращения: 17.02.2017).
20. Positive Technologies. Обнаружен способ деанонимизации пользователей с помощью «звуковых отпечатков» / SecurityLab, 23.05.2016. URL: http://www.securitylab.ru/news/482344.php (дата обращения: 17.02.2017).
21. Jose Carlos Norte. Advanced Tor Browser Fingerprinting : Security // Jose Carlos Norte Personal Blog, 6.03.2016. URL: http://jcarlosnorte.com/security/2016/03/06/advanced-tor-browser-fingerprinting.html (дата обращения: 14.02.2017).
22. Бессонова Е.Е., Зикратов И.А., Росков В.Ю. Анализ способов идентификации пользователя в сети Интернет // Научно-технический вестник информационных технологий, механики и оптики. – 2012. – № 6 (82).
23. Yinzhi Cao, Song Li, Erik Wijmans. (Cross-)Browser Fingerprinting via OS and Hardware Level Features / Yinzhi Cao, Lenigh University, 2017. URL: http://yinzhicao.org/TrackingFree/crossbrowsertracking_NDSS17.pdf
24. Глущенко А. Чек-лист проверки анонимности сёрфинга / Хабрахабр, 26.07.2015. URL: https://habrahabr.ru/post/263557/ (дата обращения: 04.02.2017).
25. Определяем пользователей VPN (и их настройки) и прокси со стороны сайта / Хабрахабр, 24.07.2015. URL: https://habrahabr.ru/post/216295/ (дата обращения: 31.01.2017).
26. Что такое атаки пересечения и подтверждения [Электронный ресурс] : Сетевая анонимность, общие вопросы // OpenPGP в России. URL: https://www.pgpru.com/faq/anonimnostjobschievoprosy#h37444-7 (дата обращения: 03.02.2017).
27. Кирилин Д.А. Глубоко эшелонированная анонимность / Хабрахабр, 14.07.2012. URL: https://habrahabr.ru/post/147792/ (дата обращения: 17.02.2017).
28. Морозов Е. Что такое сеть Tor и как она работает / iGuides.ru, 7.08.2017. URL: https://www.iguides.ru/main/other/chto_takoe_set_tor_i_kak_ona_rabotaet/ (дата обращения 16.09.2017)
29. Tor Network Status / TorStatus. URL: https://torstatus.blutmagie.de/#Stats (дата обращения: 8.09.2017)
30. Tor: Pluggable Transports: Documentation / Tor Project. URL: https://www.torproject.org/docs/pluggable-transports.html.en (дата обращения 10.09.2017)
31. Things NOT to Do / Whonix Wiki. URL: https://www.whonix.org/wiki/DoNot (дата обращения: 8.02.2017).
32. Нефёдова М. В Firefox обнаружена 0-day уязвимость, использующаяся для атак на пользователей Tor / Журнал «Хакер», 30.11.2016. URL: https://xakep.ru/2016/11/30/firefox-0day/ (дата обращения: 18.02.2017)
33. Positive Technologies. В сети Tor обнаружено 110 отслеживающих активных узлов / SecurityLab, 26.07.2016. URL: http://www.securitylab.ru/news/483200.php (дата обращения: 10.09.2017).
34. Юнусов Т. Tor и новые альтернативы в области обеспечения анонимности / Geektimes, 26.09.2016. URL: https://geektimes.ru/post/280762/ (дата обращения: 7.06.2017).

35. Сравнение протоколов VPN / vpnMentor, 22.11.2016. URL: https://ru.vpnmentor.com/blog/сравнение-протоколов-vpn-pptp-vs-l2tp-vs-openvpn-vs-sstp-vs-ikev2/ (дата обращения 11.09.2017)
36. Установка и настройка SoftEther VPN Server / SecurityForAll, 22.06.2017. URL: https://secfall.com/ustanovka-i-nastroyka-soft-etther-vpn/ (дата обращения 13.08.2017)
37. Кричевский В. Мысли об идеальной анонимности: Блог компании Whoer.net // Geektimes, 13.04.2016. URL: https://geektimes.ru/company/whoer/blog/274292/ (дата обращения 3.02.2017)
38. Создаём OpenVPN-сервер. Анонимно арендуем VPS : Защита информации // Runion, 25.05.2017. URL: https://lwplxqzvmgu43uff.onion.rip/viewtopic.php?id=14778 (дата обращения 01.06.2017)
39. Савчук И. Технология Port knocking / Blogerator, 30.01.2013. URL: http://blogerator.org/page/pozadi-zakrytyh-dverej-port-knocking-bezopasnost-dostupa-knockd-zaschita-ssh-1 (дата обращения: 7.08.2017)
40. Методы анонимности в сети. Часть 4. Tor&VPN. Whonix / Хабрахабр, 30.11.2013. URL: https://habrahabr.ru/post/204266/ (дата обращения 12.02.2017)
41. Организация работы на ОС Whonix / Runion, 13.12.2016. URL: https://lwplxqzvmgu43uff.onion.rip/viewtopic.php?id=11369 (дата обращения: 8.09.2017)
42. Joanna Rutkowska. Software compartmentalization vs. physical separation / Invisible Things Lab, 2014. URL: https://invisiblethingslab.com/resources/2014/Software_compartmentalization_vs_physical_separation.pdf
43. Райтман М.А. Искусство легального, анонимного и безопасного доступа к ресурсам Интернета. — СПб.: БХВ-Петербург, 2017. — 624 с.
44. Татаринов Т. Делаем «шпионскую флешку» с защищённой ОС Tails / Журнал «Хакер», 1.11.2016. URL: https://xakep.ru/2016/11/01/tails-live-flash/ (дата обращения: 10.09.2017)
45. Анонимное поведение / HiddenGate Wiki, 2014. URL: http://hiddengate.i2p.xyz/wiki/Анонимное_поведение (дата обращения: 18.10.2016).
46. Осторожнее с копипастом: фингерпринтинг текста непечатаемыми символами / Хабр, 6.04.2018. URL: https://habr.com/post/352950. Дата обращения: 10.06.2018.
47. Рекомендуемые настройки безопасности для Firefox / cryptopunks, 26.02.2015. URL: https://cryptopunks.org/article/firefox-secure-tweak. Дата обращения: 10.09.2017.
48. Что такое VPS, принцип работы : Техническая документация // Мастерхост. URL: https://masterhost.ru/support/doc/vps/ (дата обращения: 21.03.2018).
49. Fionn Fitzmaurice. OpenVPN with Modern Cryptography // Trinity College Dublin. URL: https://www.maths.tcd.ie/~fionn/misc/ec_vpn.php (дата обращения: 18.03.2018).
50. Предупреждение по криптографии на основе эллиптических кривых : Шифрование VPN // Private Internet Access. URL: https://rus.privateinternetaccess.com/pages/vpn-encryption#ecc_warning (дата обращения: 20.03.2018).
51. Установка OpenVPN на CentOS 7 // SecurityForAll, 07.06.2017. URL: https://secfall.com/anonimnost-v-internete-svoimi-rukami-ustanovka-i-nastroyka-vpn-servera/ (дата обращения: 19.03.2018).

Приложение А

Раздел 2

Сравнительный обзор и анализ методов обеспечения анонимности в Интернете

Студент:

Группа	ФИО	Подпись	Дата
8ВМ6Б	Айд Михаил Александрович		

Консультант отделения ИТ:

Должность	ФИО	Учёная степень, звание	Подпись	Дата
Старший преподаватель	Дорофеев Вадим Анатольевич			

Консультант – лингвист отделения ИЯ:

Должность	ФИО	Учёная степень, звание	Подпись	Дата
Старший преподаватель	Куркан Наталия Владимировна			

2 Methods for ensuring anonymity on the Internet

2.1 Main categories of anonymization tools

1) Proxy servers. There are several types of proxy servers with different features, but for anonymization, SOCKS5 is usually used. Currently, they cannot be considered reliable because they alone do not provide traffic encryption and are relatively easy to deanonymize even if a proxy chain was built: the sequential examination of logs on each server will allow an investigator to determine the real IP at any length of the chain. Preferably to be used in combination with VPN.

2) VPN service also includes several protocols. These services are often charged. They provide high reliability of channel encryption. However, as with the use of a proxy server, the main problem is the issue of trust to the service provider. The vast majority of VPN providers claim that there is no logging but in fact it is impossible to verify, most often they keep logs. In addition, VPN has the following disadvantage: if the VPN connection is suddenly interrupted, all traffic will go directly to the Internet, which leads to the disclosure of a real IP. This problem is usually solved by an additional configuration of firewall rules.

3) SSH tunnels were originally created (and still in use) for other purposes, but they are also used "for anonymity". Partially similar to the VPN by traffic encryption, they have different operating principles and potentially lower speed. Unlike the VPN, the SSH do not forward all traffic to the tunnel by default (although there are special programs for this), and are used like a local proxy server.

4) Dedicated servers can be used as a remote workstation or as a platform for launching your own VPN server. Often, virtualization (VPS) is used, when several virtual servers are located on one physical host, which makes it difficult to track connections to a particular server [15].

5) Tor anonymity network. For some time it was considered to be the most reliable instrument of providing anonymity on the Internet but later there were several cases of deanonymization of users. Traffic is monitored at many exit nodes, moreover, the access to a website from an IP address belonging to the Tor node is often regarded as suspicious.

6) JonDonym or JAP (Java Anonymous Proxy). It directs traffic through a chain of servers, the user can choose which "cascades" are used. It has a free and a premium access. The JonDoFox browser of earlier versions was a Firefox build with a set of add-ons, and now it is a modified Tor Browser.

7) I2P is an anonymous, decentralized network operating over the Internet, not using IP addressing. It surpasses Tor for the reliability and complication of encryption of transmitted data. Sometimes it is positioned as an alternative to Tor, but in fact it is of little use to anonymize access to the Internet (and it was not originally intended for this) because of unstable and slow connection, especially without a public IP address.

8) Virtual machines solve a number of additional security tasks for anonymous work and used in combination with other means. It is usually easier to direct all the traffic of the virtual machine to the VPN or Tor channel than to do it with the traffic of the host system. An Internet browser inside the virtual machine does not have the access to the physical host hardware information. It is recommended to use the visual theme in the guest system, which differs markedly from the host one, so as not to accidentally confuse the windows. Visual difference between browsers is especially important. It is not allowed to install software with a license associated with real user data, in order to avoid the leakage of these data to an anonymous channel [27].

9) The so-called "antidetect" are assemblies of browsers with built-in spoofing of various identifiers. They are often created for illegal activities (aimed at bypassing anti-fraud systems), they are of high price and not laid out freely. There are also free solutions with varying efficiency. The task of traffic anonymizing usually remains at the discretion of the user. The term "antidetect" is also applied to the virtual machines modified for plausible masking for a real PC.

10) Other means of anonymization: tools that are poorly popular, insufficiently tested or not providing strong anonymity. Also, here are programs and browser extensions designed for tracking protection in the browser. They may complement the anonymization system in those aspects that are not provided by the means listed above.

2.2 TOR network

The Onion Router is the most significant and popular tool for providing anonymity on the Internet. This is free and open-source software that operates on the principle of so-called «onion routing»: all data coming into the TOR network passes through three randomly selected network nodes, and before being sent are sequentially encrypted with the keys of the selected nodes. When the first node receives the packet, it deciphers the "upper" layer of the cipher (hence the analogy with peeling an onion) and finds out where to send the package further. The second and third server do the same. The most vulnerable points in this chain is the exit nodes, on which the traffic is finally decrypted and directed to the target resource. On the exit nodes, traffic can be listened, and this should be remembered when a connection to a resource occurs over an unsecure protocol – for example, a non-HTTPS site is visited [28].

In fact, TOR is a network of encrypting proxy servers, or virtual tunnels, supported primarily by volunteers. For 2017, this network has about 7000 nodes, of which 11% are output nodes [29]. Thus, the number of possible routes is very large, in addition, TOR changes its paths every 10 minutes. Entry nodes provide protection from interception and falsification of data on the path between the entry node and the client. In addition, there are bridges – nodes whose addresses are not published in the general catalog, but can be provided on the client request [30]. Bridges provide access to the network in cases where the ISP blocks known TOR input nodes, and also obfuscates (disguises) traffic, which prevents its identification and blocking by DPI systems. Several types of bridges have been developed, at present the most effective is *obfs4*.

Probably, for many users experience with Tor is limited to working in Tor Browser. This assembly consists of a Tor application and a modified version of the Firefox browser. Modern versions are relatively reliable and at the same time an affordable tool for counteracting the monitoring and preservation of anonymity. Many of Tor Browser's enhancements are gradually being introduced into the Firefox (the Tor Uplift project). However, user should clearly distinguish between Tor Browser and Tor itself, which can be run without a browser. Previously, Vidalia, a graphical interface for managing the Tor node, was widely used, but its development was

discontinued. There is also AdvOR (Advanced Onion Router), which allows you to force the traffic of applications through Tor and configure various parameters of the site. Generally speaking, the usual Tor Browser also allows Tor to be used as a proxy for various applications. While Tor is running, it provides a local SOCKS5 interface, which parameters can be seen in the proxy settings of the Tor Browser. For applications that do not support work through a proxy, it is possible to use the Proxifier program or the above AdvOR. An important limitation: Tor only supports TCP traffic, but not UDP. In the case when UDP operation is required, additional tunneling of UDP traffic via VPN will be required.

The main disadvantage of Tor Browser is that the fact of using it can easily be determined by the visited resource. First, the IP addresses of the Tor exit nodes are publicly known, and some sites restrict access from such addresses, since various intruders often use Tor. Also Tor Browser has distinctive fingerprints. The tracking prevention mechanisms used by this browser make all instances of Tor Browser indistinguishable from each other (or, in any case, aspire to this), therefore it is very difficult to track a particular user, however it is easy to recognize that he uses Tor Browser. Of course, this does not apply to internal Tor network sites – onion resources, which are directly intended for visiting via Tor.

It is strongly recommended against to use Tor for BitTorrent. This not only threatens anonymity, but also creates unnecessary strain on the Tor network. We list some other things that should not be done [31]. User should not sign through Tor in the accounts associated with the real person, and also should not sign without anonymization into the accounts created via Tor. If the account has at least once been used with a real IP, it is no longer anonymous. Do not forget about the social methods of deanonymization: you should not disclose identification data in anonymous communication or publications. It is undesirable to use the same digital personality for too long – the longer one pseudonym is used, the more it accumulates profiling information about it. It is not recommended to remain authorized in any account for longer than necessary. You should not connect to the resource at the same time anonymously and not anonymously, as this allows you to detect correlations between

the two connections. Downloadable files, especially executables, should be treated with the utmost care. In addition, it is undesirable to install any add-ons in Tor Browser and generally to change its standard configuration.

The Tor network is considered a relatively reliable means of anonymization, but cases of disclosure of the identity of users have repeatedly occurred. First of all, note that deanonymization is not always connected with the vulnerability of the Tor itself, social engineering methods are often used, and the user himself can make mistakes. However, the FBI at least twice has successfully exploited [32] the «zero day vulnerability» in Firefox (on which the Tor Browser is based). In addition, some methods of browser tracking, the so-called fingerprinting, turned out to be suitable for Tor Browser, although by now the developers significantly strengthened its protection [21]. Tor also periodically encountered the problem of malicious sites that intercepted and even infected traffic, and this applies not only to the output relay - in 2016, the researchers found 110 hidden service directories (HSDir) that track requests for onion resources and used to find vulnerabilities of these resources [33]. Malicious nodes in Tor continue to be detected and blocked from time to time by the Tor network.

The vulnerability of Tor to attacks that analyze traffic has been known for a long time. The original project documentation indicates the vulnerability of the system to the "global passive adversary", capable of listening to all traffic of input and output nodes. By matching both traffic streams, such an attacker can deanonymize each user. In reality, this is possible on a smaller scale, since no organization is able to control the entire Tor network completely, but the presence of even two monitored nodes (entry and exit) already gives the chance to identify some, albeit insignificant, of users whose traffic will pass through both node [34]. Tor was not originally designed to withstand large-scale attacks, when an attacker has multiple points of presence within the network. Here it is appropriate to recall the I2P network, created with the account that each node can be listened.

So, at the moment Tor remains a relatively effective free tool for providing anonymity and anti-tracking (in the Tor Browser), continues to actively develop and receive new security mechanisms. However, its use is associated with some

inconveniences and is not sufficient for reliable anonymization. It is advisable to consider Tor as a basis for constructing combinations that are more complex.

2.3 Virtual private network

The Virtual Private Network technology, designed for secure data transmission through an encrypted tunnel between two computers, has today become a popular way of anonymizing and is often perceived by Internet users as an alternative to Tor. In fact, this is incorrect – the preservation of anonymity here is entirely based on the trust of the VPN service provider, except when the user configures his own VPN server. It is more correct to say that the VPN provides data privacy, for example, it allows the user to hide the history of his activity from the Internet provider. The connection speed for paid VPNs is usually much higher than in Tor.

2.3.1 Protocols

There are several common VPN protocols:

- PPTP. Fast, easily configurable, but relatively unsafe and obsolete. Point-to-Point Tunneling Protocol was invented by Microsoft and for a long time was the standard protocol for VPN. To ensure security, it relies on various authentication methods. Although PPTP is commonly used with 128-bit encryption, in 1999 a number of vulnerabilities were found. The most serious was the vulnerability of the authentication protocol MSCHAP v.2, and with its use PPTP was hacked within 2 days. Although Microsoft corrected this error by using the PEAP authentication protocol instead of MSCHAP, she recommended using the L2TP or SSTP protocols for VPN [35].
- L2TP / IPsec. The Layer 2 tunneling protocol, unlike other VPN protocols, does not encrypt or protect data. Therefore, additional protocols are usually used, in particular IPSec, through which data is encrypted before transmission. All modern devices and systems compatible with VPN have built-in L2TP / IPSec protocol. Installation and configuration are easy and do not take much time, but there may be a problem with using the UDP port 500, which is blocked by NAT firewalls. So, if the protocol is used with the firewall, you may need to redirect the ports. It is not known about any major IPSec vulnerabilities, and with proper application it provides reliable

data protection. Nevertheless, Edward Snowden noted that this protocol is also not so safe. John Gilmour, founder and security specialist of Electric Frontier Roundation, states that the US National Security Agency deliberately weakens the protocol. Moreover, double encapsulation of data makes the protocol not as effective as, for example, SSL-based solutions, and therefore it works slower than other protocols.

- OpenVPN is a relatively new open source technology that uses the OpenSSL library and SSLv3 / TLSv1 protocols along with many other technologies to provide a reliable VPN solution. One of the main advantages is that OpenVPN is very flexible in the settings. This protocol can be configured to work on any port, including on the 443 TCP port, which allows to mask traffic inside OpenVPN as normal HTTPS, so it is difficult to block it. Another advantage is that OpenSSL libraries support many cryptographic algorithms (for example, AES, Blowfish, 3DES, CAST-128, Camelia and others). Typically, VPN-providers use only AES and Blowfish.

The speed of OpenVPN depends on the level of encryption, but it is usually higher than for IPSec. And although OpenVPN is now used by most VPN providers, it is not supported by default on any platforms. However, the corresponding third-party applications are already developed not only for the PC, but even for Android and iOS. There is another problem with OpenVPN - flexibility can make it inconvenient to configure. In particular, when using a typical OpenVPN software implementation (for example, a standard open client for Windows), it is necessary not only to download and install the client, but also to download the configuration files. Many VPN providers solve this problem by using preconfigured VPN clients.

Taking into account all the factors and information presented by E. Snowden, we can assume that the OpenVPN protocol is the safest now. It is also assumed that it is protected from interference of the US National Security Agency, as it uses experimental encryption methods. Naturally, no one knows all the possibilities of the NSA, but most likely, OpenVPN is the only truly secure protocol for today [35].

- SSTP. Microsoft introduced the Secure Socket Tunneling Protocol in Windows Vista SP1, and although it is now available on Linux, RouterOS and SEIL, it is still used largely by only Windows systems. SSTP uses SSL v.3 and therefore offers similar

benefits to OpenVPN (for example, the ability to use TCP port 443 to bypass NAT), and since it is integrated into Windows, it is easier to use and more stable than OpenVPN. However, SSTP does not have open source, and all rights to it belong to Microsoft, so OpenVPN should preferably be used.

- IKEv2 (key exchange protocol, version 2) developed by Cisco and Microsoft, is built into Windows 7 and later versions. The protocol allows open source modifications, in particular for Linux and other platforms, Blackberry devices are also supported. It is well suited for setting up an automatic VPN connection if the Internet connection is interrupted periodically. Users of mobile devices can use it as a protocol for wireless networks by default, it is very flexible and allows you to easily switch networks. Although IKEv2 is available on fewer platforms than, for example, IPSec, it is considered to be a fairly good protocol in terms of stability, security and speed. The disadvantage is the closed source code.
- SoftEther VPN is a multiprotocol VPN server under the GPLv2 license, is being developed since 2013, has a wide range of capabilities. It has its own SSL-VPN protocol, which is indistinguishable from normal HTTPS traffic. Declared support for L2TP / IPsec, MS-SSTP, OpenVPN, L2TPv3 and EtherIP, and L2TP indicates strict compatibility with embedded clients in iOS and Android. The server itself has versions for Windows, Linux, OS X, FreeBSD and Solaris. It runs faster than OpenVPN, does not require TUN / TAP, has built-in NAT and DHCP. SSL-VPN protocol can work through TCP, and it supports multiple TCP sessions, UDP and even ICMP [36].

2.3.2 The problems of choosing a VPN provider

So, when choosing a protocol, we should probably choose OpenVPN, and if it's about configuring your own VPN server, it makes sense to use SoftEther VPN. Some of the free public VPN Gateway servers also provide SoftEther (SSL-VPN) access. Note that many VPN providers offer their own client applications for connection – it can be convenient, but potentially unsafe. The OpenVPN protocol implies the use of an open client and a configuration file, which should be given by the provider. On the other hand, the provider application can have useful functions: the so-called kill switch (prevention of traffic leaks bypassing the VPN when the connection

is interrupted), protection against DNS leaks. However, the reliability of their work must be thoroughly tested.

The choice of a VPN provider should be approached very carefully and responsibly. Free VPNs often cause distrust, as it is unclear who and for what purpose sponsors the service - perhaps all user activity is tracked. Case in point: in 2017, the human rights group Center for Democracy and Technology (Center for Democracy and Technology, CDT) caught the popular Hotspot Shield service in violation of its own privacy policy. The researchers found that Hotspot Shield tracks user behavior on the Internet, redirects Internet traffic, sells data to third-party users, and discloses sensitive data, including wireless network names, MAC addresses, and IMEI device IDs. In addition, the application injected the Javascript code for advertising purposes. As shown by the reverse engineering of the source code of the application, Hotspot Shield used more than five different third-party libraries to track users. In some cases, the service redirected traffic to partner sites, including advertising companies, for profit.

Large paid VPN-services, as a rule, are more serious about maintaining confidentiality. However, one should not trust statements about the absence of logging, most often logging activity is performed, but much depends on the amount of data collected, the time of their storage and the possibility of providing them at the request of authorized organizations. It is useful to ask the technical support of the service whether the account can be blocked in case of malicious activity of the user. If the answer is that access will be blocked only when complaints (abuses) are received, then activity is not tracked really. Also of great importance is the possibility of anonymous payment for the service. Disclosure of payment data to the VPN provider is clearly contrary to the preservation of anonymity. If the service is positioned as providing anonymity, it must accept crypto currency. Note that Bitcoin is usually only accepted, but it does not provide reliable anonymity unless you use mixers. Preferred would be crypto-currencies such as Monero or Dash, more transaction-oriented, but there are practically no VPN services that would accept them for payment.

It is recommended to choose a foreign VPN provider in the jurisdiction of the country that does not maintain diplomatic relations with the country of the user, or a

country with liberal legislation, where obtaining server logs is difficult even for the local police. The same applies to the use of two VPNs (not DoubleVPN, but different providers) – it is desirable to select servers in countries that do not cooperate with each other [37]. In addition, the countries of the "Five Eyes" alliance - the main participants of the UKUS SIGINT agreement – should be avoided. In general, the choice of a reliable VPN provider is a difficult task even for an experienced user. In 2016, the site thatoneprivacysite.net was launched, which provides a detailed comparison of over a hundred VPN-services on a set of parameters. The table does not give an unambiguous answer "which VPN is the best", but Proxy.sh that located in Seychelles, Swedish oVPN.se and IPredator, Gibraltar IVPN and Icelandic CryptoStorm can be called the leaders. Private Internet Access, NordVPN, Mullvad, AirVPN also has a good reputation. Also, there are a small number of providers that host their ads on "dark" resources, in fact openly offering their services to potential intruders. The attitude to such providers is usually contradictory. Theoretically, this behavior should mean that this provider basically does not cooperate with law enforcement agencies and will provide reliable anonymity for any user. The real situation can be exactly the opposite. If there are no compelling reasons for trusting such VPNs, it is preferable to refrain from using it.

As for the various DoubleVPN, TripleVPN, QuadVPN, it is more a marketing move than an increase in security, since all the chain servers belong to the same VPN provider, and their number does not prevent the logging of user activity and the possibility of disclosing this data by the provider. However, replacing a single VPN with DoubleVPN reduces the likelihood of de-anonymization. Note that this is not a two-layer encryption – unlike Tor, the traffic on the staging server is decrypted. But it is possible to make Parallel VPN – a way of connecting through two parallel VPN-channels, in which traffic is encrypted twice (channel in the channel). This somewhat reduces the speed, but solves the problem of unprotected traffic on the staging node.

Summary: VPN should not be considered as a reliable means of providing anonymity, but with the right choice of provider and the correct configuration, a high level of confidentiality can be achieved.

2.4 Using VPS

A virtual private server, with respect to anonymization, is used to configure your own VPN, SSH or proxy server, and sometimes the Tor node, if the VPS hoster allows it. The cost of renting a VPS can be lower than buying a VPN. At the same time, administrative access to the server allows you to completely disable logging and generally configure the VPN server for your own needs if you have the appropriate skills. The disadvantage of this solution is that the user on the server is only one, and it is much easier to track than using large paid and free VPNs. On the other hand, there are several virtual servers on a physical server, so it will still be difficult for an external observer to map outgoing connections from that server to a particular user. When choosing a provider, you can follow the same considerations as for a VPN. At a minimum, the server should not fall under the jurisdiction of the special services of the country where the user is located, or countries that are in cooperation with it.

There are a lot of VPS providers, and a significant number of foreign companies accept Bitcoin for payment. However, if it is supposed to remain anonymous during registration, problems can arise already at this stage. Many VPS hosters do not allow anonymous registration. In the case of the presence of an anti-fraud system, several basic factors should be considered: the IP address should not be a Tor address or a public proxy server; personal data must be plausible, you do not need to enter random character combinations instead of the name; the address is also plausible, the country must match the IP address; telephone – belonging to the specified country [38]. In general, with any anonymous registration, when it is required to specify personal data, it is desirable to create the most plausible pseudonym, and not to attract attention by entering meaningless data. And, of course, if in the future it is planned to connect to VPS from a real IP-address, then anonymous purchase does not make sense.

When choosing a server, you need to pay attention to the traffic limit and bandwidth. The capacity of the hard disk is almost not important, but at least 512 megabytes of RAM is recommended. To deploy a VPN server, you need TUN / TAP support (not needed for SoftEther). Depending on the particular host and type of virtualization, you may need to request a support service to enable the TUN adapter.

Access to the server is usually provided through SSH. It should be configured for certificate authorization to secure the server from hacking the SSH password. Then, we probably need to configure the firewall rules, and then install and configure the main software. Your own server allows you to configure the VPN so that a website will not determine its use by MTU or specific ports. In addition, it is possible to protect services from detection by intruders using the so-called port knocking. This is an implicit form of allowing access to a certain service, if a predefined sequence of connections is made with the different ports of the target server. The special software on the server side keeps track of all incoming connections, and if a characteristic "connection chain" is fixed, corresponding to the previously specified "reference knock" – temporarily opens access to the closed port and, accordingly, the hidden service on it [39].

2.5 Operating systems for online anonymity

Several Linux distributions specifically aimed at providing anonymity and security. Typically, such assemblies are based on Debian, use the Tor network and various additional security features. If we do not consider systems whose development was terminated, the following projects are currently being singled out:

- Whonix
- Tails
- Kodachi
- MOFO Linux
- Subgraph OS
- heads

Let us consider in more detail the first two items of this list.

2.5.1 Whonix

OS Whonix is an anonymous system based on Debian and consists of two virtual machines, one of which is a gateway sending all traffic to the Tor network and the other an isolated workstation that connects only to the gateway. There is also the option of physically dividing the gateway and workstation. Whonix implements the mechanism of the so-called isolation proxy server. The workstation does not receive

an external IP address on the Internet, and it helps to neutralize many vulnerabilities, for example, even if malware gets root access to the workstation, it will not have the ability to know the real IP address. [40]

Whonix, according to the developers, has successfully passed many leak tests. Even such applications as Skype, BitTorrent, Flash, Java, known for their features to go to the open Internet bypassing Tor, have been successfully tested for the absence of leakage of compromising data. OS Whonix implements the following anonymization mechanisms:

- All traffic of any applications goes through the Tor network;
- To protect against traffic profiling Whonix implements the concept of thread isolation. Pre-installed in Whonix applications are configured to use a separate Socks-port, and since each Socks-port uses a separate chain of nodes in the Tor network, profiling is impossible;
- Secure hosting of Tor Hidden services services is provided. Even if an attacker breaks a web server, he cannot steal the private key of the Hidden service, since the key is stored on the Whonix gateway;
- Whonix is protected from DNS leaks, because it uses the principle of an isolated proxy in its architecture. All DNS requests are redirected to DnsPort Tor;
- Whonix supports Tor obfuscated bridges;
- Technologies "Protocol Leak Protection and Fingerprinting Protection" are used, which reduce the risk of identification by the digital fingerprint of the browser or the system by using the most common values, for example, username is *user*, time zone – UTC, etc .;
- It is possible to tunnel other anonymous networks: Freenet, I2P, JAP, Retroshare via Tor, or work with each such network directly;
- It is important to note that in Whonix all VPN / SSH / Proxy combining schemes with Tor have been tested, documented and work well [41];
- Whonix is a completely open project that uses free software.

The Whonix installation is possible in several ways. Running virtual machines in VirtualBox is the easiest way. More reliable is the use of Qubes-Whonix when

Qubes OS is used as the host operating system, and Whonix-Gateway is installed through the built-in virtualization. The Qubes OS system uses the Xen hypervisor to implement the "security through isolation" approach. It is also possible to run Whonix with KVM virtualization using qemu-kvm, and the last option is physical isolation, installing two Whonix components into two physical machines. It is recommended that you install the gateway directly on the hardware of the PC, and the workstation (Workstation) in the virtual machine. Note that the developers after the studies have recognized Qubes-Whonix safer than physical isolation [42]. However, vulnerabilities are also possible in Xen. Another feature of Whonix is the ability to connect via Gateway to virtually any virtual machine instead of Whonix-Workstation.

At the present time, the installation of Whonix under Windows is simplified to the maximum extent due to the appearance of an automatic installer that automatically downloads and imports images of virtual machines into VirtualBox, and then allows them to be launched at the push of a button. Testing revealed a problem: the installer installs a separate instance of VirtualBox, even if VirtualBox is already present in the system. As a result, a conflict occurs, and both instances become inoperative. In this situation, you should uninstall the original VirtualBox, and then reinstall it in the directory that was created by the Whonix installer.

2.5.2 TAILS

The Amnesic Incognito Live System became known as the "system used by Edward Snowden" and "the most anonymous OS." In fact, it's hard to say that Tails are better (or worse) than Whonix, because their concepts vary significantly. Tails is a live distribution for downloading from a Flash drive and leaves no traces on the computer where it was used. Like Whonix, Tails is based on Debian. All outgoing connections are made through the Tor network, and attempts of non-anonymous connections are blocked [43]. Tor Browser works in protected mode (AppArmor). At the same time, Tails has an "Unsafe browser" (regular Firefox), allowing you to visit sites directly, without Tor. In general, Tails may seem less secure than Whonix, since it has access to a physical system, MAC address, real IP, while Whonix-Workstation is isolated in a virtual machine. On the other hand, in the case of Whonix, there may be

vulnerabilities in both its components, and in VirtualBox and in the operating system of the host. In principle, running Tails in a virtual machine is also possible, but you need to use the virt-manager package in Debian.

In addition to Tor Browser, Tails preinstalled a set of software, in particular:

- Pidgin - Jabber + OTR
- Electrum - Easy Client for Bitcoin
- KeePassX - password manager (s)
- GPG - asymmetric encryption system
- MAT - removing metadata from different file types
- Programs for editing documents, photos, audio, video, etc.
- Thunderbird - mail client
- It's easy to install Psi or Psi + (Jabber with GPG support)

The procedure for installing Tails from under Windows is somewhat unique, it requires two Flash-drives. First, the Tails installation image is written to the first medium (2 GB in size) - this is an "intermediate" Tails, which is limited for work (when installing from Linux, the procedure is simpler and no intermediate media is required). Then you should download the PC from this media. Often at this stage, a problem occurs, the BIOS can not correctly load the image. In this case, we recommend that you overwrite Tails on the media using Rufus instead of the recommended Universal USB Installer. Usually, after this, the download succeeds. Then, the second drive is connected, and the "basic" Tails is installed on it. To do this, go to Applications → Tails → Tails Installer → Install by cloning. After the installation is successfully completed, the second media is ready for use, and the first media is no longer required. You can shut down the system.

We are loading from the second drive. Now, to be able to save any data in the system, you should create a permanent partition - the LUKS crypto container. We select in the menu Application → Tails → Configure Persistence and set the password, preferably crypto-resistant. It is possible to choose which data will be saved. Anything that is not stored in the persistent partition is cleared after the Tails reboot. Note that Tor Browser has the ability to read and write only 2 folders, they are in the bookmarks

of the explorer: Tor Browser and Tor Browser (Persistent). Downloading and uploading files is only possible in / from them. If you have really important data, you should periodically make a backup copy to another media, since the chance of a sudden failure of the Flash drive is much higher than the hard drive.

Using VPN in Tails is not recommended by the developers, so this feature is not available by default, and the VPN configuration requires intervention in iptables rules. It is believed that the chain "VPN via Tor" harms anonymity; this is stated in the official Tor documentation. The fact is that Tor's important advantage is the frequent change of traffic routes, and when connecting to a VPN server via Tor, a permanent route, a fixed destination, is actually created. However, to realize such a chain allows Whonix. For Tails, a "Tor via VPN" scheme is possible if you use a router with dd-wrt firmware and connect to the VPN from the router.

If it is necessary to hide encrypted data more securely, it is advisable to use TrueCrypt (or VeraCrypt). Currently, the creators of Tails recommend using cryptsetup, based on LUKS. This program allows you to create hidden partitions, but this section is not hidden until the end. It is possible to detect the title of a hidden partition, which allows you to determine its presence. The title of the hidden TrueCrypt section is indistinguishable from random data, and, as far as we know, it is impossible to detect it (plausible deniability) [44].

When started, Tails synchronizes the system clock. If this detects a significant time difference, Tor Browser stops working and restarts. From an external observer's point of view, this behavior can be used to identify Tails users, mainly because synchronization occurs every time the system is started.

2.5.3 Whonix and Tails comparsion

Both systems are based on Debian and use Tor Browser. In general, Whonix is more intended for installation on a regularly used PC, while Tails is more like a "travel" tool that allows you to anonymously access the Internet from someone else's PC. Below are some of the differences.

Table 1 – comparison of two operating systems

	Whonix	Tails
Type	General purpose OS available as VM images and normal install	Live DVD or Live USB
Can run in VirtualBox	Yes	Yes, but not recommended
IP/DNS protocol leak protection	Full, except for the case of exploit against Whonix-Gateway	Leakage is possible with system software bugs or virus infection
Cold Boot Attack Protection	No	Yes
VPN support	Yes, well-documented	No
Hides your MAC address from local LAN	No	Yes
Gateway and “torify” any operating system	Yes	No
Ability to visit sites directly, bypassing Tor	No, but you can use your usual browser on the host	Yes, via a special browser

2.6 Specificity of anonymous behavior

The anonymous use of the Internet is rarely limited to viewing web pages, it can include registration on any sites, publication of texts, communication on forums, communication via e-mail or Jabber, etc. without loss of anonymity. In such situations, technical anonymity becomes insufficient; there is a need to prevent information leakage from user itself. Not all users may need such security measures. First of all, when creating an alternative person, you should remember that it should not intersect with the real identity even indirectly.

- Assess the level of trust in the resource on which the profile is registered.
- If possible, use a temporary e-mail address (Dropmail, 10MinuteMail) or a permanent one, but specially created in an anonymous session.
- Do not disclose the date of birth or provide incorrect information.
- In cases where it is necessary to specify a name and surname, one should not make them excessively exotic or absurd, so as not to attract additional attention.

- Sometimes it is advisable to specify a real city of residence in order to make the profile more believable. Otherwise, in the process of communication, it can be seen that the anonymous person practically does not know the city in which he allegedly resides. If there is no need to specify a city, then it is not necessary to do this. If possible, do not disclose geographic data, including the time zone.
- "Multi-nick": you should use different nicknames in different places, if there is no explicit desire to identify yourself as the same person.
- "Cross-posting": do not publish the same texts and links to them from different profiles [45].
- The style of speech can talk about the level of education, professional skills, etc.
- Characteristic speech, "key phrases," repeated mistakes in speech can indicate the relationship of two profiles or even a real person.
- When registering in anonymous networks, do not use your nicknames from the "regular" Internet.
- Be sure to delete the metadata from the sent files, for example, EXIF from the photos, the user name from the documents. The received files from unknown persons should be treated with extreme caution [27]. For example, images obtained from an unverified source can contain a steganographic tag. If you plan to publish them anywhere from another profile, it makes sense to recode them with losses.
- The time of publication of messages can localize the main pastime.
- In an anonymous work session, user should not visit accounts associated with a real person, especially in social networks. Even if the profile does not contain real data, but it was created with a non-anonymous connection, this profile is already unsafe. Conversely, in normal work without anonymization, do not enter an anonymous account.
- In some cases, especially on low-bandwidth resources, the commonality of several anonymous connections becomes apparent from a simple logical consideration: if several unknown users with a rare browser fingerprint have entered in a short period of time, most likely, the user is one and the same [16].

• When copying text from a website, it is worth checking it for hidden (nonprinting) characters [46].

Summary: there is a significant amount of software aimed at ensuring anonymity and privacy. Modern means can achieve a high level of security, but it is always dependent on the human factor. The most powerful concealment tool is Tor and anonymous operating systems based on it. VPN services are less secure, but more convenient to use. Connecting to a VPN via Tor has both advantages and disadvantages.

Приложение Б

Содержимое файла конфигурации сервера OpenVPN

```
port 443
proto tcp
dev tun
server 10.8.0.0 255.255.255.0
push "redirect-gateway def1 bypass-dhcp"
topology subnet
max-clients 200

ca ca.crt
cert server.crt
key server.key
dh none
tls-crypt tc.key
crl-verify crl.pem

mssfix 0
client-to-client
push "dhcp-option DNS 10.8.0.1"
ping 10
ping-restart 120
push "ping 10"
push "ping-restart 120"
persist-tun
cipher AES-256-GCM
tls-version-min 1.2
ncp-ciphers AES-256-GCM:AES-256-CBC
tls-cipher TLS-ECDHE-ECDSA-WITH-CHACHA20-POLY1305-SHA256:TLS-ECDHE-
ECDSA-WITH-AES-256-GCM-SHA384
auth SHA512
remote-cert-tls client
tls-server

status-version 2
script-security 2
sndbuf 393216
rcvbuf 393216
reneg-sec 2592000
hash-size 1024 1024
verb 3
mute 3
replay-window 128
compress
log /dev/null
```

Приложение В

Содержимое файла конфигурации клиента OpenVPN

```
client
dev tun
dev-type tun
remote 185.141.27.70 443 tcp
nobind
persist-tun
cipher AES-256-GCM
tls-cipher TLS-ECDHE-ECDSA-WITH-CHACHA20-POLY1305-SHA256:TLS-ECDHE-ECDSA-WITH-AES-256-GCM-SHA384
auth SHA512
verb 4
mute 10
mssfix 0
ping 10
ping-restart 120
hand-window 70
server-poll-timeout 4
reneg-sec 2592000
sndbuf 393216
rcvbuf 393216
remote-cert-tls server
tls-client
compress
block-outside-dns
script-security 2
auth-nocache
<ca>
# -----CERTIFICATE-----
</ca>
<tls-crypt>
# OpenVPN static key
</tls-crypt>
<cert>
# -----CERTIFICATE-----
</cert>
<key>
# -----PRIVATE KEY-----
</key>
```

Полный клиентский профиль (файл .ovpn с сертификатами), пригодный для подключения к VPN-серверу, прилагается на CD.

Приложение Г

Параметры конфигурации браузера Firefox

privacy.resistFingerprinting = true – активировать некоторые возможности противодействия отслеживанию, заимствованные из Tor Browser (в данной работе это было нежелательно, поскольку некоторые отпечатки в таком режиме идентичны отпечаткам Tor Browser, например, Canvas fingerprint).

privacy.firstparty.isolate = true – политика First Party Isolation также заимствована из Tor, это блокировка стороннего контента, в том числе Cookies, которые не относятся напрямую к вызываемой странице. Может вызвать проблемы с некоторыми сайтами.

browser.safebrowsing.enabled = false

browser.safebrowsing.downloads.enabled = false

browser.safebrowsing.malware.enabled = false – отключение Safe browsing, что в теории увеличивает риск заражения, но прежде всего отключает отправку информации о всех посещаемых сайтах и закачанных файлах на ресурсы Google и Mozilla.

browser.search.suggest.enabled = false – отключает передачу текста, набираемого в окне поиска, поисковой системе без явного подтверждения запроса со стороны пользователя.

dom.enable_performance = false – отключить передачу браузером информации о времени начала и окончания загрузки страницы.

network.dns.disablePrefetch = true – запретить предварительное разрешение имён для всех ссылок на веб-странице.

dom.battery.enabled = false – не отслеживать уровень заряда батареи.

dom.network.enabled = false – не определять параметры соединения с сетью (при этом передаётся тип соединения).

media.peerconnection.enabled = false – запретить поддержку WebRTC, для защиты от утечки IP-адреса. Альтернатива: опция «Предотвратить утечку локального IP-адреса через WebRTC» в расширении uBlock.

geo.enabled = false – отключение геолокации.

media.navigator.enabled = false

media.navigator.video.enabled = false — отключение взаимодействия с микрофоном и камерой.

media.navigator.streams.fake = true — режим генерирования тестового аудио и видеосигнала, подменяющих реальный сигнал от камеры и микрофона.

webgl.disable-extensions = true

webgl.min_capability_mode = true – ограничение функций WebGL, запрещает передачу сайтам подробной информации о графических возможностях системы. Можно отключить WebGL и полностью (webgl.disabled=true) или блокировать его с помощью NoScript, разрешая при необходимости.

privacy.trackingprotection.enabled = true – активировать защиту от отслеживания. В настоящее время эта функция доступна в обычных настройках, либо можно использовать для этой цели uBlock с дополнительными фильтрами (EasyPrivacy, Merged Ultimate List).

general.useragent.override = <строка> – подмена User-agent вручную (но для этого удобнее использовать расширения).

dom.webaudio.enabled = false – отключение AudioContext API (на данный момент уже существуют дополнения для борьбы с Audio fingerprinting).

layout.css.visited_links_enabled = false – не выделять посещённые ссылки.