

Санкт-Петербургский государственный университет

Кафедра системного программирования

Группа 21.Б11-мм

Разработка технологий для реализации “цифрового почерка” абонента

Задорожный Александр Сергеевич

Отчёт по учебной практике
в форме «Производственное задание»

Научный руководитель:
д.ф.-м.н., проф. каф. СП А.Н. Терехов

Консультант:
главный конструктор ООО «ЛИС» В.О. Аксенов

Санкт-Петербург
2024

Оглавление

Введение	3
1. Постановка задачи	5
2. Обзор	6
2.1. Виды цифрового почерка	6
2.2. Существующие аналоги	9
2.3. Методы классификации сетевого трафика	11
2.4. Используемые технологии	13
3. Архитектура системы	15
3.1. Обработка начальных данных	15
3.2. Цифровой почерк на уровне радио интерфейса	16
3.3. Цифровой почерк на сетевом уровне	20
3.4. Целостная система	26
4. Реализация	28
4.1. Наборы данных	28
4.2. Мессенджер IVA	31
4.3. Мессенджер Telegram	37
4.4. Внедрение реализованных моделей в существующие инструменты	42
Заключение	45
Список литературы	47

Введение

В современном информационном обществе, с увеличением влияния цифровых технологий в различных сферах жизни, вопросы безопасности и надежной идентификации пользователя в интернете приобретают все большую значимость. Развитие таких областей, как интернет вещей¹ и увеличение объемов онлайн-транзакций², делает необходимым постоянное усовершенствование методов защиты и верификации личных данных. Это в свою очередь, требует интеграции различных технологий, включая элементы биометрии и машинного обучения, для повышения надежности и точности идентификации. В этом контексте, концепция цифрового почерка абонента выступает как одно из перспективных направлений, предлагая новые подходы к обеспечению кибербезопасности.

“Цифровой почерк” представляет собой уникальный набор поведенческих характеристик пользователя, таких как стиль взаимодействия с пользовательским интерфейсом, образцы движения мыши и другие параметры, которые могут быть использованы для повышения безопасности в компаниях. Внедрение системы “свой-чужой” на основе анализа цифрового почерка позволяет выявлять необычное или подозрительное поведение даже после того, как устройство прошло техническую и физическую проверку. Т. е. если поведение отклоняется от установленной нормы, система может автоматически инициировать дополнительные меры безопасности, включая временную блокировку доступа пользователя к корпоративным ресурсам. Такой подход обеспечивает дополнительный слой безопасности, позволяя предотвращать внутренние угрозы и атаки, основанные на украденных учетных данных [54, 55].

Переходя от общей концепции цифрового почерка к более узкому фокусу на анализе сетевого трафика, становится ясно, что данное направление позволяет выделить большое количество уникальных характеристик, которые могут быть ключевыми в идентификации конечно-

¹Statista: Internet of Things — Worldwide [Электронный ресурс]. (Дата обращения 10.11.2023)

²Statista: Digital Payments — Worldwide [Электронный ресурс]. (Дата обращения 10.11.2023)

го пользователя. Именно анализ сетевого трафика, на различных его уровнях, позволяет глубоко понять индивидуальные особенности поведения человека в интернете, что является особенно актуальным в условиях растущего количества сетевых взаимодействий и необходимости обеспечения высокой степени безопасности в цифровом пространстве [10, 14, 27, 34, 47, 48, 49]. Это подводит к сути проекта, т. е. создание комплексной системы идентификации личности, основанной на анализе цифрового почерка абонента, объединяющей поведенческие и сетевые характеристики для обеспечения высокоуровневой безопасности и точной верификации пользователя в цифровом мире.

Эта система разрабатывается с целью быть универсальной, чтобы она могла применяться в широком спектре компаний, охватывая подавляющее большинство сценариев использования. В данной работе будет представлена конкретные реализации продукта на нескольких примерах, а именно корпоративном мессенджере IVA³ и Telegram. Они демонстрируют свою эффективность и адаптивность в конкретных бизнес-контекстах. Кроме того, будет описана общая схема интеграции разработанного инструмента с существующим продуктом компании ООО “Мобил-груп”, который предназначен для анализа сетевого трафика. Это позволит понять, как новая система может усиливать и дополнять уже существующие механизмы анализа и безопасности, обеспечивая более глубокий и многоуровневый подход к защите данных и идентификации пользователя.

³Корпоративный мессенджер IVA [Электронный ресурс]. (Дата обращения 05.10.2023)

1. Постановка задачи

Целью работы является разработка и внедрение технологий для реализации цифрового почерка абонента, предназначенных для улучшения безопасности и идентификации пользователей в корпоративных сетях и приложениях, с помощью передовых методов машинного обучения и анализа поведенческих данных. Для её выполнения были поставлены следующие задачи.

1. Изучение существующих алгоритмов и техник распознавания поведенческих паттернов пользователей, включая анализ клавиатурного ввода, стилей взаимодействия с интерфейсом и прочих уникальных характеристик.
2. Разработка методов сбора и анализа как сетевых, так и радио данных, включая временные метки, частоту запросов, паттерны использования устройств и приложений.
3. Разработка архитектуры системы, способной адаптироваться к различным корпоративным средам и приложениям. А также ее апробация на примере мессенджеров IVA и Telegram
4. Обучение моделей для распознавания активности и пользователей. Сюда входит как подготовка обучающих данных, включая разметку и пред обработку для эффективного обучения моделей, так и настройка моделей для повышения точности и надёжности в идентификации индивидуального цифрового почерка.
5. Интеграция разработанного инструмента в существующие корпоративные системы ООО “Мобил-груп”, предоставляющие инструменты анализа сетевого трафика и безопасности.

2. Обзор

В данном разделе представлен обширный анализ текущего состояния и перспектив развития технологий, связанных с идентификацией и верификацией личности в цифровой среде. Особое внимание уделено изучению различных видов цифрового почерка, их уникальных характеристик и приложений в различных сферах. Рассматриваются существующие аналоги и решения, уже применяемые в индустрии, что позволяет оценить текущее состояние технологий и выявить потенциальные возможности для дальнейшего развития. Кроме того, проанализированы методы классификации сетевого трафика, которые играют ключевую роль в определении и анализе цифрового почерка, особенно в контексте повышения безопасности и точности идентификации в условиях постоянно изменяющейся сетевой среды. И, наконец, освещаются используемые технологии, что дают комплексное представление о том, как различные инструменты взаимодействуют для создания эффективных систем идентификации личности.

2.1. Виды цифрового почерка

В первую очередь рассмотрим клавиатурный почерк пользователя [25]. Он основан на анализе уникальных поведенческих характеристик при вводе данных на клавиатуре, включая скорость набора, ритм, интервалы времени между нажатиями клавиш и время их удержания. Эти факторы обеспечивают уникальность клавиатурного почерка, делая его важным инструментом в задачах безопасности [56, 51]. Однако потенциальная нестабильность характеристик и возможность подделки при достаточно детальном изучении стиля набора текста требуют постоянной корректировки и обновления эталонных моделей для обеспечения точной идентификации.

Далее стоит обратить внимание на динамику работы с манипулятором “мышь” [53]. Анализируя скорость движения курсора, паттерны нажатий и общее взаимодействие с мышью, можно выявить уникальные особенности, которые служат ценным инструментом для идентифика-

ции личности. Этот вид цифрового почерка ценится за его способность предоставлять детальную информацию о пользователе, что делает его подделку сложной задачей [52]. Однако, несмотря на эти преимущества, данный метод имеет и недостатки. Влияние внешних факторов, таких как физическое состояние пользователя [37] или использование различных устройств ввода, может влиять на точность и стабильность динамики работы с мышью, а следовательно привести к ошибкам в идентификации. Кроме того, этот метод требует специального программного обеспечения для сбора и анализа данных, что может ограничивать его применение в некоторых средах.

Идентификация пользователей смартфонов на основе их взаимодействия с устройством [20, 29, 21] является передовым методом в области цифровой идентификации. Она включает анализ данных акселерометра, геолокации, GPS, а также наблюдение за тем, как пользователи кладут свой телефон на стол или держат его в руках. Эти параметры предоставляют обширный набор поведенческих данных, способствуя точной идентификации, затрудняя процесс имитации уникальных характеристик пользователя. Однако, существуют недостатки данного метода. Изменения в поведении пользователя, вызванные, например, травмами рук или изменением привычек использования [37, 18], могут снижать точность идентификации. Кроме того, вопросы приватности и сбора данных могут вызывать опасения среди пользователей, требуя баланса между точностью идентификации и защитой личных данных [19].

Биометрия, включающая идентификацию по отпечаткам пальцев, распознавание лица и другие физиологические характеристики, считается одной из самых надежных форм идентификации [43, 4]. Она широко используется в различных сферах, от безопасности доступа до транзакционных систем. Однако, помимо риска компрометации биометрических данных, существуют и другие недостатки. Ключевым из них является необходимость постоянного подтверждения личности, особенно в динамичных средах, где требуется частый доступ к защищенным ресурсам. Это может создавать неудобства для пользователей и требовать наличия непрерывного доступа к биометрическим устройствам.

Кроме того, проблемы с функционированием или доступностью этих устройств могут привести к сложностям в обеспечении стабильного и надежного доступа к защищенным системам или услугам.

Идентификация устройств на основе радио интерфейса представляет собой перспективный и активно развивающийся подход в современных исследованиях [47, 34, 27, 46, 44, 15]. Данная технология позволяет не только определять класс устройства, но и, при наличии достаточного объема данных, идентифицировать конкретную модель с высокой точностью. Ключевым преимуществом является возможность непрерывного мониторинга активности устройств в сети, что достигается благодаря специализированному оборудованию, производимому компанией ООО “Мобил-групп”. Наличие доступа к такому оборудованию, позволяет напрямую считывать данные с ядра сети и открывает новые горизонты для анализа поведения различных устройств в динамике. Однако несмотря на высокую эффективность цифрового почерка на уровне радио интерфейса, данный подход будет рассмотрен в работе как дополнение к более высокоуровневому методу идентификации, рассмотренному далее.

Последний вид цифрового почерка, основывается на анализе сетевого трафика [35]. Данный способ является ключевым элементом в современных методах идентификации. Он включает изучение паттернов использования интернета, предпочтений в веб-поиске и общих поведенческих особенностей пользователя [40]. В современном мире, где интернет стал неотъемлемой частью жизни большинства людей и компаний [8], этот подход приобретает особую актуальность. Он позволяет точно идентифицировать “своих” и “чужих” в цифровом пространстве, обеспечивая высокий уровень безопасности. Одним из главных преимуществ анализа сетевого трафика является его способность непрерывно собирать и обновлять данные, оставаясь незаметным для пользователя [17]. Это обеспечивает постоянное обновление информации о поведенческих паттернах, увеличивая точность идентификации.

Таким образом, в условиях глобализации и всё более тесной интеграции бизнеса и личной жизни с интернетом, анализ сетевого трафика

на нескольких уровнях одновременно становится одним из самых эффективных способов обеспечения безопасности и контроля доступа. Это делает его важным инструментом в арсенале современных методов кибербезопасности.

2.2. Существующие аналоги

В первую очередь стоит обратить внимание на системы анализа сетевого трафика (Network Traffic Analysis, NTA) [22], которые предназначены для перехвата потоков данных и обнаружения признаков сложных, чаще всего целевых атак (APT). С их помощью можно проводить ретроспективное изучение сетевых событий, обнаруживать и расследовать операции злоумышленников в информационной инфраструктуре предприятия, а также эффективно реагировать на соответствующие происшествия [1]. Решения класса NTA отслеживают трафик и коммуникации внутри корпоративной сети и применяют различные техники (поведенческий анализ, машинное обучение) для того, чтобы быстро обнаружить, проанализировать и обработать угрозы, которые в противном случае оставались бы скрытыми. NTA может применяться в сетях любого масштаба, равно как и любой архитектуры: локальной, облачной, гибридной.

В 2019 году компания Gartner проводила исследование решений класса Network Traffic Analysis⁴. Результаты сосредоточены в отчёте «Market Guide for Network Traffic Analysis», согласно которому на сегодняшний день на мировом рынке выбор поставщиков на мировом рынке NTA-решений весьма велик. Однако для решения непосредственно нашей задачи стоит рассматривать представителей рынка, которые специализируются на анализе трафика с использованием таких технологий для обнаружения угроз внутри сети, как машинное обучение, правила детектирования, индикаторы компрометации, глубокая аналитика. Среди всех инструментов можно выделить следующих игроков: Awake Security Platform [3], Bricata [6], Cisco Stealthwatch [9], Corelight

⁴Market Guide for Network Traffic Analysis [Электронный ресурс]. (Дата обращения 18.11.2023)

Sensor [11], Corvil Security Analytics [12], и др. Хотя изучив данные инструменты более детально, стоит отметить, что все эти решения эффективны в поиске подозрительных или вредоносных данных в сети, однако они оказываются бессильными, когда речь идёт об отслеживании подозрительной активности со стороны сотрудника компании, который собирает или наблюдает за потоками данных, не имея к ним доступа. Это подчеркивает необходимость разработки решений, способных распознавать и предотвращать такие виды инсайдерских угроз. Аналогичная ситуация наблюдается и на российском рынке: PT Network Attack Discovery (Positive Technologies) [31], Threat Detection System (Group-IB) [38], Kaspersky Anti Targeted Attack («Лаборатория Касперского») [24], Гарда Монитор («Гарда Технологии») [50].

После тщательного рассмотрения существующих промышленных решений и не находя в них подходящих вариантов, стоит перейти к изучению академических исследований в области науки, которые могут предложить новые перспективы и подходы к поставленной задаче. На сегодняшний день проведено множество исследований по теме классификации сетевого трафика [23, 30, 7, 33]. Однако большинство из них сосредоточились на классификации семейства протоколов, также известного как характеристика трафика (например, потоковая передача, чат, P2P и т. д.) либо на идентификации отдельного приложения, которая известна как идентификация приложения (например, Spotify, Hangouts, BitTorrent и т. д.) [26, 16].

Таким образом, на текущий момент не было обнаружено работ, направленных непосредственно на составление цифрового почерка через сетевой трафик с целью обеспечения кибербезопасности и создания системы «свой-чужой». А значит остаётся значительный потенциал для развития в этом направлении. Если сосредоточить усилия не на классификации протоколов или идентификации приложений, а на анализе действий, которые пользователи выполняют в этих приложениях, можно достичь более глубокого понимания поведения пользователя. Это откроет возможности для создания уникального цифрового почерка каждого человека, взаимодействующего с программой, что будет спо-

способствовать повышению уровня кибербезопасности и эффективности системы различения “своих” и “чужих”.

2.3. Методы классификации сетевого трафика

В этом разделе приводится обзор наиболее важных методов классификации сетевого трафика. В частности, данный подход можно разделить на три основные категории следующим образом: (i) основанные на портах, (ii) проверка полезной нагрузки и (iii) статистическое и машинное обучение. Ниже приведен краткий обзор наиболее важных и недавних исследований, касающихся каждого из вышеупомянутых подходов.

Подход, основанный на портах: Классификация трафика по номеру порта является старейшим и наиболее известным методом решения этой задачи [14]. Классификаторы на основе портов используют информацию в заголовках TCP/UDP пакетов для извлечения номера порта, который, как предполагается, связан с конкретным приложением или действием [32]. Классификация на основе портов, как известно, является одним из самых простых и быстрых методов идентификации сетевого трафика. Однако повсеместное использование обфускации портов, преобразования сетевых адресов (NAT), переадресации портов и другие техники значительно снизило точность этого подхода. Согласно [30, 28], только от 30% до 70% текущего интернет-трафика может быть классифицировано с использованием методов классификации на основе портов. Потому что по вышеупомянутым причинам для классификации современного сетевого трафика необходимы более сложные методы классификации трафика.

Большинство методов проверки полезной нагрузки, также известных как глубокая проверка пакетов (DPI), используют предопределенные шаблоны, такие как регулярные выражения, в качестве подписей для каждого протокола [13, 36]. Производные шаблоны затем используются для отличия протоколов друг от друга. Необходимость обновления шаблонов всякий раз, когда выпускается новый протокол, и проблемы конфиденциальности пользователей являются

одними из наиболее важных недостатков этого подхода. И хотя в работе [5] была предложена новая система DPI, которая может проверять зашифрованную полезную нагрузку без расшифровки, таким образом решив проблему конфиденциальности пользователей проблема, но он может обрабатывать только защищенный HTTP (HTTPS) трафик.

Статистический подход и подход к машинному обучению: Статистический подход включает в себя следующие два основных метода.

1. **Простые и сложные статистические методы:** Эти методы основаны на предвзятом предположении, что базовый трафик для каждого приложения обладает некоторыми статистическими характеристиками, которые практически уникальны для каждого приложения. Каждый статистический метод использует свои собственные функции и статистику. В статье [41] предложили идентифицировать отпечатки протоколов, основываясь на функции плотности вероятности (PDF) времени между поступлениями пакетов и нормализованных пороговых значениях. Они достигли точности до 91% для группы протоколов, таких как HTTP, Post Office Protocol 3 (POP3) и Simple Mail Transfer Protocol (SMTP). В аналогичной работе [45] рассматривался формат PDF и размер пакета. Их схема позволила идентифицировать более широкий спектр протоколов, включая протокол передачи файлов (FTP), протокол доступа к интернет-сообщениям (IMAP), SSH и TELNET с точностью до 87%.
2. **Методы, основанные на машинном обучении:** Для классификации трафика было опубликовано огромное количество подходов к машинному обучению. Например, в [2] предложили байесовскую нейронную сеть, которая была обучена классифицировать наиболее известные протоколы P2P, включая Kazaa, BitTorrent, GnuTella, и достигли точности 99%. Были предложены подходы с применением искусственных нейронных сетей (ANN) для идентификации трафика [42, 39]. Более того, в [39] было показано,

что подход ANN может превзойти наивные байесовские методы. Наиболее важной статьёй, опубликованной с использованием набора данных “VPN-nonVPN dataset (ISCXVPN2016)”, является работа [7]. В ней для обучения были использованы параметры связанные со временем, такие как продолжительность потока, количество байтов потока в секунду, время прямого и обратного взаимного поступления и т. д. Для распознавания сетевого трафика использовали метод k-ближайших соседей (k-NN) и алгоритмы деревьев принятия решений. Они достигли примерно 92% точности, характеризуя шесть основных классов трафика, включая просмотр веб-страниц, электронную почту, чат, потоковую передачу, передачу файлов и VoIP.

Исходя из обширного обзора различных подходов и методов, представленных выше, было принято решение ориентироваться на те, что основываются на машинном обучении. Они показывают хорошую точность и высокую эффективность в классификации сетевого трафика. Однако, в рассматриваемой задаче фокус будет смещен, как отмечалось в подразделе 2.2, с определения конкретных приложений на идентификацию активности из ранее определенной группы или же конкретного пользователя, соответствующего определенному паттерну.

2.4. Используемые технологии

1. **Python==3.10.10** — интерпретируемый, интерактивный, объектно-ориентированный язык программирования. Он включает в себя модули, динамические типы данных очень высокого уровня и классы.
2. **Scikit-learn==1.3.0** — открытая библиотека машинного обучения для языка программирования Python. Она предоставляет простой и эффективный инструментарий для решения разнообразных задач машинного обучения, включая классификацию, регрессию, кластеризацию, обучение с учителем и без учителя, а также

предварительную обработку данных.

3. **PyTorch==2.2.0** — открытая библиотека машинного обучения для языка программирования Python. Данная библиотека предоставляет мощные возможности для работы с тензорами и построением нейронных сетей. PyTorch используется как в исследовательских, так и в производственных целях, предлагая гибкость и высокую производительность для широкого спектра задач машинного обучения, включая компьютерное зрение, обработку естественного языка и многое другое.
4. **Numpy==1.24.3, Pandas==2.0.3** — это ключевые инструменты в экосистеме Python для работы с данными и выполнения вычислений. Они предоставляют мощные функциональности и структуры данных, упрощая анализ и манипуляции с данными.
5. **FastAPI==0.104.0** — это современный, быстрый (высокопроизводительный) веб-фреймворк для создания API с использованием современных практик разработки, который полностью соблюдает стандарты для документации и взаимодействия с API.

3. Архитектура системы

В данном разделе представлено подробное описание компонентов и функциональности системы, разработанной для верификации пользователей на основе анализа их поведения в сети. Этот раздел является ключевым для понимания того, как различные элементы системы взаимодействуют друг с другом для обеспечения надежной идентификации пользователя. Первая часть раздела посвящена описанию способа сбора наборов данных, для анализа которых и строится вся дальнейшая система по распознаванию активности пользователя. Во второй части раздела рассматривается обработка данных, полученных с радио интерфейса базовых станций. Здесь описывается как система анализирует трафик нижнего уровня для определения класса, к которому принадлежит устройство пользователя. Третья часть описывает процесс формирования долгосрочных поведенческих моделей для создания профиля цифрового почерка пользователя. Система учитывает различные аспекты поведения, такие как частота, время активности и предпочтения в использовании определенных сервисов. И, наконец, в последней части приведена общая архитектура всей системы. Она представляет собой комплексное решение, включающее сбор данных, их обработку (обработчики событий) и анализ, а также механизмы реагирования на обнаруженные угрозы.

3.1. Обработка начальных данных

Перед разработкой любой системы с применением искусственного интеллекта критически важно уделить первостепенное внимание сбору и обработке исходных данных. При работе с данной задачей обычно данные представлены в формате pcap (Packet Capture). Этот формат является широко применяемым стандартом в области сетевых технологий и используется для записи сетевых пакетов. Они могут содержать обширную информацию о сетевых взаимодействиях, включая, но не ограничиваясь, передачей данных между различными IP-адресами пользователей и многим другим.

Для получения же собранных данных необходимо организовать канал связи между ядром базовой станции и системой обработки данных. Для этого, например, можно использовать инструмент `socat`, который позволяет перенаправлять данные между различными типами каналов, включая TCP-соединения, Unix-сокеты и последовательные порты. Полученные данные будут сохранены в хранилище, а после чего будут переданы на следующие этапы обработки, такие как извлечение признаков и построение моделей машинного обучения.

Однако в первую очередь, пока у нас еще нет обученной системы, необходимо вручную подготовить и структурировать имеющуюся информацию в формат CSV, содержащий такие поля как идентификатор (IMSI или IP, в зависимости от уровня), имя файла и тип активности (либо класс устройства), который был использован во время записи pcap (табл. 1).

ID	Имя файла	Действие
id1	file1.pcap	act1
id2	file2.pcap	act2
id3	file3.pcap	act3
id4	file4.pcap	act4
id5	file5.pcap	act5

Таблица 1: Пример csv файла после этапа сбора данных

3.2. Цифровой почерк на уровне радио интерфейса

Одним из ключевых аспектов данной работы является анализ характеристик устройств (User Equipment — UE) на уровне радио интерфейса.

Хотя на этом уровне невозможно напрямую идентифицировать конкретного абонента, мы можем наблюдать за различными параметрами устройств, такими как LCID (Logical Channel ID) на уровнях MAC/RLC⁵. Эти данные могут служить ценным источником информации для по-

⁵4G/LTE — MAC Standart [Электронный ресурс]. (Дата обращения: 05.02.2024)

строения уникального цифрового почерка пользователя. В первую очередь, стоит отметить почему был выбран именно LCID⁶. На выбор данной характеристики оказал влияние целый ряд причин.

- LCID разделяются на те, что используются в направлении Downlink, и те, что используются в направлении Uplink. При этом LCID разных направлений могут иметь одинаковый номер, но при этом содержать совершенно разную информацию.
- LCID могут содержать полезные данные (данные пользователя) и служебные данные (MAC CE). Подробнее на рис. 1.
- Существуют разные Release одного и того же стандарта и с каждым последующим Release появляются новые виды сообщений (новые номера LCID).
- Разные виды устройств поддерживают разные Release и соответственно отличаются по видам доступных LCID.

mac_lte_rnti	mac_lte_sfn	mac_lte_subframe	mac_lte_dlch_lcid	Frame Number	Time since reference or first frame
3	391	0		1	0.000000000
61	391	7		2	0.003334000
61	392	1	UE Contention Resolution Identity, CCCH, Padding	3	0.014415000
61	395	2		4	0.014458000
61	395	6	1, Padding	5	0.049278000
61	395	9	1	6	0.049311000
61	399	2		7	0.052385000
61	445	9	Timing Advance, Padding	8	0.089447000
61	496	4	Timing Advance, Padding	9	0.552305000
61	501	2		10	1.057319000
61	501	6	1, Padding	11	1.109333000
61	501	9	1, Padding	12	1.109358000
61	505	2		13	1.112243000
61	546	5	Timing Advance, Padding	14	1.149340000
61	575	2		15	1.558210000
61	575	6	1, Padding	16	1.849244000
61	575	7		17	1.849269000

Frame 4: 66 bytes on wire (528 bits), 66 bytes captured (528 bits)
 DLT: 147, Payload: mac-lte-framed (mac-lte-framed)
 MAC-LTE DL-SCH: (SFN=392, SF=1) UEId=1 (UE Contention Resolution Identity) (CCCH:26 bytes) (Padding:remainder)
 [Context (RNTI=61)]
 [DL PHY Context (DL: UEId=1 RNTI=61 DCI Format=1A Res Alloc=2 Aggr_Level=1 MCS=3 RV=0 Res_Block_len=8 HARQ_id=0 NDI=1)]
 MAC-LTE Header (UE Contention Resolution Identity) (CCCH:26) (Padding:remainder) [3 subheaders]
 Sub-header (Lcid=UE Contention Resolution Identity)
 0... = SCH reserved bit: 0x0
 0... = Format2: Data length is < 32768 bytes
 ..1... = Extension: 0x1
 ...1100 = Lcid: UE Contention Resolution Identity (0x1c)
 Sub-header (Lcid=CCCH, length=26)
 0... = SCH reserved bit: 0x0
 0... = Format2: Data length is < 32768 bytes
 ..1... = Extension: 0x1
 ...0 0000 = Lcid: CCCH (0x00)
 0... = Format: Data length is < 128 bytes
 001-1010 = Length: 26
 Sub-header (Lcid=Padding, length is remainder)
 0... = SCH reserved bit: 0x0
 0... = Format2: Data length is < 32768 bytes
 ..0... = Extension: 0x0
 ...1111 = Lcid: Padding (0x1f)
 Contention Resolution (matches Msg3 from frame 3, 0ms ago)
 LTE Radio Resource Control (RRC) protocol
 Padding data: 000000000
 [Padding length: 5]

Рис. 1: Анализ LCID в pcap файле при помощи wireshark

По мере сбора характеристик со все большего кол-ва UE, были выделены следующие классы устройств:

⁶ 4G/LTE — LTE Advanced, Releases [Электронный ресурс]. (Дата обращения: 05.02.2024)

1. Флагман
2. Смартфон
3. Модем
4. Планшет
5. Бюджетное устройство

Однако, стоит отметить, что на уровне радио интерфейса отсутствуют IP-адреса, которые традиционно используются для идентификации пользователей в сетях передачи данных. Это ставит новые задачи и требует разработки специализированных решений для разбиения трафика и сопоставления его с конкретными пользователями. Поэтому был предложен алгоритм решения, описанной выше проблемы. Каждый пакет обладает собственным RNTI, поэтому вся задача сводится к созданию системы определения RNTI относящихся к одному UE:

1. Для начала выбираем все IMSI устройств из рсар файла, которые нас интересуют, либо /all, чтобы выбрать все
2. Рассматриваем все идентификаторы парами
 - RNTI и IMSI
 - RNTI и IMEISV
 - RNTI и MTMSI
3. Получаем тройку связанную по RNTI, т. е. (IMSI, MTMSI, IMEISV) будет являться UE
4. Итерируемся по списку RNTI и mTMSI, где сравниваем mTMSI с MTMSI в списке UE, чтобы понять к какому UE относится этот RNTI

Для упрощения сбора и анализа данных было решено в первую очередь написать консольное приложение(рис. 2), которое позволяет полностью автоматизировано извлекать данные из рсар файлов, которые пишутся на базовой станции.

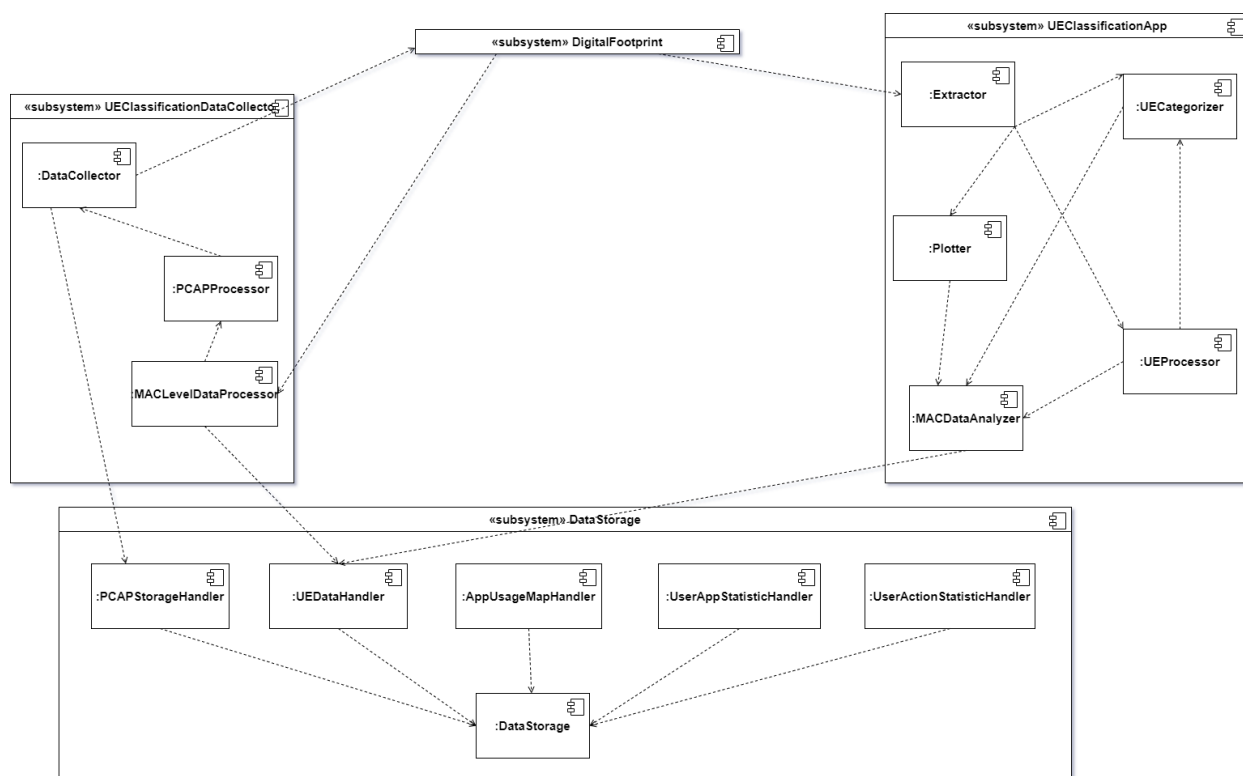


Рис. 2: Диаграмма компонентов для инструмента по классификации класса UE

Активный же сбор данных с разных устройств начался совсем недавно. При этом, как можно заметить по графикам(рис. 3 и 4), классы устройств имеют четкие отличительные признаки, что позволит использовать менее затратные средства для их распознавания.

Таким образом, если рассмотреть ситуацию, когда пользователь меняет свое мобильное устройство, но при этом сохраняет свою SIM-карту, несмотря на изменение аппаратных характеристик, мы можем идентифицировать его. Соединив информацию о цифровом почерке на уровне радио интерфейса с данными о поведении пользователя на уровне сервисов, мы получаем более точную картину его уникального цифрового отпечатка. Более того, можем ответить на дополнительные вопросы, например, почему он решил сменить устройство.

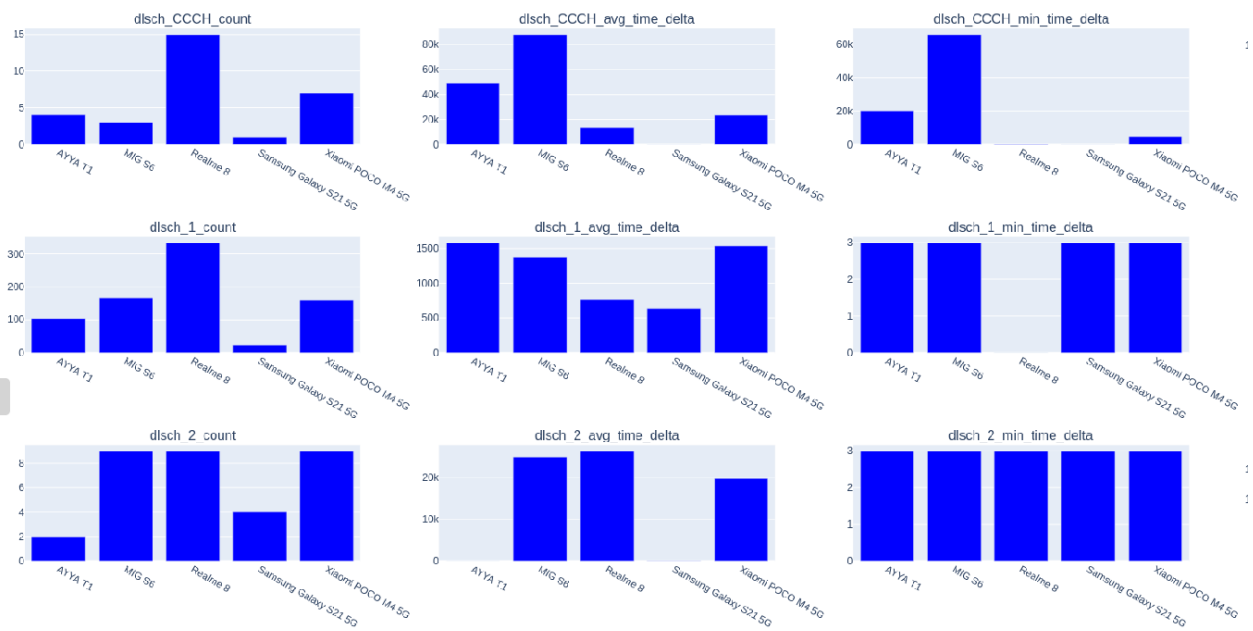


Рис. 3: Пример распределения LCID для отдельных UE

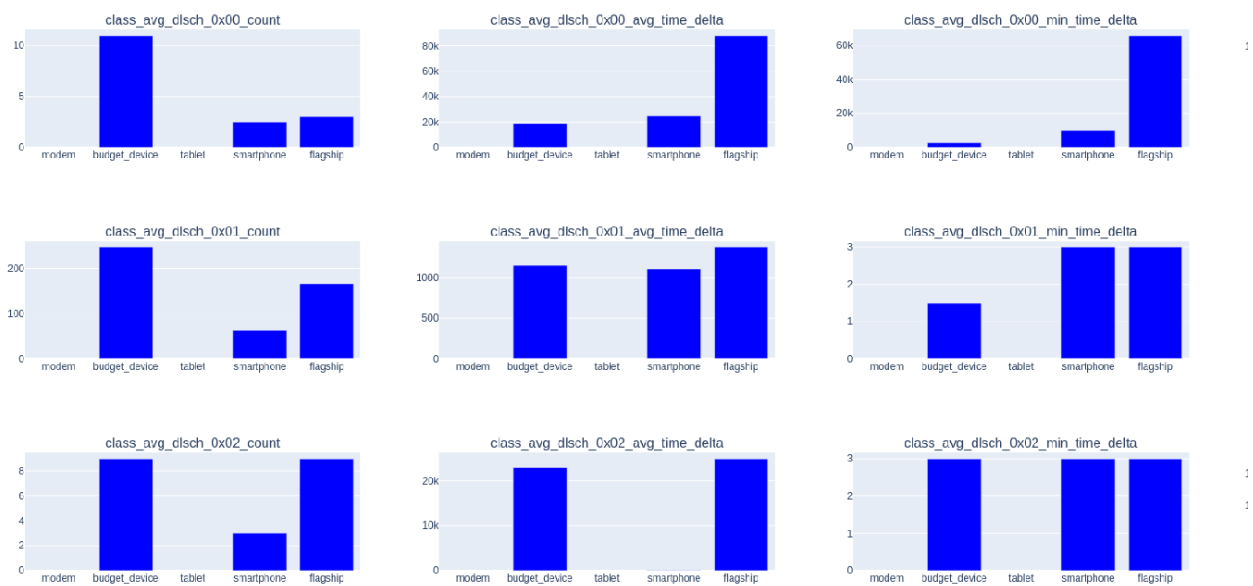


Рис. 4: Пример распределения LCID для класса UE

3.3. Цифровой почерк на сетевом уровне

3.3.1. Карта тяготений (предпочтений) абонентов

Карта тяготений (предпочтений) абонентов представляет собой графическое отображение поведения пользователя в различных приложе-

ниях. Она позволяет визуализировать предпочтения и интересы пользователя, основываясь на его активности в различных сервисах. Эта информация может быть использована для анализа интересов пользователя с целью персонализации контента, а также, что более интересно для поставленной задачи, для опознавания конкретного пользователя или категории, к которой он относится.

Построение такой карты тяготений должно иметь возможность импортировать данные из разных источников. Поэтому инструмент поддерживает обработку как данных, полученных из приложения AppUsage, которое отслеживает использование различных приложений пользователем за большой промежуток времени, так и сетевого трафика в реальном времени (рис. 5).

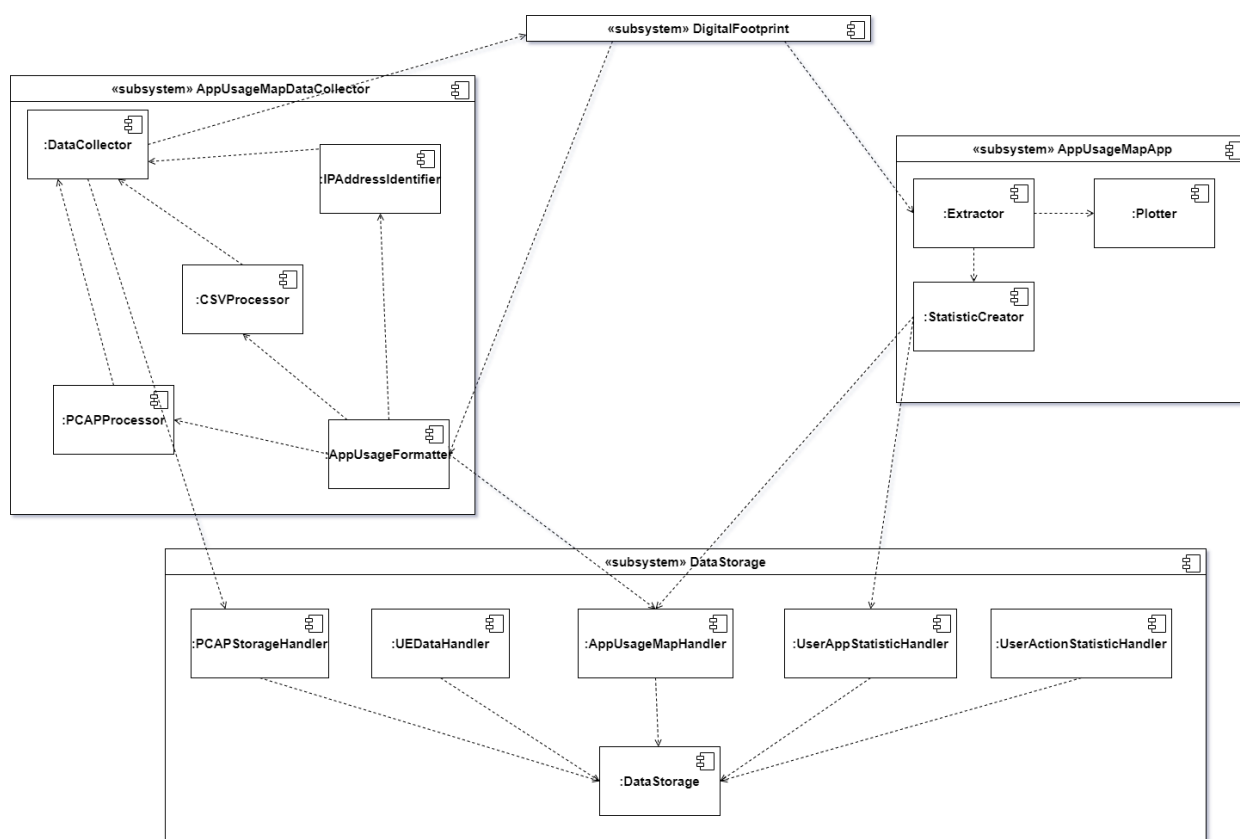


Рис. 5: Диаграмма компонентов для инструмента по построению карты предпочтений

На данный момент инструмент позволяет выделять следующие характеристики для отдельного приложения:

- Общее количество использований приложения;
- Среднее количество использований в день;
- Общая продолжительность использования приложения;
- Процент времени, проведенного в приложении, по отношению к остальным;
- Средняя продолжительность использования приложения;
- Самая продолжительная сессия использования приложения;
- Самая короткая сессия использования приложения;

Также инструмент по построению карты тяготений поддерживает выделение статистики о пользователе в целом за все время наблюдения:

- Количество использованных уникальных приложений;
- Общее время, проведенное во всех приложениях;
- Среднее время, проводимое в приложениях за день;
- Наиболее часто используемое приложение;
- Наименее часто используемое приложение;
- Пиковое время использования приложения;

Пример карты тяготений абонента может выглядеть следующим образом (рис. 6):

включать в себя анализ взаимодействия с интерфейсом приложения, последовательность действий, тип вводимых данных и другие характеристики, которые могут быть учтены при формировании уникального цифрового почерка для каждого пользователя. Распознавание такой активности представляет собой ключевой процесс в рамках разработки передовых технологий, нацеленных на реализацию концепции цифрового почерка абонента. Начинается он как было описано в разделе 3.1 с обработки исходных данных.

В зависимости от конкретного приложения, процесс извлечения признаков для классификации активности может различаться. Однако общая схема обработки рсар файла остается неизменной. Так каждый рсар файл проходит следующие шаги обработки (рис. 7).

1. Разделение рсар файла на временные отрезки.
2. Предобработка данных — выделение tcp/udp статистики, вычисление скорости передачи файлов и др.
3. Сохранение как обработанных характеристик, так и исходных рсар файлов в общее хранилище данных. Отсюда данные могут быть запрошены в любой момент различными элементами системы.

Далее, автономная служба по контролю безопасности с некоторой периодичности обращается к системе, чтобы получить информацию о том, не замечена ли подозрительная активность от некоего пользователя. В этот момент будет запущен следующий механизм (рис. 7):

1. Запрос данных с радио уровня.
2. Отслеживание статуса использования всевозможных приложений и получение общей статистики о каждом из них.
3. Вычисление более подробной информации о действиях в конкретных сервисах. Для этого из хранилища данных отбираются все действия пользователя за некий временной промежуток и отправляются на анализ специализированному ПО.

4. На основе всех полученных данных определяется паттерн поведения пользователя.
5. Сравнение паттерна с более ранними проверками, и если есть значимые отличия — блокировка доступа к системе до удостоверения личности.

В целом, такая последовательность шагов создает комплексный процесс, который позволяет глубоко анализировать и понимать активности пользователя на основе сетевого трафика. Это сочетание предварительной обработки, анализа и пост обработки данных гарантирует, что результаты являются как точными, так и полезными для понимания поведения пользователя.

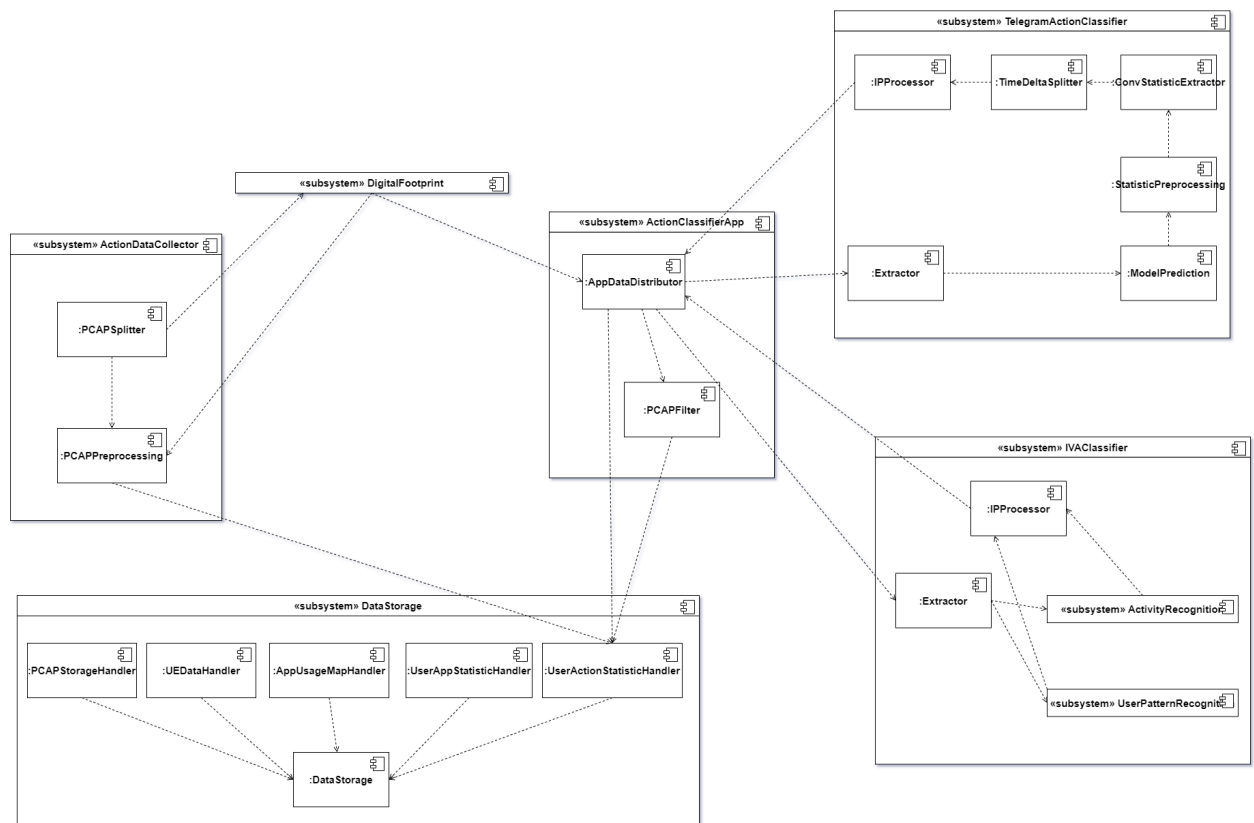


Рис. 7: Диаграмма компонентов для инструмента по распознаванию действий пользователя

3.4. Целостная система

В данном разделе подробно рассматривается как общая архитектура, так и основные функциональные аспекты разработанной комплексной системы, предназначенной для реализации цифрового почерка сетевого трафика абонента. Ниже представлена детальная схема (рис. 8), а после описание ключевых этапов решения.

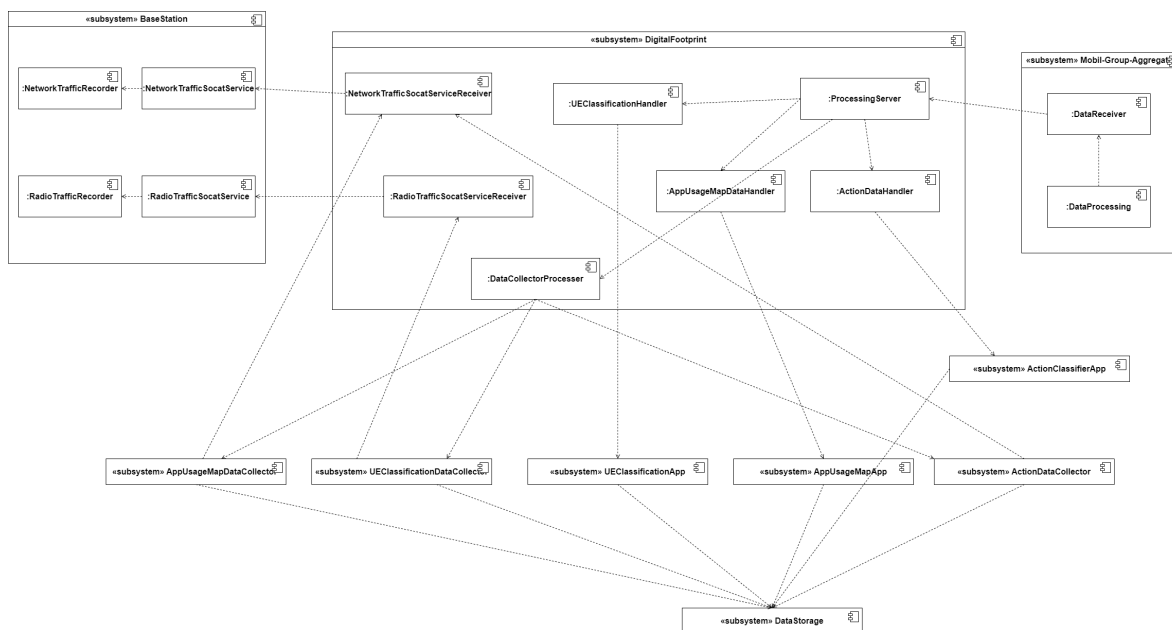


Рис. 8: Высокоуровневая диаграмма компонентов всего продукта

Процесс начинается с получения нескольких больших рсар файлов с разных уровней, которые содержат данные о всей активности в сети за определенный период. После чего необходимо отобрать только те пакеты, которые относятся к реальным пользователям. После чего проверить не появились ли устройства впервые использующие систему. Это позволяет сфокусировать анализ на интересующих абонентов и уменьшить объем данных для обработки.

После этого производится детальный анализ информации, связанной с каждым пользователем. А именно построение карты предпочтений, распознавание активности и паттерна поведения абонента в каждом из отслеживаемых приложений, обученными на предыдущих шагах моделями. В результате инструмент позволяет не только определять, что делает пользователь в данный момент, но и сравнивать получен-

ный паттерн с его обычным поведением. Табл. 2, расположенная ниже, является примером того, как может выглядеть результат работы реализованного инструмента при анализе паттерна поведения в одном из приложений.

В итоге все полученные данные сохраняются в общем файловом хранилище, что позволяет использовать их в дальнейшем анализе. Так, например, для эффективной интеграции с другими web-инструментами анализа трафика будет достаточно создать специализированный сервер, который будет обращаться к уже функционирующим анализаторам. Это позволит легко интегрировать систему распознавания с существующей инфраструктурой без значительных изменений в работе заказчика.

IP Адресс	Действия	ID Пользователя
192.168.202.1	—	—
192.168.202.2	act1 -> act2	1
192.168.202.3	act2	2
192.168.202.4	act2	2
192.168.202.5	act1 -> act4 -> act1	3
192.168.202.6	—	—
192.168.202.7	act1 -> act3 -> act1	3
192.168.202.8	act2 -> act1	2
192.168.202.9	act1	5

Таблица 2: Итоговый результат работы реализованной системы

Таким образом, разработанная система представляет собой мощный инструмент для анализа сетевого трафика, способный обеспечить детальное понимание сетевого поведения абонентов и их идентификацию на основе уникальных характеристик. Однако необходимо подчеркнуть, что эффективная реализация и интеграция этой системы требует тщательного планирования и учета всех аспектов взаимодействия с другими компонентами инфраструктуры кибербезопасности.

4. Реализация

Использование системы “свой-чужой” на основе цифрового почерка при работе с различными корпоративными приложениями значительно скажется на безопасности и сохранности данных компании. Анализируя сетевой трафик и отслеживая почерк абонентов, организации могут гарантировать конфиденциальность, предотвращая несанкционированный доступ и поддерживая целостность корпоративных обсуждений и обмена данными не только на уровне кибератак извне, но и постоянно следить за действиями уже проверенных членов компании, чтобы предотвратить доступ злоумышленников через их аккаунты.

Для подтверждения эффективности описанной в предыдущем разделе структуры инструмента, она была протестирована на реальных мессенджерах, таких как IVA и Telegram. Результаты этих испытаний показали высокую точность идентификации пользователей на основе их уникального цифрового почерка, даже в условиях использования зашифрованных каналов связи. Это открывает новые возможности для обеспечения безопасности корпоративных коммуникаций в эпоху повсеместной цифровизации.

4.1. Наборы данных

4.1.1. Набор данных IVA

Корпоративный мессенджер IVA — это инструмент, предназначенный для облегчения общения внутри организаций. Обычно он позволяет пользователям обмениваться сообщениями, файлами, а также совершать звонки в чатах. Это приложение разработано специально для улучшения совместной работы и производительности в корпоративной среде, предоставляя безопасный и эффективный способ общения между членами команды.

Подробное описание полученных данных представлено в табл. 3. Используемые же для обучения данные в формате pcap были собраны с использованием инструмента tcpdump во время активных сессий непо-

средственно на сервере IVA, развернутом в частной сети ООО “Мобил-груп”. Общее кол-во собранных данных равняется примерно 250 действиям, что является достаточным для анализа и дальнейшего обучения модели. В дальнейшем все собранные данные классифицируются и хранятся в защищенной среде для последующего использования.

Действие	Описание	Наименование
Сообщение	Отправка текстовых сообщений через приложение	message
Аудио Звонок	Пакеты, связанные с аудио-звонок	call
Видео Звонок	Активность во время передач видеоданных	vcall
Передача файлов	Передача файлов между пользователями	file
Видеоконференция без активности	Сценарии, когда в приложении отсутствовала активность	dvks
Активная видеоконференция	Камера, поднятая рука, голосование	avks

Таблица 3: Собранные данные о видах активности пользователей в приложении IVA

Данные о паттернах поведения пользователей в IVA, аналогично активностям, были собраны с устройств пользователей во время использования приложения, а также во время видео-конференций за период в 10 минут. Подробное описание полученных данных представлено в табл. 4. Общее кол-во собранных данных равняется примерно 200 паттернам, разделенных на 10 категорий. Стоит отметить, что так как на данном этапе был выбран достаточно небольшой промежуток в 10 минут, то 200 паттернов вполне хватит для обучения классификатора, однако для интервала превышающего 60 минут потребуется в разы больше данных.

ID пользователя	Почерк
1	5 messages -> 2 call 30 sec -> 5 messages
2	4 call 30sec -> 3 messages -> 1 dvks 30sec
3	2 call 20sec -> 2 vcall 20sec -> 2 file -> 1 avks 30sec
4	2 avks 25sec -> 2 messages -> 1 file -> 1 call 45sec
5	1 messages -> 1 call 10sec -> 1 vcall 10sec -> 1 avks 30sec -> 1 file
6	10 call 10sec
7	2 vcall 20sec -> 5 messages -> 1 call 15sec -> 2 messages
8	2 files -> 1 messages -> 3 files
9	3 call 15-20sec -> 3 messages -> 1avks 10sec -> 1 dvks 15sec
10	4 dvks 20sec

Таблица 4: Собранные данные о паттернах поведения пользователей IVA

4.1.2. Набор данных Telegram

Мессенджер Telegram — это инструмент, специально разработанный для обеспечения эффективного и безопасного общения внутри организаций. В контексте цифрового почерка, Telegram представляет собой платформу, где пользователи могут обмениваться сообщениями, файлами, аудио- и видеозаписями, а также проводить голосовые и видеозвонки. Этот мессенджер обладает широким спектром функций, благодаря чему можно составить более полный цифровой почерк.

Подробное описание полученных данных представлено в табл. 6. Данные для обучения были собраны аналогично мессенджеру IVA. Общее кол-во собранных рсар файлов равняется 870 штук.

Действие	Описание	Наименование
Аудио Звонок	Пакеты, связанные с аудио-звонок	Audio Call
Фон	Телеграмм свернут в фоновый режим	Background
Видео сообщение	Передача видеол-файлов записанных в реальном времени	Circle
Группа	Создание группы с несколькими пользователями	Group Create
Сообщение	Отправка текстовых сообщений через приложение	Message
Фото	Отправка фото	Photo
Стикер	Отправка стикеров	Sticker
Скроллинг	Просмотр записей публичных каналов	Surf Public Channels
Видео	Передача видеол-файлов	Video
Видео Звонок	Активность во время передач видеоданных	Video Call

Таблица 5: Собранные данные о видах активности пользователей в приложении Telegram

В заключение, накопленный опыт и методология, применяемые при анализе цифрового почерка (паттерна поведения) пользователей IVA, могут быть успешно адаптированы и использованы для исследования аналогичных характеристик в мессенджере Telegram. Однако, ввиду отсутствия необходимым данных по Telegram, данное направление не будет подробно освещено в рамках текущей работы.

4.2. Мессенджер IVA

4.2.1. Предобработка данных

Процесс предобработки данных начинается с разделения всего файла на некоторые осмысленные промежутки, т. е. их группировка. Это значительно облегчает понимание характера взаимодействия и упрощает дальнейшую классификацию каждого фрагмента. Таким образом, разработана методика разделения pcap файла на сгруппированные временные отрезки, основываясь на пакетах в сетевом трафике:

1. Выделение начальных признаков. Из исходного pcap выделяется четыре основных признака для каждого пакета: `frame.len`, `frame.time_epoch`, `frame.time_delta`, `ip.proto`
2. Расширение признакового пространства. На основе этих четырех признаков используя различные математические операции получаем 16 более информативных.
3. Выбор алгоритма кластеризации и дальнейшее применение на каждом из пакетов. В зависимости от задачи, могут применяться различные методы кластеризации (DBSCAN, KMeans, Agglomerative-Clustering, MeanShift, OPTICS), которые можно настраивать для достижения оптимальной точности и эффективности.
4. Ликвидация выбросов в кластерах. Данный шаг повышает точность анализа, убирая ошибки, которые могли возникнуть из-за недостатков в алгоритмах кластеризации или из-за шума в данных.
5. Формирование временных интервалов. Необходимо найти все последовательности пакетов, имеющие один и тот же кластер, и записать все временные метки, в которых происходит смена значения.

В итоге благодаря алгоритму кластеризации, система может идентифицировать неявные структуры в данных и классифицировать ме-

няющееся кол-во активности без явных меток классов, что может быть полезно в задачах, где нет возможности однозначно определить размерность выходного пространства.

4.2.2. Распознавание активности пользователя

После проделанной предобработки данных, следующим важным шагом становится непосредственно распознавание и классификация активности пользователей. На данном этапе каждый из полученных на предыдущем шаге pcap файлов, сгруппированных по временным меткам, подвергается следующей процедуре:

1. Извлечение 90 признаков на основе tshark статистики с параметрами -z conv,ip, -z conv,tcp, -z conv,udp, -z plen,tree;
2. Удаление всех столбцов, которые никаким образом не способствуют распознаванию активности, а именно либо являются None(Null), либо содержат только 1 значение;
3. На основе корреляционного анализа происходит отсеивание менее значимых признаков, таким образом остаются только те свойства, коэффициент корреляции которых больше наперед заданного threshold в зависимости от сложности и кол-ва данных;

На основе проведенного анализа полученных результатов, включая построение множества графиков, отражающих картину активности в приложении, из 90 признаков было отобрано 38 наиболее значимых для дальнейшей работы(рис. 9).

ставя перед собой цель работы в реальном времени.

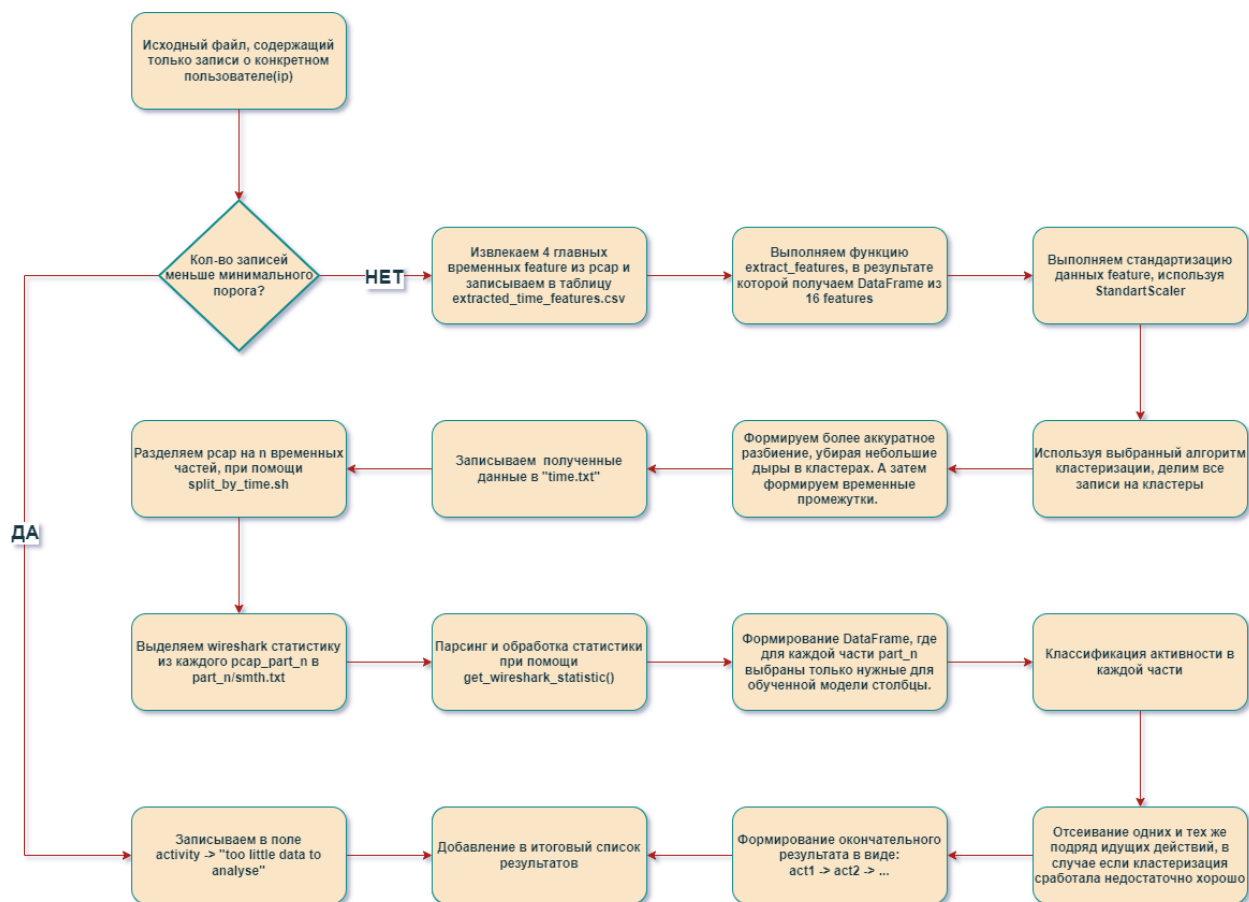


Рис. 10: Подробная блок-схема по распознаванию пользовательской активности в мессенджере IVA

В целом, такая последовательность шагов создает комплексный процесс, который позволяет глубоко анализировать и понимать активности пользователя на основе сетевого трафика. Это сочетание предварительной обработки, анализа и пост обработки данных гарантирует, что результаты являются как точными, так и полезными для понимания поведения пользователя. Более подробная схема представлена на рис. 10.

4.2.3. Распознавание паттерна поведения пользователя

Распознавание паттерна поведения пользователя — это не менее сложный процесс, требующий анализа больших объемов данных и точной идентификации индивидуальных особенностей. Входные данные

для этой задачи аналогично разделу 4.2.2 представляют собой сетевые пакеты, записанные в формате pcap, которые уже отфильтрованы таким образом, чтобы содержать информацию, относящуюся только к конкретному пользователю.

Перед тем как переходить к дальнейшим шагам реализации важно отметить ключевое отличие распознавания паттерна поведения от активности. Для классификации последовательности действий наилучшим решением является использование только нескольких последних сессий, так как это позволит системе быстрее и точнее реагировать на текущие действия пользователя. В то же время для классификации пользователя (паттерна) необходимо сохранять гораздо больший объем данных, дабы обеспечить более специализированную и всестороннюю классификацию, учитывая историю действий пользователя.

Решением поставленной проблемы является ведение отдельного файла о каждом конкретном пользователе, и последующее обновление в общем хранилище. Такой подход позволит системе постепенно дополнять и уточнять профиль каждого пользователя по мере поступления новых данных. Кроме того, в описываемой системе реализован механизм, который контролирует размер сохраняемого файла, поддерживая временной инвариант (например, 300 секунд). Это позволяет инструменту адаптироваться к ограничениям по памяти и производительности, сохраняя при этом высокую точность идентификации за счет до уточнения паттерна поведения. Подробная схема данного метода представлена ниже (рис. 11).

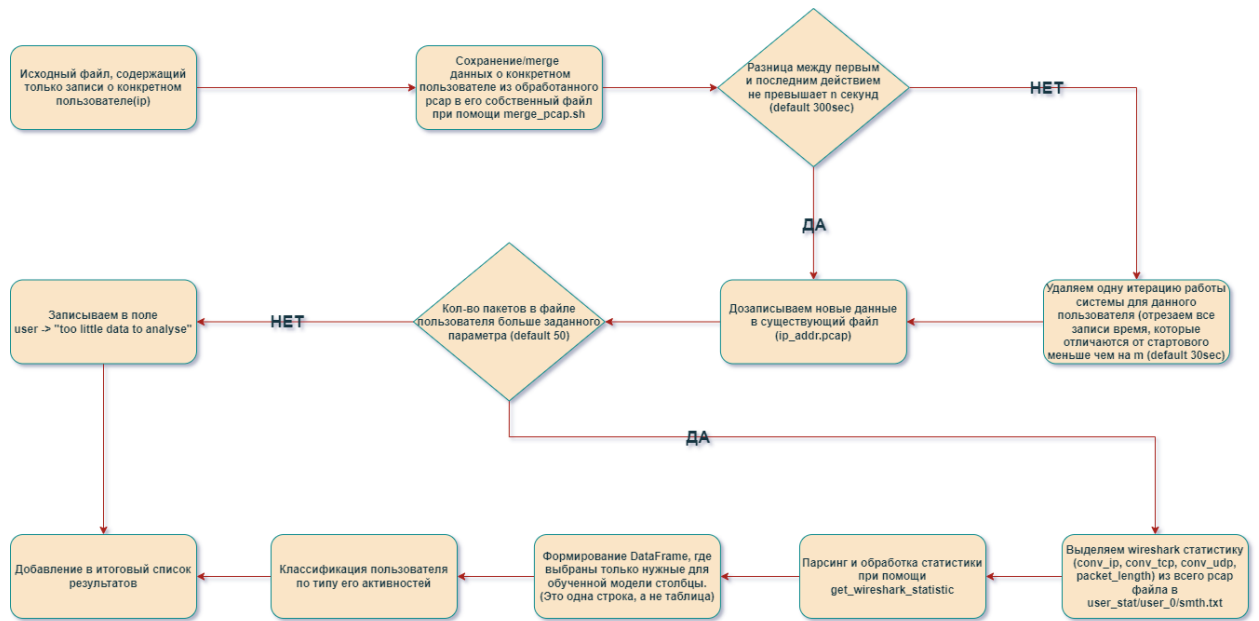


Рис. 11: Подробная блок-схема по распознаванию паттерна поведения пользователя в мессенджере IVA

Дальнейший этап заключается в обработке полученного объединенного pcap, аналогично распознаванию действий, совершаемых пользователем, как было описано в разделе 4.2.2. И наконец, финальный шаг в имплементации инструмента для классификации паттерна поведения абонента состоит непосредственно в обучении модели случайного леса (RandomForest). Однако в отличие от предыдущего этапа, целью является не определение типа активности, а распознавание самого паттерна.

На данном же этапе, в отличие от раздела 4.2.2, из 90 признаков, извлеченных из pcap файла, было отобрано лишь 18 наиболее значимых для дальнейшей работы (рис. 12).

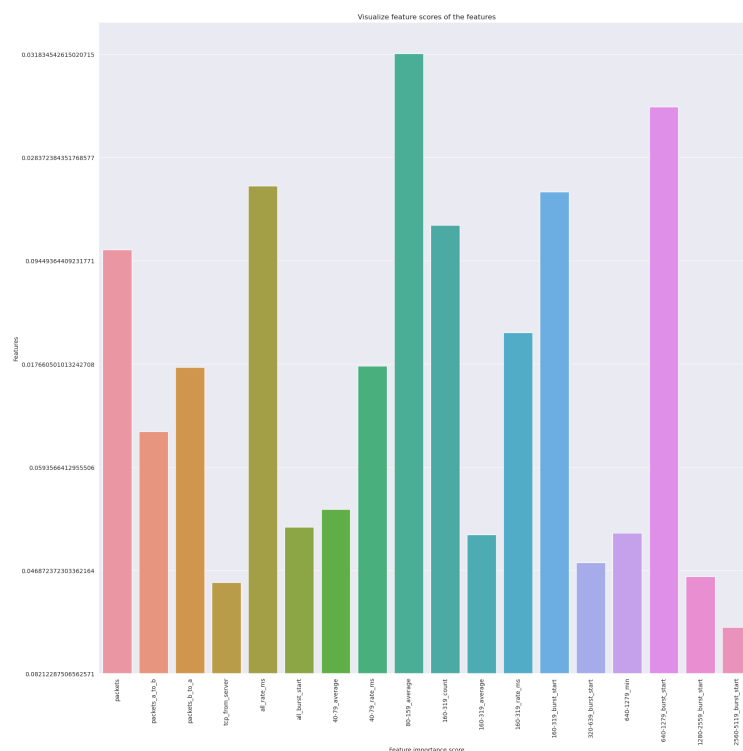


Рис. 12: Наиболее полезные feature при классификации пользователя

В результате чего обученная модель обеспечивает 94% точность. А успешное решение этой задачи открывает новые возможности для обеспечения безопасности корпоративных коммуникаций и защиты конфиденциальной информации.

4.3. Мессенджер Telegram

Переходя к распознаванию активности пользователей в мессенджере Telegram, возникает новая проблема, а именно проблема масштабируемости, которая была описана в пункте 4.2.2. В данном контексте был выбран совершенно иной путь для решения поставленной задачи, отличающийся от традиционных методов. Предложенная стратегия практически не зависит от объема трафика, что открывает широкие перспективы для применения в различных приложениях и сценариях использования.

В данном разделе мы рассмотрим подробности разработанного подхода к распознаванию активности в Telegram, его принципы работы, особенности реализации и потенциальные преимущества для обеспе-

чения безопасности и эффективности коммуникаций в корпоративной среде.

4.3.1. Предобработка данных

Процесс предобработки данных в контексте мессенджера Telegram играет ключевую роль в подготовке информации для дальнейшего анализа и распознавания активности пользователей. Общий алгоритм обработки представлен ниже:

1. Выделение *UDP/TCP* статистики сессий из всего pcap файла;
2. Разделение всей последовательности сессий на временные ряды с заданным *timedelta*;
3. Выделение дополнительных *feature*, помимо *conversation* статистики wireshark:
 - Кол-во пакетов в секунду;
 - Отношение кол-ва пакетов к кол-ву байт информации;
 - Отношение пакетов из А в В к пакетам из В в А;
 - Логарифм кол-ва пакетов;
 - Процент кол-ва пакетов в одну из сторон по отношению к общему объему;
 - ...
4. Стандартизация и нормализация данных;
5. Передача в модель классификации;

В отличие от предыдущих методов, в данном случае мы рассматриваем весь файл целиком, извлекая статистику UDP/TCP сессий из всего pcap файла и разделяя его на временные ряды. Этот подход позволяет учитывать больше информации во время классификации определенного интервала из-за возможности рассматривать последовательности

сессий разной длины, при этом время начала и завершения каждой из них может выходить за пределы исследуемого участка времени. Однако такое решение создает определенные трудности при выборе механизма распознавания, вынуждая использовать рекуррентные нейронные сети из-за разной длины входных данных.

После выделения временных рядов следует процесс Feature Engineering, где мы создаем новые признаки на основе имеющихся данных. Заключительным же шагом перед обучением или классификацией модели является стандартизация, необходимая для приведения признаков к единому масштабу и обеспечения стабильной работы алгоритмов машинного обучения. Этот процесс позволяет нивелировать влияние различий в абсолютных значениях признаков, вызванных помехами в работе сети или скорости сигнала, и сфокусироваться на относительных изменениях, которые несут более ценную информацию для идентификации пользователей.

4.3.2. Распознавание активности пользователя

Перед тем как перейти непосредственно к обучению модели классификации активности пользователя, рассмотрим процесс формирования обучающего датасета. Сбор данных является достаточно трудозатратным, ведь нам нужно записывать отдельные файлы с каждым из 10 видов активности, а также учитывать реальное время совершения действий. Как было сказано в разделе 4.1.2, удалось собрать только 870 тренировочных последовательности сессий для фиксированного *timedelta* разбиения, чего, несомненно, будет недостаточно для обучения рекуррентной нейронной сети. Поэтому было решено как соединить сразу несколько разбиений с *timedelta* = 5, 10, 15 секунд, так и применить методы аугментации данных. В результате обучающая выборка составила 5000 последовательностей.

Модель	Лучшая точность (Accuracy)
RNN	0.30
GRU	0.35
LSTM	0.50
Bidirectional LSTM	0.65
RNN With Attension	0.68
LSTM With Self-Attention	0.97

Таблица 6: Результаты обучения моделей для классификации активностей пользователей Telegram

После формирования полноценного датасета наступает ответственный этап подбора оптимальной архитектуры и гиперпараметров для обучения нейронной сети. Результаты этого процесса представлены в табл. 6. Как можно заметить, наилучшая точность (рис. 13) была достигнута при помощи архитектуры LSTM With Self-Attention (рис. 14), которая продемонстрировала впечатляющие 97% на валидационной выборке. Применение LSTM (Long Short-Term Memory) сетей в сочетании с механизмом Self-Attention позволило модели эффективно улавливать долгосрочные зависимости и выявлять наиболее значимые элементы в последовательностях данных.

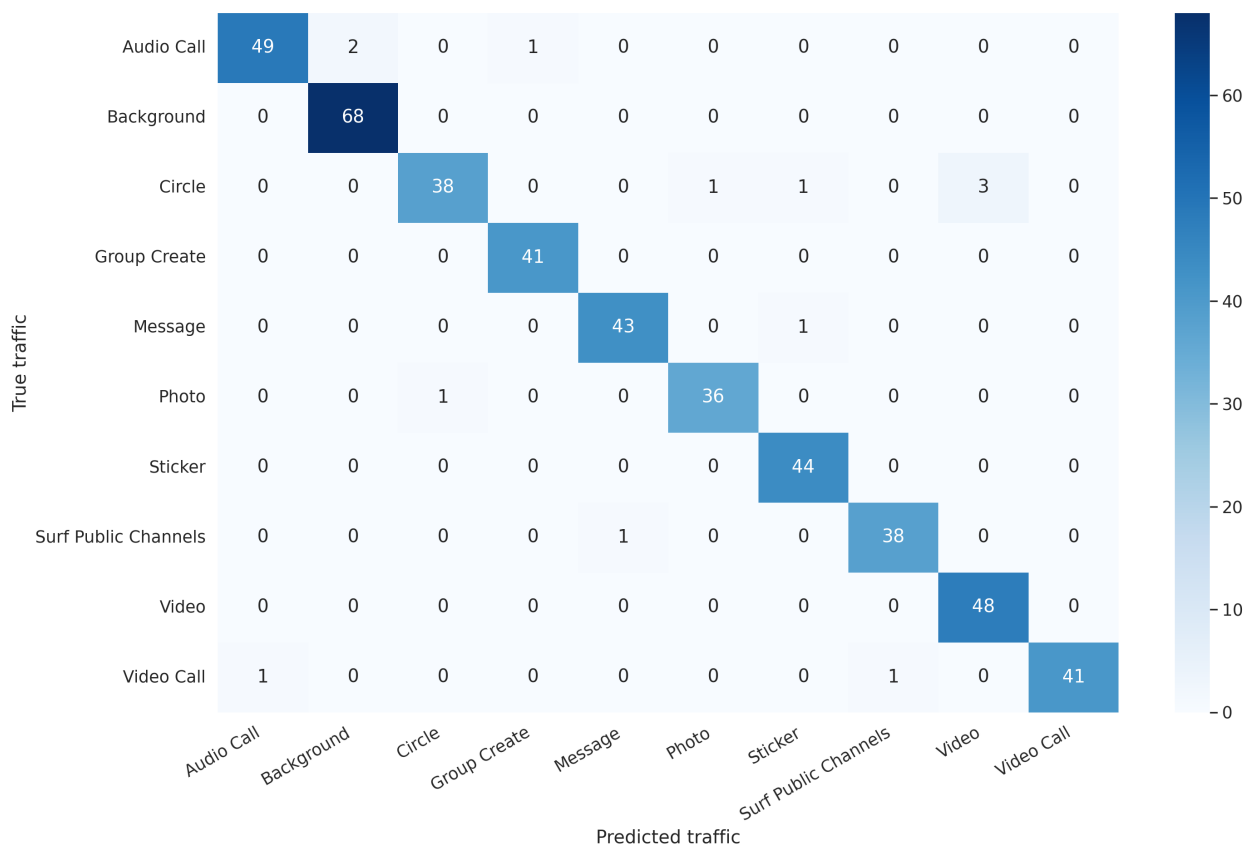


Рис. 13: Результаты обучения классификатора активности Telegram

В ходе тестирования на альтернативной тестовой выборке, собранной при использовании другой базовой станции и в различных внешних условиях, модель продемонстрировала удовлетворительную точность на уровне 40%. Этот результат показывает потенциал модели и подчеркивает важность дальнейшего совершенствования обучающей выборки, а также расширения диапазона данных для обеспечения более полного покрытия разнообразных сценариев использования.

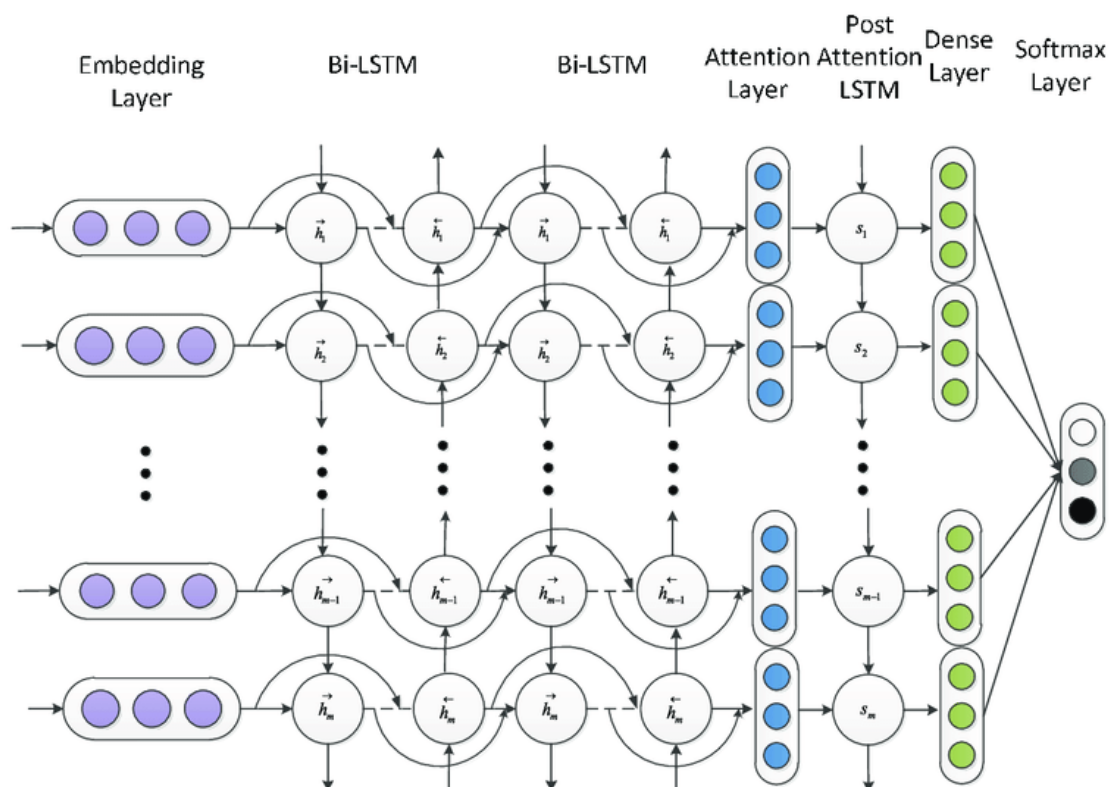


Рис. 14: Архитектура LSTM with Self-Attention

4.4. Внедрение реализованных моделей в существующие инструменты

Система “свой-чужой”, на примере мессенджера IVA, была интегрирована в существующую инфраструктуру ООО “Мобил-груп” для анализа сетевой активности. Для этого был написан промежуточный сервер на основе FastAPI и websockets, который обеспечивает связь между моделью и приложением. Данный элемент соответствует компоненту “ProcessingServer”, описанному на диаграмме 8 в разделе 3.4. Далее на блок-схеме ниже (рис. 15) описана последовательность действий, которая выполняется для достижения поставленной цели.

1. **Запуск серверной части.** Это основополагающий шаг, который инициирует работу всей системы, запуская необходимые серверные процессы, обрабатывающие запросы. При помощи служб `iva_client.service` и `iva_server.service` запускаются все необходимые

фоновые процессы для дальнейшей работы клиентской и серверной части.

2. **Запись серверного трафика.** Все данные о сетевом трафике в течении заранее отведенного временного интервала записываются в рсар файл и передаются дальше для последующего анализа и отладки. При этом систему распознавания пользователей регулярно проверяет наличие новых файлов для обработки, что позволяет системе оперативно реагировать на поступление новых данных.
3. **Файл с результатами работы системы в формате JSON.** После обработки данных о действиях пользователей результаты работы системы сохраняются в формате JSON.
4. **Инструмент для анализа сети от ООО “Мобил-груп”.** Далее все полученные данные передаются в специализированный инструмент от ООО “Мобил-груп” для анализа сетевого трафика, который ранее был подключен к реализованному серверу. При этом постоянное соединение между клиентом и сервером через WebSockets позволяет в режиме реального времени обмениваться всеми необходимыми данными.

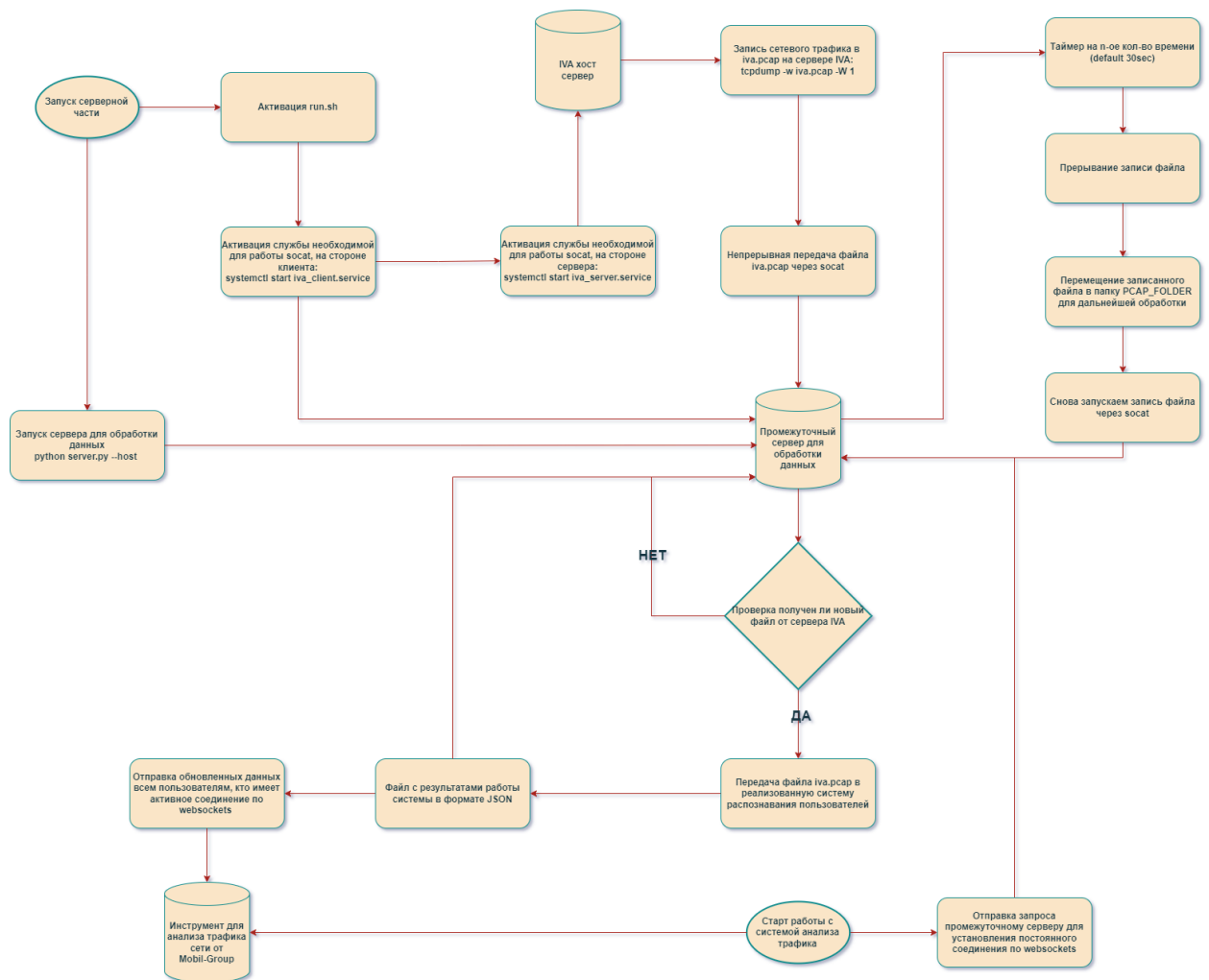


Рис. 15: Блок-схема интегрирования одного из инструментов (IVA) в существующий инструмент анализа сетевого трафика

Заключение

Целью данной работы было создание и апробация комплексной системы для формирования цифрового почерка пользователя, направленной на повышение уровня безопасности. Поставленная цель была достигнута. Для реализации проекта были решены следующие задачи:

1. Проанализированы и исследованы передовые методы и подходы к распознаванию поведенческих особенностей пользователей, включая изучение их взаимодействия с устройствами ввода и интерфейсами, а также другие индивидуальные особенности.
2. Разработаны комплексные процедуры для сбора как сетевой информации, так и радио данных. Также применены различные методы анализа данных, в том числе графические, такие как карта предпочтений.
3. Спроектирована и опробована уникальная архитектура системы на основе машинного обучения, настроенная для гибкой интеграции в разнообразные корпоративные среды, в том числе на практике с использованием различных мессенджеров.
4. Выполнено тщательное обучение моделей для идентификации пользовательской активности, включая всестороннюю подготовку и обработку данных для обучения, а также fine-tuning моделей для достижения высокой точности и надежности при распознавании уникальных цифровых отпечатков.
5. Часть разработанного инструмента успешно интегрирована в инфраструктуру ООО “Мобил-груп”, обеспечивая тем самым улучшенный контроль и анализ сетевой активности.

Исходный код проекта является проприетарным и не подлежит разглашению.

Направления будущей работы. На текущем этапе был создан макет системы, который служит начальной точкой в разработке. Этот

макет является концептуальной основой, демонстрирующей основные возможности и подходы на примере двух мессенджеров. В дальнейшем, необходимо разработать дополнительные образцы для большего кол-ва различных приложений, что позволит расширить спектр применения и гибкость полученного инструмента в разнообразных сценариях использования. Еще одним направлением для дальнейших исследований является анализ трафика как самостоятельной единицы, не полагаясь на отдельные приложения, а используя их как вспомогательные инструменты, для формирования общего паттерна поведения пользователя.

Список литературы

- [1] Abbasi Mahmoud, Shahraki Amin, Taherkordi Amir. Deep learning for network traffic monitoring and analysis (NTMA): A survey // Computer Communications. — 2021. — Vol. 170. — P. 19–41.
- [2] Auld Tom, Moore Andrew W, Gull Stephen F. Bayesian neural networks for internet traffic classification // IEEE Transactions on neural networks. — 2007. — Vol. 18, no. 1. — P. 223–239.
- [3] Awake Security Platform — автономный аналитик сетевых данных и платформа для обеспечения безопасности на основе искусственного интеллекта. [Электронный ресурс] (дата обращения: 07.11.2023) URL: <https://www.arista.com/en/solutions/security>.
- [4] Biometric user identification with dynamic footprint / Jaeseok Yun, Gregory Abowd, Woontack Woo, Jeha Ryu // 2007 Second International Conference on Bio-Inspired Computing: Theories and Applications / IEEE. — 2007. — P. 225–230.
- [5] Blindbox: Deep packet inspection over encrypted traffic / Justine Sherry, Chang Lan, Raluca Ada Popa, Sylvia Ratnasamy // Proceedings of the 2015 ACM conference on special interest group on data communication. — 2015. — P. 213–226.
- [6] Bricata — автономный аналитик сетевых данных и платформа для обеспечения безопасности на основе искусственного интеллекта. [Электронный ресурс] (дата обращения: 07.11.2023) URL: <https://bricata.com>.
- [7] Characterization of encrypted and vpn traffic using time-related / Gerard Draper-Gil, Arash Habibi Lashkari, Mohammad Saiful Islam Mamun, Ali A Ghorbani // Proceedings of the 2nd international conference on information systems security and privacy (ICISSP). — 2016. — P. 407–414.

- [8] Chowdhury Rajarshi Roy, Idris Azam Che, Abas Pg Emeroylariffion. Internet of things: Digital footprints carry a device identity // AIP Conference Proceedings / AIP Publishing. — Vol. 2643. — 2023.
- [9] Cisco Stealthwatch — автономный аналитик сетевых данных и платформа для обеспечения безопасности на основе искусственного интеллекта. [Электронный ресурс] (дата обращения: 07.11.2023) URL: <https://www.cisco.com/site/us/en/products/security/security-analytics/secure-network-analytics/index.html>.
- [10] Comparison of machine-learning algorithms for classification of VPN network traffic flow using time-related features / Sikha Bagui, Xingang Fang, Ezhil Kalaimannan et al. // Journal of Cyber Security Technology. — 2017. — Vol. 1, no. 2. — P. 108–126.
- [11] Corelight Sensor — автономный аналитик сетевых данных и платформа для обеспечения безопасности на основе искусственного интеллекта. [Электронный ресурс] (дата обращения: 07.11.2023) URL: <https://corelight.com/products>.
- [12] Corvil Security Analytics — автономный аналитик сетевых данных и платформа для обеспечения безопасности на основе искусственного интеллекта. [Электронный ресурс] (дата обращения: 07.11.2023) URL: <https://www.pico.net/corvil-analytics/>.
- [13] Cute: Traffic classification using terms / Soheil Hassas Yeganeh, Milad Eftekhari, Yashar Ganjali et al. // 2012 21st International Conference on Computer Communications and Networks (ICCCN) / IEEE. — 2012. — P. 1–9.
- [14] Dainotti Alberto, Pescapè Antonio, Claffy Kimberly C. Issues and future directions in traffic classification // IEEE network. — 2012. — Vol. 26, no. 1. — P. 35–40.
- [15] Danev Boris, Zanetti Davide, Capkun Srdjan. On physical-layer identification of wireless devices // ACM Computing Surveys (CSUR). — 2012. — Vol. 45, no. 1. — P. 1–29.

- [16] Deep packet: A novel approach for encrypted traffic classification using deep learning / Mohammad Lotfollahi, Mahdi Jafari Siavoshani, Ramin Shirali Hossein Zade, Mohammdsadegh Saberian // *Soft Computing*. — 2020. — Vol. 24, no. 3. — P. 1999–2012.
- [17] Digital footprints: Using WiFi probe and locational data to analyze human mobility trajectories in cities / Martin W Traunmueller, Nicholas Johnson, Awais Malik, Constantine E Kontokosta // *Computers, Environment and Urban Systems*. — 2018. — Vol. 72. — P. 4–12.
- [18] Digital footprints and changing networks during online identity transitions / Oliver L Haimson, Jed R Brubaker, Lynn Dombrowski, Gillian R Hayes // *Proceedings of the 2016 CHI Conference on Human Factors in Computing Systems*. — 2016. — P. 2895–2907.
- [19] Henry Colin, Gohdes Anita, Dorff Cassy. Digital footprints and data-security risks for political scientists // *PS: Political Science & Politics*. — 2022. — Vol. 55, no. 4. — P. 804–808.
- [20] Identifying smartphone users based on how they interact with their phones / Mohammed A Alqarni, Sajjad Hussain Chauhdary, Maryam Naseer Malik et al. // *Human-centric Computing and Information Sciences*. — 2020. — Vol. 10. — P. 1–14.
- [21] Identifying smartphone users based on their activity patterns via mobile sensing / Muhammad Ehatisham-ul Haq, Muhammad Awais Azam, Usman Naeem et al. // *Procedia computer science*. — 2017. — Vol. 113. — P. 202–209.
- [22] Joshi Manish, Hadi Theyazn Hassn. A review of network traffic analysis and prediction techniques // *arXiv preprint arXiv:1507.05722*. — 2015.
- [23] Karagiannis Thomas, Papagiannaki Konstantina, Faloutsos Michalis. BLINC: multilevel traffic classification in the dark // *Proceedings of the 2005 conference on Applications, technologies, architectures, and protocols for computer communications*. — 2005. — P. 229–240.

- [24] Kaspersky Anti Targeted Attack — автономный аналитик сетевых данных и платформа для обеспечения безопасности на основе искусственного интеллекта. [Электронный ресурс] (дата обращения: 07.11.2023) URL: <https://www.kaspersky.ru/enterprise-security/anti-targeted-attack-platform>.
- [25] Kellas-Dicks Mechthild R, Stark Yvonne J. Keystroke dynamics authentication techniques. — 2012. — 11. — US Patent 8,332,932.
- [26] Khalife Jawad, Hajjar Amjad, Diaz-Verdejo Jesus. A multilevel taxonomy and requirements for an optimal traffic-classification model // International Journal of Network Management. — 2014. — Vol. 24, no. 2. — P. 101–120.
- [27] Kim Yungeun, Chon Yohan, Cha Hojung. Smartphone-based collaborative and autonomous radio fingerprinting // IEEE Transactions on Systems, Man, and Cybernetics, Part C (Applications and Reviews). — 2010. — Vol. 42, no. 1. — P. 112–122.
- [28] Madhukar Alok, Williamson Carey. A longitudinal study of P2P traffic classification // 14th IEEE international symposium on modeling, analysis, and simulation / IEEE. — 2006. — P. 179–188.
- [29] Mahfouz Ahmed, Mahmoud Tarek M, Eldin Ahmed Sharaf. A survey on behavioral biometric authentication on smartphones // Journal of information security and applications. — 2017. — Vol. 37. — P. 28–37.
- [30] Moore Andrew W, Papagiannaki Konstantina. Toward the accurate identification of network applications // International workshop on passive and active network measurement / Springer. — 2005. — P. 41–54.
- [31] PT Network Attack Discovery — автономный аналитик сетевых данных и платформа для обеспечения безопасности на основе искусственного интеллекта. [Электронный ресурс] (дата обращения: 07.11.2023) URL: <https://www.ptsecurity.com/ru-ru/products/network-attack-discovery/>.

- [32] Packet classification algorithms: From theory to practice / Yaxuan Qi, Lianghong Xu, Baohua Yang et al. // IEEE INFOCOM 2009 / IEEE. — 2009. — P. 648–656.
- [33] Personalized federated learning framework for network traffic anomaly detection / Jiaming Pei, Kaiyang Zhong, Mian Ahmad Jan, Jinhai Li // Computer Networks. — 2022. — Vol. 209. — P. 108906.
- [34] Rasmussen Kasper Bonne, Capkun Srdjan. Implications of radio fingerprinting on the security of sensor networks // 2007 Third International Conference on Security and Privacy in Communications Networks and the Workshops-SecureComm 2007 / IEEE. — 2007. — P. 331–340.
- [35] Robust smartphone app identification via encrypted network traffic analysis / Vincent F Taylor, Riccardo Spolaor, Mauro Conti, Ivan Martinovic // IEEE Transactions on Information Forensics and Security. — 2017. — Vol. 13, no. 1. — P. 63–78.
- [36] Sen Subhabrata, Spatscheck Oliver, Wang Dongmei. Accurate, scalable in-network identification of p2p traffic using application signatures // Proceedings of the 13th international conference on World Wide Web. — 2004. — P. 512–521.
- [37] Studying the impact of mood on identifying smartphone users / Khadija Zanna, Sayde King, Tempestt Neal, Shaun Canavan // arXiv preprint arXiv:1906.11960. — 2019.
- [38] Threat Detection System — автономный аналитик сетевых данных и платформа для обеспечения безопасности на основе искусственного интеллекта. [Электронный ресурс] (дата обращения: 07.11.2023) URL: <https://www.facct.ru/products/threat-intelligence/>.
- [39] Ting Hu, Yong Wang, Xiaoling Tao. Network traffic classification based on kernel self-organizing maps // 2010 International Conference on Intelligent Computing and Integrated Systems / IEEE. — 2010. — P. 310–314.

- [40] Tourists' digital footprint: the spatial patterns and development models of rural tourism flows network in Guilin, China / Xiaohua Qin, XingMing Li, Wei Chen et al. // Asia Pacific Journal of Tourism Research. — 2022. — Vol. 27, no. 12. — P. 1336–1354.
- [41] Traffic classification through simple statistical fingerprinting / Manuel Crotti, Maurizio Dusi, Francesco Gringoli, Luca Salgar-elli // ACM SIGCOMM Computer Communication Review. — 2007. — Vol. 37, no. 1. — P. 5–16.
- [42] Traffic classification using probabilistic neural networks / Runyuan Sun, Bo Yang, Lizhi Peng et al. // 2010 Sixth International Conference on Natural Computation / IEEE. — Vol. 4. — 2010. — P. 1914–1919.
- [43] Uhl Andreas, Wild Peter. Footprint-based biometric verification // Journal of Electronic Imaging. — 2008. — Vol. 17, no. 1. — P. 011016–011016.
- [44] Ureten Oktay, Serinken Nur. Wireless security through RF fingerprinting // Canadian Journal of Electrical and Computer Engineering. — 2007. — Vol. 32, no. 1. — P. 27–33.
- [45] Wang Xiaoming, Parish David J. Optimised multi-stage tcp traffic classifier based on packet size distributions // 2010 Third International Conference on Communication Theory, Reliability, and Quality of Service / IEEE. — 2010. — P. 98–103.
- [46] Wireless device identification with radiometric signatures / Vladimir Brik, Suman Banerjee, Marco Gruteser, Sangho Oh // Proceedings of the 14th ACM international conference on Mobile computing and networking. — 2008. — P. 116–127.
- [47] A review of radio frequency fingerprinting techniques / Naeimeh Soltanieh, Yaser Norouzi, Yang Yang, Nemai Chandra Karmakar // IEEE Journal of Radio Frequency Identification. — 2020. — Vol. 4, no. 3. — P. 222–233.

- [48] A survey of methods for encrypted traffic classification and analysis / Petr Velan, Milan Čermák, Pavel Čeleda, Martin Drašar // International Journal of Network Management. — 2015. — Vol. 25, no. 5. — P. 355–374.
- [49] A survey of payload-based traffic classification approaches / Michael Finsterbusch, Chris Richter, Eduardo Rocha et al. // IEEE Communications Surveys & Tutorials. — 2013. — Vol. 16, no. 2. — P. 1135–1156.
- [50] Гарда Монитор — автономный аналитик сетевых данных и платформа для обеспечения безопасности на основе искусственного интеллекта. [Электронный ресурс] (дата обращения: 07.11.2023) URL: <https://gardatech.ru/produkty/monitor/>.
- [51] Диденко С. М., Шапцев В. А. Методика отображения информационного почерка пользователя // Вестник кибернетики. — 2005. — no. 4. — P. 74–78.
- [52] Мазниченко Н. И. БИОМЕТРИЧЕСКАЯ ИДЕНТИФИКАЦИЯ ПОЛЬЗОВАТЕЛЕЙ НА ОСНОВЕ ПОВЕДЕНЧЕСКИХ ХАРАКТЕРИСТИК: ОБЗОР И АНАЛИЗ // ГРААЛЬ НАУКИ. — 2021. — no. 8. — P. 183–192.
- [53] Рублев Д. П., Федоров В. М. Идентификация пользователя по динамическим характеристикам работы с манипулятором “мышь” с использованием нейронных сетей // Известия Южного федерального университета. Технические науки. — 2017. — no. 5 (190). — P. 67–74.
- [54] Трокоз Д.А. Диссертация: Методы машинного обучения для динамической биометрической верификации операторов беспилотных летательных аппаратов // Место защиты: ФГБОУ ВО «Пензенский государственный университет». — 2021. — P. 0–295.

- [55] Трокоз Д.А. Методика прямой динамической биометрической верификации // Вестник Ростовского государственного университета путей сообщения. — 2021. — по. 1. — Р. 70–79.
- [56] Ямченко Ю.В. Методы решения задач аутентификации и идентификации пользователя на основе анализа клавиатурного почерка // Вестник Московского государственного технического университета им. НЭ Баумана. Серия «Приборостроение». — 2020. — по. 1 (130). — Р. 124–139.