**Творческий проект на тему:**

**«Конфиденциальность в социальных сетях и**

**мессенджерах»**

**по профилю «Информационная безопасность»**

**2023**

Муниципальное бюджетное общеобразовательное учреждение «Кульбаево-Марасинская средняя общеобразовательная школа Нурлатского муниципального района Республики Татарстан»

**«Конфиденциальность в социальных сетях и мессенджерах»**

**Творческий проект**

**по профилю «Информационная безопасность»**

|  |  |
| --- | --- |
|  | **Выполнил: обучающийся 10 класса Нигматуллин Рамис Раисович**  **Руководитель : учитель технологии Садретдинов Марат Харисович** |

**г. Нурлат**

**2023**

**РЕФЕРАТ**

- сведения об общем объеме отчета, количестве иллюстраций, таблиц, использованных источников, приложений;

- перечень ключевых слов (от 5 до 15 слов или словосочетаний);

- текст реферата.

- объект исследования или разработки;

- цель работы;

- методы или методологию проведения работы;

- результаты работы и их новизну;

- область применения результатов;

- рекомендации по внедрению или итоги внедрения результатов НИР;

- экономическую эффективность или значимость работы;

- прогнозные предположения о развитии объекта исследования.

Если отчет не содержит сведений по какой-либо из перечисленных структурных частей реферата, то в тексте реферата она опускается, при этом последовательность изложения сохраняется.

**СОДЕРЖАНИЕ**

**ВВЕДЕНИЕ** 4

- Обоснование актуальности и проблемы в исследуемой сфере 4

- Формулировка темы, цели и задач проекта 4

**ОСНОВНАЯ ЧАСТЬ ОТЧЕТА О НИР** 5

**Глава 1 Теоретическое исследование** 5

1.1 Сбор информации по проблеме 5

1.2 Предпроектное исследование: анализ наличия прототипов и аналогов 6

1.3 Предложения решения выявленной проблемы. Авторская концепция проекта. Выбор оптимальной идеи. Описание проектируемого решения

выявленной проблемы 7

1.4 Применение методов проектирования и исследования анализируемой проблемы 7

**Глава 2 Креативность и новизна проекта** 8

2.1 Оригинальность предложенных идей 8

2.2 Значимость и корректность проекта 8

**Глава 3 Разработка технологического процесса** 9

3.1 Выбор технологии реализации, формы итогового решения и

инструментария его получения 9

3.2 Представление ожидаемого результата, его специализированных и

пользовательских свойств 10

3.3 Оценка потенциала применения результата проекта. Анализ результатов исследования, обобщение, предложения по внедрению

**ЗАКЛЮЧЕНИЕ**

**СПИСОК ИСПОЛЬЗОВАННЫХ ИСТОЧНИКОВ**

**ПРИЛОЖЕНИЕ**

- ТЕРМИНЫ И ОПРЕДЕЛЕНИЯ

- ПЕРЕЧЕНЬ СОКРАЩЕНИЙ И ОБОЗНАЧЕНИЙ

**ВВЕДЕНИЕ**

**Обоснование актуальности и проблемы в исследуемой сфере**

***Актуальность.***

Почти каждый, кто сидит в Интернете, пользуется социальными сетями и мессенджерами. Так или иначе, никто не хочет, чтобы его личные данные были похищены, но не каждый знает, как себя обезопасить в таких ситуациях.

***Проблема.***

Множественные взломы аккаунтов и пользование личной информацией третьими лицами.

**Формулировка темы, целей и задач проекта**

***Тема проекта***

Конфиденциальность в социальных сетях и мессенджерах

***Цель*** – узнать, какие способы защиты информации предоставляют популярные социальные сети и мессенджеры, и выявить самое безопасное приложение для общения.

***Задачи:***

1. Собрать информацию о способах защиты популярных социальных сетей и мессенджеров.
2. Проверить на личном опыте надежность этих способов.
3. Подготовить статистику.
4. Выявить самое безопасное приложение для общения.

**ОСНОВНАЯ ЧАСТЬ ОТЧЕТА О НИР**

**Глава 1 Теоретическое исследование**

**1.1 Сбор информации по проблеме**

Я часто слышу от друзей и знакомых, что их сайт взломали или похитили личную информацию. Если зайдем в Интернет, то увидим, что подобные проблемы волнуют не только нас.

Такая страница может появиться у тех, кого взломали в VK (рисунок 1).



*Рисунок 1 –* Замороженный аккаунт VK

Поэтому я решил найти самый безопасный мессенджер и проверить на надёжность популярные социальные сети.

**1.2 Предпроектное исследование: анализ наличия прототипов и**

**аналогов**

***Анализ прототипов и аналогов.***

Мною были рассмотрены работы людей, которые до меня решали подобную проблему. Результаты приведены в таблице (таблица 1).

*Таблица 1 – Прототипы и аналоги*

| ***Прототипы / аналоги*** | ***Достоинства*** | ***Недостатки*** |
| --- | --- | --- |
| Проект «Безопасность при сетевом общении». | Автор проводит анализ поведения людей в социальных сетях, дает советы по обеспечению безопасности личных данных. | Автор рассматривает только те факторы обеспечения безопасности, которые зависят от пользователя, но никак не от самой социальной сети. |
| Исследовательская работа на тему «Безопасность подростков в интернете». | Автор рассматривает проблему надёжности социальных сетей, группы интернет - угроз и способы их решений. | Способы решений проблемы, заданной автором, больше относится к подросткам и детям. |

Как видно из таблицы прототипов и аналогов очень мало, в большей степени информация на эту тему в Интернете приведена в виде статьи, но раздроблена. Также в этих работах не рассматриваются мессенджеры.

Поэтому я выдвигаю такие требования к проектному решению:

1. Решение должно содержать информацию о мессенджерах.
2. Решение должно содержать информацию о способах защиты данных в самих социальных сетях и мессенджерах.
3. Решение должно быть полезным и простым в понимании для большинства пользователей Интернета

**1.3 Предложения решения выявленной проблемы. Авторская концепция проекта. Выбор оптимальной идеи.**

***Предложения решения выявленной проблемы.***

Я собираюсь искать информацию в разных статьях и сайтах в Интернете, а также расспросить об этом друзей и знакомых, пообщаться с экспертами. Затем проверить на своём опыте найденные способы обеспечения конфиденциальности. По итогу, записать в таблице плюсы и минусы популярных социальных сетей и мессенджеров

***Авторская концепция проекта.***

Я считаю выдвинутое решение самым оптимальным и буду следовать ему, при этом учитывая все вышесказанные требования.

***Выбор оптимальной идеи.***

Так как других идей у меня нет, поэтому выберу ту, которую изначально придерживаюсь.

**1.4 Применение методов проектирования и исследования анализируемой проблемы**

В ходе проектирования и исследования мной были использованы следующие методы:

***Для поиска информации:***

1. Интервью и опросы
2. Экспертная оценка
3. Парсинг

***Для обработки полученной информации:***

1. Аннотирование

**Глава 2. Креативность и новизна проекта**

**2.1. Оригинальность предложенных идей**

Отсутствуют известные прямые аналоги предложенного решения, а по уже имеющимся, нет полных по содержанию работ.

Выдвинутая проблема затрагивает нынешнее общество людей как нельзя кстати. Ведь сейчас большинство пользуется Интернетом, передает некоторые свои данные на «общий показ», не подозревая, что их могут использовать в корыстных целях.

Получив сведения о том, как социальные сети и мессенджеры защищают данные пользователей, человек поймет, что можно писать в Интернете и где безопаснее это сделать. Благодаря полученным знаниям он будет меньше попадать в неприятные ситуации в сети.

**2.2 Значимость и корректность проекта**

Значимость проекта обоснована тем, что всё больше людей общаются в сети. Работа корректна в большинстве случаев, т.к. многие социальные сети находятся в открытом доступе по всему миру, исключениями являются Facebook, Instagram, Twitter, Viber, Wickr Me из-за санкции.

**Глава 3. Разработка технологического процесса**

**3.1 Выбор технологии реализации, формы итогового решения и инструментария его получения**

Технология реализации соответствует АРИЗ-82.

Формой итогового решения будет являться таблица, в которой будут записаны плюсы и минусы каждой социальной сети и каждого мессенджера.

Для получения итогового решения будут использованы следующие оборудования: компьютер или ноутбук с доступом в Интернет, сенсорный телефон, поддерживающий доступ к нужным социальным сетям и мессенджерам.

Технологическая карта реализации решения поставленной проблемы приведена в таблице (таблица 2).

*Таблица 2 – Технологическая карта реализации решения поставленной проблемы*

| ***№***  ***п/п*** | ***Наименование операции*** | ***Объяснение операции*** | ***Оборудование, инструменты, приспособления*** |
| --- | --- | --- | --- |
| 1 | Поиск информации в интернете. | Я вводил в поисковик разные запросы, похожие на «Как мессенджер Х защищает данные своих пользователей». Затем заходил на первые 10 сайтов и брал оттуда информацию. Также я расспросил друзей и знакомых, которые разбираются в кибербезопасности | Ноутбук, компьютер. |
| 2 | Обработка полученной информации. | Полученную информацию я упорядочил и кратко записал для себя. | Ноутбук, компьютер. |
| 3 | Проверка на личном опыте надёжность этих способов. | На протяжении трёх недель я пробовал эти способы, также попросил друзей их использовать. | Телефон. |
| 4 | Составление таблицы итогового решения | Результаты, плюсы и минусы популярных социальных сетей и мессенджеров я записал в таблице (таблица 3, стр. 10) | Ноутбук, компьютер. |

**3.2 Представление ожидаемого результата, его специализированных и пользовательских свойств**

Я готов предъявить готовую таблицу итогового решения поставленной проблемы.

Благодаря таблице можно узнать, какие социальные сети и мессенджеры безопасные и чем именно они гарантируют безопасность.

*Таблица 3 – Плюсы и минусы популярных социальных сетей и мессенджеров, итог.*

| №  п/п | Наименование социальной сети или мессенджера | Плюсы | Минусы |
| --- | --- | --- | --- |
| 1 | WhatsApp | 1. Все сообщения, изображения, видео и звонки защищены сквозным шифрованием(End-to-end encryption).  2. Можно включить двухфакторную аутентификацию. Она защитит вас, если мошенники каким‑то образом получат доступ к сим‑карте.  3. Можно отключить всплывающие сообщения. Это удобно,если вы не хотите, чтобы другой человек не прочитал то, что вам отправили, даже если устройство выключено.  4. Не зная ваш номер телефона, никто не сможет вам написать или посмотреть ваш статус, отсутствует система поиска пользователя по общей базе данных.  5. Не хранит сообщения на серверах, поэтому, если киберпреступники взломают платформу, они не смогут расшифровать сообщения.  6. Полная поддержка VPN, анти-шпионского софта и антивирусов. | 1. При резервном копировании сообщений все переписки попадут либо в Google Drive на Android либо в iCloud в IOS, где они будут уже не зашифрованы. Советую отключить эту функцию.  2. После применения новой политики конфиденциальности WhatsApp стал передавать данные своих пользователей Facebook, а именно: данные о местоположении, метаданные ваших сообщений (с кем, когда и как часто вы общаетесь), данные об используемом устройстве или браузере, IP-адреса и сведения о вашей мобильной сети, платежную информацию.  3. Привязка к телефону обязательна, так как на этой основе и создаётся аккаунт, но увы, есть способы перехвата кодов, отправляемых через SMS (атака MITM).  4. Мессенджер много раз взламывали, что вызывает недоверие со стороны пользователей.  5. WhatsApp допускает чтение сообщений сотрудниками управляющих компаний. |
| 2 | Telegram | 1. Можно включить двухфакторную аутентификацию.  2. Все сообщения шифруются изначально по MTProto протоколу, который создали разработчики, основываясь на симметричном алгоритме шифрования AES и протоколу Диффи-Хеллмана.  3. Есть функция секретного чата, в котором включено сквозное шифрование, а также исчезновение сообщений по истечению определённого времени.  4. Приложения с открытым исходным кодом и Telegram Database Library.  5. Есть сквозное шифрование.  6. Превосходное Р2Р-шифрование. | 1. Опять же привязка к телефону обязательна, что создаёт возможность для атаки MITM.  2. Все сообщения проходят через сервер, где они расшифровыются, сохраняются на нём, затем обратно шифруются и идут к получателю.  3. Не раз взламывали как сам данный мессенджер, так и его сервер, причём даже публично.  4. Выключено шифрование по умолчанию.  5. Частично открытый исходный код.  6. Telegram допускают чтение сообщений сотрудниками управляющих компаний.  7. Telegram не использует протоколы TLS/Noise для шифрования сетевого трафика.  8. Telegram использует сквозное шифрование только для звонков и для функции «секретные чаты». |
| 3 | VK | 1.Можно включить двухфакторную аутентификацию. Она защитит аккаунт, если ваш пароль каким-то образом попадёт не в те руки. | 1. Отсутствие приватности. Если не выставить специальные настройки, то к разделу с документами доступ будет у каждого. |
| 2. Во вкладке «Безопасность» можно увидеть, когда, откуда, и с какого устройства заходили в этот аккаунт последний раз.  3. Во вкладке «Приватность» можно ограничить круг тех, кому видна ваша страница и отдельная информация на ней, и тем самым защитить от лишних глаз данные, которыми вы не хотите делиться со всеми подряд.  4. При подключении двухфакторной аутентификации «ВКонтакте» сгенерирует для вас десять одноразовых резервных кодов. Если у вас не будет доступа к SMS-сообщениям. | 2. Правоохранительные органы имеют доступ ко всем данным пользователей.  3. Очень частые взломы и заморозки аккаунтов. |
| 4 | Одноклассники | 1. Можно включить двухфакторную аутентификацию. | 1. «Невидимка» как и «Закрытый профиль» оба платные услуги. |
| 2. Во вкладке «история посещений» указано, когда и откуда в ваш аккаунт логинились за последний месяц. | 2. Частые взломы аккаунтов. |
| 3. Если вы не хотите, чтобы другие знали, что вы просматривали их профиль, можете купить **Невидимку.**  **4. Вы можете установить «Закрытый профиль».**  5. При подключении двухфакторной аутентификации «Одноклассники» сгенерирует для вас десять одноразовых резервных кодов. Если у вас не будет доступа к SMS-сообщениям. | 3. Привязка к телефону обязательна, что создаёт возможность для атаки MITM. |
| 5 | Facebook | 1. Можно включить двухфакторную аутентификацию, а так же использовать генератор кода, функция которого позволяет вместо SMS использовать коды, которые генерирует мобильное приложение Facebook.  2. При вводе конфиденциальной информации (например, номера кредитной карты или пароля), система шифрует эти данные с помощью технологии SSL.  3. Facebook сохраняет список компьютеров, гаджетов и браузеров, которыми вы обычно пользуетесь при входе в соцсеть. Если соцсеть зарегистрирует авторизацию с незнакомого устройства или браузера, вам придет оповещение на электронную почту. Так вы сможете вовремя узнать, что кто-то посторонний залогинился в ваш аккаунт, и поменять свой пароль.  4. С помощью функции «Открытый ключ» можно дать другим пользователям свой public key, и полученные ими сообщения расшифровать своим private key.  5. Откуда вы вошли — очень удобная функция, которая позволяет посмотреть, на каких устройствах вы сейчас залогинены в Facebook и при надобности выйти из них. | 1. Facebook  может собирать данные даже о тех людях, у которых нет аккаунта в этой социальной сети. И, что самое интересное, это практически неизбежно.  2. Вся бизнес-модель основана на обмене данными с рекламодателями, маркетинговыми компаниями и другими организациями, которым крайне важно иметь сравнительно легкий способ доступа к такой информации.  Фактически, любой, кто платит деньги, может получить доступ к вашей персональной информации.  3. Не раз наблюдались утечки информации, так в первом полугодии 2021 года случилась наибольшая из них. Были похищены данные свыше полумиллиарда пользователей. |
| 6 | Instagram | 1. Можно включить двухфакторную аутентификацию.  2. Разработчики придумали, как защитить своих пользователей от фишинга через почту. Теперь в настройках приложения вы можете посмотреть, какие письма социальная сеть присылала вам за последние две недели. Если вы получили письмо якобы от Instagram, но в приложении его нет — можете смело отправлять его в спам. | 1. Заблокирован в России |
| 7 | Discord | 1. Можно включить двухфакторную аутентификацию. | 1.Через Discord распространяются вредоносные файлы. В свежем исследовании было выявлено несколько десятков типов зловредов. Очевидной угрозой это является просто потому, что каждый загружаемый в Discord файл получает постоянный URL. |
| 8 | Twitter | 1. Можно включить двухфакторную аутентификацию.  2. Можно включить приватный аккаунт, после этого никто, кроме тех, кого вы сами одобрили, не сможет следить за вашим аккаунтом.  3. Twitter переходит на защищенный протокол HTTPS. | 1. Передает метаданные пользователей рекламодателям. |
| 9 | Viber | 1. Сквозное шифрование. Сообщения шифруются в момент отправки с вашего устройства и расшифровываются только на устройстве получателя. Ключи шифрования находятся только на устройствах пользователей, и больше нигде.  2. Некоторые чаты особенно важны и требуют дополнительного уровня безопасности. Для таких случаев используйте скрытые чаты. Они хранятся отдельно от обычных чатов и доступ к ним можно получить, введя PIN-код.  3. Каждый чат Viber имеет цветовую маркировку в зависимости от уровня шифрования «Зелёный» «Серый» «Красный». | 1. По умолчанию имеет доступ к списку ваших контактов и другим пользовательским данным.  2. Может отслеживать вашу геолокацию, продолжительность использования приложения и периоды онлайн-активности. |
| 10 | Signal | 1. Открытый исходный код.  2. Диалоги в приложении Signal зашифрованы сквозным шифрованием.  3. Используются самоуничтожающиеся исчезающие сообщения.  4. Алгоритмы шифрования: протокол передачи сигналов с Perfect Forward Secrecy (PFS) для текстовых сообщений, голосовых сообщений и видеозвонков. | 1. Привязка к телефону обязательна, что создаёт возможность для атаки MITM.  2. Нету двухфакторной аутентификации. |
| 11 | Wickr Me | 1. Приложение использует сквозное шифрование для всех сообщений и файлов, включая изображения и видео.  2. Алгоритмы шифрования: AES 256, ECDH521 и RSA 4096 с идеальной прямой секретностью (PFS).  3. Анонимные аккаунты.  4. Удаляющиеся после прочтения сообщения и вложения.  5. Не ведётся запись IP-адресов и идентификаторов устройств.  6. Соответствие требованиям GDPR.  7. Все сообщения Wickr шифруются локально на устройстве с использованием отдельного ключа для каждого сообщения.  8. В Wickr реализована функция, позволяющая пользователям обнаруживать снимки экрана: если кто-то сделает снимок экрана с отправленным сообщением, отправитель этого сообщения получит уведомление. | 1. Код публично доступен на GitHub, но не является открытым. |
| 12 | Советы, не касающиеся мессенджеров и социальных сетей | 1. Не сообщайте пароли, данные кредитных карт и другие личные данные в сообщениях.  2. Остерегайтесь раскрытия личных данных незнакомцам, с которыми вы общаетесь посредством мгновенных сообщений. Злоумышленники могут использовать против вас  даже такую на первый взгляд невинную информацию, как название вашего работодателя.  Чтобы не стать жертвой [фишингового мошенничества](https://www.kaspersky.ru/resource-center/preemptive-safety/phishing-prevention-tips), никогда не переходите по ссылкам в мгновенных сообщениях от людей, с которыми вы не знакомы и которым вы не доверяете и не встречались в реальной жизни.  3. Наряду с защитой устройства паролем или PIN-кодом, рекомендуется также использовать программу безопасности. Например, [Kaspersky Internet Security для Android](https://www.kaspersky.ru/android-security) блокирует подозрительные приложения, веб-сайты и файлы, а также не дает шпионским программам отслеживать звонки, текстовые сообщения и местоположение. |  |

**3.3 Оценка потенциала применения результата проекта. Анализ результатов исследования, обобщение, предложения по внедрению**

Моя проектная работа полезна тем, что станет больше информационно грамотных пользователей, соответственно уменьшиться количество взломов и киберпреступлений.

Экономическая оценка:

Себест-сть *= Ст. мат.+Ст. эл. эн.+ Аморт.об.+Ст. тр.*

1. Расчет стоимости материалов (*Ст. мат.*):

Затраты приведены в таблице (таблица 4) на общую сумму *Ст. мат.= 34 руб.*

*Таблица ... – Использованные материалы и их стоимость*

|  |  |  |  |
| --- | --- | --- | --- |
| ***Затраты*** | ***Количество***  ***(ед., шт.)*** | ***Стоимость за единицу (руб.)*** | ***Общая стоимость (руб.)*** |
| Бумага (тетрадь в клетку 12 листов) | 2 | 12 | 24 |
| Ручка | 1 | 8 | 8 |
| **Итого:** | | | **32** |

2.Расчет стоимости электроэнергии (*Ст. эл. эн.*):

Расчёт ведётся исходя от того, что мы в среднем сидели 3 часа в день на протяжении трёх недель за электронными устройствами (в основном ноутбук), средняя мощность которых равна 40 Вт. Стоимость электроэнергии за 1 кВт/ч равен 3,8 руб. Соответственно общая стоимость электроэнергии равна 9,12 руб.

3.Амортизация оборудования (*Аморт.об.*):

Наш ноутбук стоит примерно 15 000 руб. Он относиться к 2 амортизационной группе основных средств, срок полезного действия которой равен 2-3 года. Условно возьмём 2,5 года. Использовали ноутбук 3 часа в день на протяжении трёх недель. Значит амортизация оборудования равна 51,37 руб.

1. Стоимость труда (*Ст.тр.*):

Мы оцениваем наш труд в 1000 руб.

Себест-сть *=* 32 руб. + 9,12 руб. + 51,37 руб. + 1000 руб. = 1092,46 руб.

Реализация:

Предположительная стоимость продажи данной информации человеку равна 3000 руб. НДФЛ составляет 13%. Прибыль равен 1517,54 руб.

Анализ результатов исследования:

Как выяснилось, большинство мессенджеров и социальных сетей используют данные пользователей либо в коммерческих целях, либо предоставляют к ним доступ государственным органам. Некоторые не обладают должной защитной системой. В итоге самыми надёжными мессенджерами становятся Signal и Wickr Me.

Экологическая оценка:

Так как мы в основном пользовались ноутбуком, то во время решения поставленной проблемы с экологической стороны ничего не было загрязнено или испорчено. А результатом проекта является информация, которая никак сама по себе не влияет на природу.

Обобщение, предложение по внедрению :

Полученный результат, а точнее информацию, можно выставить на сайт в свободном доступе и продвигать его, чтобы больше людей узнали, как защитить свои данные, а чтобы получать прибыль можно внедрить рекламу. **ЗАКЛЮЧЕНИЕ**

Данная практическая работа предназначена для того, чтобы обезопасить времяпрепровождение большинства пользователей Интернета, в частности Рунета. Могу заявить, что самыми безопасными на данный момент времени мессенджерами являются Signal и Wickr Me.

Были выполнены все поставленные задачи.

Хорошая экономическая эффективность.

**СПИСОК ИСПОЛЬЗОВАННЫХ ИСТОЧНИКОВ**

Сайты:

[ТОП-5 Самых защищённых и безопасных мессенджеров 2023 года (trashexpert.ru)](https://trashexpert.ru/software/security/best-secure-and-encrypted-messaging-apps/?ysclid=le6ozkjgvn440359456)

[Самые безопасные приложения для обмена сообщениями (kaspersky.ru)](https://www.kaspersky.ru/resource-center/preemptive-safety/messaging-app-security?ysclid=le6ox5h1ng504063210)

[WhatsApp, Signal и Telegram с треском провалили банальнейший тест на безопасность - CNews](https://www.cnews.ru/news/top/2020-09-17_samye_bezopasnye_messendzhery?ysclid=le6p4khgio280206983)

[Особенности шифрования популярных мессенджеров: выбираем самый безопасный / Хабр (habr.com)](https://habr.com/ru/company/first/blog/668736/)

[Как защитить аккаунт ВКонтакте от взлома и спама | Блог Касперского (kaspersky.ru)](https://www.kaspersky.ru/blog/vk-security-and-privacy-settings/22858/?ysclid=le6v1cjqtf455513341)

<https://www.kaspersky.ru/blog/twitter-security/11638/>

<https://xaer.ru/chto-oznachaet-zamok-v-twitter/>

[http://yaslit.ru/bezopasno-li-ispolzovat-twitter/](http://yaslit.ru/bezopasno-li-ispolzovat-twitter/%20)

[https://trashexpert.ru/software/security/best-secure-and-encrypted-messaging-apps/](https://trashexpert.ru/software/security/best-secure-and-encrypted-messaging-apps/%20)

[https://blog.themarfa.name/12-zashchishchionnykh-miessiendzhierov-dlia-biezopasnogho-obshchieniia/](https://blog.themarfa.name/12-zashchishchionnykh-miessiendzhierov-dlia-biezopasnogho-obshchieniia/%20)

<https://habr.com/ru/company/group-ib/blog/522178/>

<https://news.rambler.ru/scitech/48407804-top-5-samyh-zaschischennyh-messendzherov-dlya-bezopasnogo-obscheniya/>

<https://trueconf.ru/blog/reviews/bezopasnyy-messendzher.html>

<https://timeweb.com/ru/community/articles/kakoy-messendzher-samyy-bezopasnyy-i-pochemu>

<https://www.ferra.ru/review/apps/top-encryption-messengers.htm>

<https://ria.ru/20221104/messendzher-1829145920.html>

**ПРИЛОЖЕНИЕ**

ТЕРМИНЫ И ОПРЕДЕЛЕНИЯ

В настоящем отчете о НИР применяют следующие термины с соответствующими определениями:

1. Парсинг - это сбор и сортировка данных с определенными параметрами.
2. Сквозное шифрование - способ передачи данных, в котором только пользователи, участвующие в общении, имеют доступ к сообщениям. Таким образом, использование сквозного шифрования не позволяет получить доступ к криптографическим ключам со стороны третьих лиц.
3. Двухфакторная аутентификация - это метод идентификации пользователя при помощи запроса аутентификационных данных двух разных типов, что обеспечивает двухслойную, а значит, более эффективную защиту аккаунта от несанкционированного проникновения.
4. MITM - Вид атаки в криптографии и компьютерной безопасности, когда злоумышленник тайно ретранслирует и при необходимости изменяет связь между двумя сторонами, которые считают, что они непосредственно общаются друг с другом.
5. P2P шифрование - Стандарт, установленный Советом по стандартам безопасности PCI для повышения безопасности электронных финансовых транзакций.
6. SSL - Криптографический протокол, который подразумевает более безопасную связь. Он использует асимметричную криптографию для аутентификации ключей обмена, симметричное шифрование для сохранения конфиденциальности, коды аутентификации сообщений для целостности сообщений.
7. Perfect Forward Secrecy - Свойство некоторых протоколов согласования ключа, которое гарантирует, что сессионные ключи, полученные при помощи набора ключей долговременного пользования, не будут скомпрометированы при компрометации одного из долговременных ключей.
8. Github - Крупнейший веб-сервис для хостинга IT-проектов и их совместной разработки.
9. Фишинг - Вид интернет-мошенничества, целью которого является получение доступа к конфиденциальным данным пользователей - логинам и паролям. Это достигается путём проведения массовых рассылок электронных писем от имени популярных брендов, а также личных сообщений внутри различных сервисов.
10. TLS - Криптографические протоколы, обеспечивающие защищённую передачу данных между узлами в сети Интернет. TLS и SSL используют асимметричное шифрование для аутентификации, симметричное шифрование для конфиденциальности и коды аутентичности сообщений для сохранения целостности сообщений.
11. URL - Система унифицированных адресов электронных ресурсов, или единообразный определитель местонахождения ресурса. Используется как стандарт записи ссылок на объекты в Интернете.

ПЕРЕЧЕНЬ СОКРАЩЕНИЙ И ОБОЗНАЧЕНИЙ

В настоящем отчете о НИР применяют следующие сокращения и обозначения:

1. MITM – Man in the middle
2. TLS - Transport Layer Security
3. SMS - Short Message Service
4. URL - Uniform Resource Locator
5. HTTPS - Hypertext Transfer Protocol Secure

В приложения могут быть включены:

- промежуточные математические доказательства и расчеты;