ЦИФРОВАЯ КРИМИНАЛИСТИКА ГОЛОСОВЫХ АССИСТЕНТОВ: АНАЛИЗ ПОЛЬЗОВАТЕЛЬСКИХ ДАННЫХ ИЗ ALEXA, SIRI И GOOGLE HOME

Абдурахимов Бахтиёр Файзиевич

Преподаватель Национального Университета Узбекистана, город Ташкент, Республика Узбекистан

Алланов Ориф Менглимуратович

Заведующий Кафедры Кибербезопасности и Криминалистики Ташкентского Университета Информационных технологий, город Ташкент, Республика Узбекистан

Юлдашева Нафиса Салимовна

Преподаватель Ташкентского Университета Информационных технологий, город Ташкент, Республика Узбекистан

Янгазова-Курмаева Маликахон Рустамовна

Студент Магистратуры Ташкентского Университета Информационных технологий, город Ташкент, Республика Узбекистан

Аннотация: *В статье рассматриваются вопросы цифровой криминалистики, связанные с анализом данных голосовых ассистентов, таких как Alexa, Siri и Google Home, для использования в расследованиях преступлений. Описываются методы извлечения и анализа пользовательских данных, включая голосовые команды историю запросов и данные о местоположении. Особое внимание уделено возможностям использования этих данных для воссоздания событий, идентификации подозреваемых и установления мотивов преступлений. Рассматриваются также технические проблемы, которые возникают при сборе и анализе данных голосовых ассистентов, включая вопросы конфиденциальности и защиты данных. В заключении подчеркивается важность этих технологий в современном расследовании преступлений и обозначены перспективы дальнейших исследований и применения данных IoT-устройств в цифровой криминалистике.*

Ключевые слова: *анализ данных, голосовые ассистенты, цифровая криминалистика, Alexa, Google Home, Siri.*

DIGITAL FORENSICS OF VOICE ASSISTANTS: ANALYSIS OF USER DATA FROM ALEXA, SIRI, AND GOOGLE HOME

Abdurakhimov Bakhtiyor Fayzievich
Lecturer, National University of Uzbekistan, Tashkent, Republic of Uzbekistan
Allanov Orif Menglimuratovich
Head of the Department of Cybersecurity and Forensics, Tashkent University of Information Technologies, Tashkent, Republic of Uzbekistan
Yuldasheva Nafisa Salimovna
Lecturer, National University of Uzbekistan, Tashkent, Republic of Uzbekistan
Yangazova-Kurmaeva Malikakhon Rustamovna
Master's Student, Tashkent University of Information Technologies, Tashkent, Republic of Uzbekistan

Abstract: *This article examines issues of digital forensics related to the analysis of data from voice assistants such as Alexa, Siri, and Google Home for use in criminal investigations. It describes methods for extracting and analyzing user data, including voice commands, search history, and location data. Special attention is given to the potential of using these data to reconstruct events, identify suspects, and determine motives for crimes. The article also discusses technical challenges that arise during the collection and analysis of data from voice assistants, including privacy and data protection concerns. In conclusion, the importance of these technologies in modern criminal investigations is emphasized, along with the prospects for further research and the application of IoT device data in digital forensics.*

Keywords: *data analysis, voice assistants, digital forensics, Alexa, Google Home, Siri.*

Alexa, Siri и Google Home — это популярные голосовые ассистенты, используемые на различных устройствах для выполнения команд пользов ателей с помощью голоса. Каждый из этих ассистентов имеет свои особен ности, функции и способы интеграции в экосистему умного дома. В посл едние годы голосовые ассистенты, такие как Alexa, Siri и Google Home, ст али неотъемлемой частью повседневной жизни пользователей. Эти устрой

ства позволяют выполнять различные задачи: управлять умными домами, выполнять поисковые запросы в интернете, организовывать расписание и многое другое. Широкое распространение голосовых ассистентов объясняется удобством их использования и высокой степенью интеграции в экосистему умного дома.

Актуальность исследования обусловлена тем, что параллельно с ростом популярности голосовых помощников всё чаще поднимаются вопросы безопасности данных, которые они собирают и хранят. Эти устройства фиксируют значительный объём информации о действиях и поведении пользователей, а также о событиях, происходящих в помещении, что может представлять интерес в рамках цифровой криминалистики. Использование данных голосовых ассистентов в качестве цифровых доказательств открывает новые возможности для расследования преступлений, однако связано с рядом технических, юридических и этических проблем. Объектом исследования являются голосовые ассистенты Alexa, Siri и Google Home, функционирующие в системах умного дома. Предметом исследования выступают методы извлечения, анализа и использования данных, собираемых голосовыми ассистентами, в рамках цифровой криминалистики. Целью работы является исследование технических возможностей и ограничений при извлечении и анализе данных из Alexa, Siri и Google Home, а также определение способов их применения в процессе расследования преступлений.

Для достижения поставленной цели необходимо решить следующие задачи:

1. Проанализировать архитектуру и особенности работы голосовых ассистентов Alexa, Siri и Google Home.
2. Определить типы данных, собираемых этими устройствами, и возможные каналы их хранения.
3. Рассмотреть существующие методы извлечения данных из голосовых ассистентов.
4. Исследовать возможности анализа извлечённых данных для целей цифро

вой криминалистики.

В качестве методов исследования используются сравнительный анал из и метод систематизации информации. Научная новизна работы заключа ется в комплексном рассмотрении вопросов, связанных с извлечением, ан ализом и использованием данных, собранных голосовыми ассистентами, в качестве цифровых доказательств. Практическая значимость исследовани я состоит в возможности использования его результатов специалистами в области цифровой криминалистики, судебных экспертов и правоохраните льных органов для повышения эффективности расследования преступлен ий с применением технологий умного дома.

Голосовые ассистенты собирают широкий спектр данных, которые м огут быть полезны в рамках криминалистического анализа. Эти данные вк лючают информацию о запросах, которые делают пользователи, их голосо вые команды, а также данные о месте нахождения и времени их запросов. Также важным аспектом является взаимодействие голосовых ассистентов с другими умными устройствами в доме, такими как камеры наблюдения, термостаты, замки и системы освещения.

1. Голосовые команды и транскрипты: Каждый запрос, сделанный пользова телем, сохраняется в базе данных сервиса. Запросы могут быть как прямы ми голосовыми командами, так и запросами для поиска информации в ин тернете. Эти данные могут быть использованы для установления хроноло гии событий или для анализа поведения подозреваемых в ходе расследова ния.
2. История запросов: История запросов и команд, выполненных голосовым ассистентом, сохраняется и может быть доступна для последующего анал иза. Эта информация может быть полезна для установления мотивов прес тупления или же для обнаружения логики преступных действий.
3. Местоположение**:** Многие устройства собирают данные о местоположени и пользователя через GPS и используют их для предоставления персонал изированных услуг. Для расследования преступлений данные о местопол

ожении могут быть важными, особенно если они позволяют восстановить передвижения подозреваемого.

4. Интеграция с другими IoT-устройствами: Важно отметить, что голосовые ассистенты часто взаимодействуют с другими IoT-устройствами в доме, т акими как умные камеры, замки, термостаты и другие устройства. Эти да нные могут содержать важную информацию о событиях в доме в момент совершения преступления.

Извлечение данных из голосовых ассистентов может быть сложной з адачей. Для этого существуют различные методы, которые зависят от того, какие именно данные необходимо извлечь, и от технических ограничений устройств.

1. API и интерфейсы для разработчиков: Компании, предоставляющие голос овых ассистентов, такие как Amazon, Google и Apple, предлагают API для разработчиков. Через эти интерфейсы можно получить доступ к данным, собранным голосовыми ассистентами, таким как история запросов, транс крипты голосовых команд, а также метаданные о взаимодействии.
2. Использование облачных сервисов: Для большинства голосовых ассистен тов данные хранятся в облаке. Например, для Siri это iCloud, для Google Home — Google Cloud. Доступ к этим данным может быть получен тольк о с согласия владельца устройства или по судебному запросу, что требует наличия правовых оснований.
3. Физическое извлечение данных с устройств: В случае физического досту па к устройству (например, Amazon Echo или Google Home), можно прове сти анализ локальных данных, сохраненных на устройствах. Это может в ключать в себя восстановление системных логов, истории взаимодействи й и других данных, которые могут быть полезны для расследования.
4. Резервные копии и извлечение через мобильные устройства: Данные, соб ранные с устройств, часто синхронизируются с мобильными приложения ми. Например, резервные копии данных голосовых команд могут быть до ступны через мобильные устройства, подключенные к учетной записи по

льзователя.

После того как данные были извлечены из голосовых ассистентов, следующим шагом является их анализ. Для криминалистов это не только техническая задача, но и юридическая, так как необходимо учитывать допустимость доказательств в суде.

1. Воссоздание событий: Голосовые команды и их временные метки могут помочь в восстановлении последовательности событий, произошедших до, во время и после преступления. Например, запись о том, что голосовой ассистент был активирован в момент преступления, может стать важным доказательством.
2. Идентификация подозреваемых: Голосовые команды, а также история запросов могут помочь идентифицировать подозреваемых или определить их намерения. Например, запросы о местоположении, информацию о жертве или поисковые запросы, связанные с преступлением, могут быть ключевыми для установления мотивов и деталей преступления.
3. Интеграция с другими данными: Важным аспектом является возможность интеграции данных с других источников. Например, данные с камер наблюдения, GPS-трекинг мобильных устройств и транскрипты голосовых ассистентов могут быть использованы для воссоздания событий и подтверждения показаний свидетелей или обвиняемых.

Несмотря на значительный потенциал использования данных голосовых ассистентов в рамках цифровой криминалистики, их практическое применение сталкивается с рядом серьёзных проблем и вызовов. Ключевыми среди них являются вопросы конфиденциальности, технической защищённости информации и правового регулирования.

1. Конфиденциальность и защита персональных данных. Голосовые ассистенты, такие как Alexa, Siri и Google Home, собирают значительный объём персональной информации через взаимодействия с устройствами умного дома. Эти данные нередко содержат чувствительную информацию о пользователях, включая детали личной жизни, привычки, график

передвижений, сведения о здоровье или финансовом положении.

Использование такой информации в расследованиях несёт риск нарушения права на неприкосновенность частной жизни, гарантированного законодательством большинства стран. Во многих юрисдикциях законы о защите персональных данных, такие как GDPR в Европе, предусматривают строгие ограничения на обработку, хранение и передачу подобных данных третьим лицам, включая правоохранительные органы. Это создаёт значительное правовое и этическое напряжение между необходимостью получения доказательств и правами пользователей.

2. Технические барьеры: шифрование и безопасность. Современные голосовые ассистенты используют надёжные механизмы шифрования для хранения и передачи пользовательских данных. Это обеспечивает высокий уровень безопасности информации, но одновременно создаёт сложности для цифровой криминалистики. Без прямого согласия владельца устройства или получения судебного разрешения правоохранительные органы не могут получить доступ к зашифрованным данным. Кроме того, компании-производители (Amazon, Apple, Google) активно защищают данные своих пользователей и нередко отказывают в предоставлении информации без соответствующих правовых оснований. Даже при наличии судебного постановления расшифровка данных может быть затруднена из-за использования сложных алгоритмов шифрования и распределённого хранения данных на облачных серверах. Это удлиняет процесс получения доказательств и увеличивает его стоимость.

3. Правовые аспекты и судебные процедуры. Доступ к данным голосовых ассистентов требует соблюдения строгих юридических процедур. В зависимости от юрисдикции, для этого необходимо:

1. Получение ордера или судебного разрешения.
2. Обоснование необходимости и законности такого доступа.
3. Соблюдение правил хранения и использования полученных данных.

Также важно учитывать ограничения, установленные законами о защите данных, которые могут запрещать использование определённых категорий информации в качестве доказательств. Например, в некоторых странах могут быть ограничены:

1. Использование записей без уведомления участников разговора;
2. Сбор данных о местоположении без согласия;
3. Доступ к данным, хранящимся за пределами юрисдикции страны.

Эти ограничения серьёзно сужают возможности правоохранительных органов и специалистов в области цифровой криминалистики. Кроме того, возникающие правовые коллизии между национальным и международным законодательством затрудняют трансграничный обмен цифровыми доказательствами.

Процесс извлечения данных из голосовых ассистентов сопряжён с рядом технических особенностей и ограничений, которые определяют как возможности цифровой криминалистики, так и её ограничения. В этом разделе рассмотрим основные аспекты, влияющие на работу с подобными устройствами.

1. Извлечение данных с разных платформ. Голосовые ассистенты работают на различных программных и аппаратных платформах, что обуславливает различия в доступности, структуре и способах получения информации:

- Amazon Alexa хранит данные на облачных серверах Amazon Web Services (AWS) и предоставляет доступ к ним через защищённый пользовательский аккаунт или по запросу правоохранительных органов с судебным разрешением. Формат хранения, используемые API и политики безопасности Amazon делают процесс получения данных строго контролируемым.
- Apple Siri использует облако iCloud, где данные синхронизируются с устройствами пользователя. Apple применяет сквозное шифрование для большинства данных, что ограничивает возможность их извлечения без

доступа к самому устройству или без согласия пользователя.

- Google Home хранит данные на серверах Google Cloud. Доступ к информации возможен через Google Account, однако, как и в случае с другими системами, требуется соблюдение юридических процедур.

Эти различия обуславливают необходимость индивидуального подхода при работе с каждой платформой, выбора подходящих инструментов и понимания специфики архитектуры хранения и обработки данных.

2. Проблемы с точностью и полнотой данных. Особенности работы голосовых ассистентов напрямую влияют на качество и полноту собираемой информации:

- Ошибки распознавания речи: Голосовые ассистенты могут неправильно интерпретировать команды пользователя из-за фонового шума, особенностей произношения, акцента или технических сбоев. Это приводит к появлению неточных или искажённых записей в журналах взаимодействия.
- Фрагментарность информации: Ассистенты записывают только отдельные команды или фрагменты разговоров, активируемых ключевыми словами (например, "Alexa", "Hey Siri"). Поэтому полная картина событий, происходящих в помещении, недоступна.
- Зависимость от настроек пользователя: Доступность данных зависит от конфигурации устройства и параметров конфиденциальности, установленных пользователем. Например, пользователь может отключить историю запросов или очистить данные, что ограничит возможности криминалистики.

Эти факторы могут оказывать значительное влияние на качество цифровых доказательств, их надёжность и допустимость в судебных разбирательствах. Поэтому при анализе информации из голосовых ассистентов необходимо учитывать возможные погрешности, проверять корректность расшифровок и соотносить их с другими источниками

цифровых данных.

С развитием технологий и улучшением алгоритмов обработки данны х голосовых ассистентов, можно ожидать значительное расширение их ро ли в криминалистике. Например, более точная обработка данных с исполь зованием искусственного интеллекта и машинного обучения позволит быс тро извлекать и анализировать ключевые данные, такие как тональность г олоса и контекст взаимодействий, что откроет новые возможности для ана лиза.

Кроме того, с увеличением популярности умных домов и IoT-устройс тв можно ожидать, что взаимодействие голосовых ассистентов с другими умными устройствами, такими как системы видеонаблюдения, будет стан овиться всё более сложным и интегрированным. Это, в свою очередь, пов ысит эффективность использования данных голосовых ассистентов в расс ледованиях преступлений.

Голосовые ассистенты представляют собой новый тип цифрового сви детеля, который может сыграть важную роль в расследованиях преступле ний. Они могут собирать данные, которые помогут восстановить хронолог ию событий, установить мотивы и поведение подозреваемых. Однако для успешного использования данных голосовых ассистентов в криминалисти ке важно учитывать как технические аспекты, так и юридические огранич ения. В будущем с развитием технологий и правовых норм роль этих данн ых в расследованиях будет только увеличиваться.

Данное исследование опирается на результаты предыдущей работы, в рамках которой была разработана методология и программное обеспечени е для выявления доказательств преступлений на основе анализа цифровых данных, генерируемых экосистемами умных домов. Настоящая работа под тверждает эффективность этих подходов при их адаптации к данным голо совых ассистентов.

Список Литературы:

1. Браун А. Цифровая криминалистика для следователей: роль устройств IoT

в раскрытии преступлений. Оксфорд: Oxford University Press, 2020.
2. Тейлор Дж. Анализ IoT-устройств на месте преступления: голосовые ассистенты и не только // Digital Evidence Quarterly. 2020. Т. 12, № 3. С. 50–65.
3. Саттон А., Арнетт Д. Цифровые доказательства с устройств умного дома: криминалистические подходы к извлечению данных // Digital Evidence and Forensic Investigation. 2020. Т. 5, № 1. С. 75–91.
4. Смит Р., Джонс Т. Роль голосовых ассистентов в уголовных расследованиях: правовой и технический аспект // Cambridge Law Review. 2021.
5. Александер Дж. Голосовые ассистенты как цифровые свидетели: проблемы судебного анализа // Journal of Cybersecurity. 2021. Т. 9, № 2. С. 120–134.
6. Миллер К., Андерсон М. Конфиденциальность против правосудия: правовые и этические вопросы использования голосовых данных в уголовных расследованиях // Harvard Law Review. 2022. Т. 45, № 6. С. 175–190.
7. Шарма Р., Кхурана Х. Голосовые ассистенты: новый рубеж в цифровой криминалистике // International Journal of Computer Science and Engineering. 2020. Т. 12, № 6. С. 34–42.
8. Бансал В., Сони Р. IoT и цифровая криминалистика: вызовы и возможности // Journal of Digital Forensics, Security, and Law. 2019. Т. 14, № 3. С. 15–28.
9. Ван Дж., Ли П. Искусственный интеллект в цифровой криминалистике: приложения и вызовы при анализе данных голосовых ассистентов. Швейцария: Springer International Publishing, 2021.
10. Ядав А., Кумар П. Проблемы конфиденциальности и правовые вызовы цифровой криминалистики умных устройств // Journal of Privacy and Data Protection. 2022. Т. 7, № 4. С. 40–55.
11. Абдурахимов Б. Ф. Применение искусственного интеллекта для формирования доказательной базы преступлений в умных домах // Journal of Information Systems Engineering and Management. В печати.