Инженерный вестник Дона, №8 (2024)
ivdon.ru/ru/magazine/archive/n8y2024/9416

Сравнительный обзор безопасности популярных корпоративных мессенджеров

А.М. Коренева, И. Саварин

Финансовый университет при Правительстве Российской Федерации, Москва

Аннотация: В данной статье рассматривается защищенность популярных в настоящее время корпоративных приложений для мгновенного обмена сообщениями (мессенджеры). Проведен сравнительный анализ безопасности некоторых решений для корпоративного пользования. Основным результатом проведенного обзора являются выводы о преимуществах и недостатках рассмотренных систем, которые могут быть использованы организациями для выбора подходящего решения.
Ключевые слова: Информационная безопасность, корпоративный мессенджер, обмен сообщениями, внутренние коммуникации, системы мгновенного обмена сообщениями, сквозное шифрование.

1. Введение

В современном мире системы мгновенного обмена сообщениями (далее – мессенджеры) являются неотъемлемой частью повседневной жизни. Мессенджеры позволяют оперативно и удобно обмениваться как личной, так и рабочей информацией, но в то же время имеют ограничения и особенности, связанные с информационной безопасностью (далее – ИБ) при их использовании.

На данный момент проведено большое количество сравнительных обзоров защищенности популярных решений для персональной коммуникации [1,2]. Но их использование не позволяет достичь уровня защищенности, необходимого для рабочей коммуникации в организациях, так как возникает риск утечки конфиденциальных данных. Персональные мессенджеры не обладают гибкой настройкой политик ИБ и не позволяют компании в полной мере контролировать передаваемую информацию. Сравнительный обзор корпоративных мессенджеров, используемых в Российской Федерации, видится важным предварительным этапом исследования, направленного на возможность построения корпоративного

мессенджера, обеспечивающего безопасный мгновенный обмен информацией как внутри организаций, так и между ними.

В статье представлен сравнительный обзор популярных корпоративных мессенджеров: Mattermost, Rocket.Chat и Slack. Рассмотрены их основные характеристики, функциональные возможности, методы обеспечения ИБ, а также удобство использования с точки зрения ИБ. Под методами обеспечения ИБ подразумеваются меры, механизмы и технологии, применяемые для обеспечения конфиденциальности и целостности информации, передаваемой через приложение, такие, как шифрование данных, контроль доступа к данным, аутентификация пользователей, контроль целостности данных, возможности аудита. Удобство использования с точки зрения ИБ относится к тому, насколько легко и удобно пользователи могут применять меры безопасности без ущерба для функциональности системы. Это включает такие аспекты, как простота использования паролей, наличие интуитивно понятных интерфейсов и функций безопасности, а также минимизацию количества шагов, необходимых для выполнения задач безопасности. Некоторые сервисы предоставляют функции, предназначенные для повышения безопасности данных, например, возможность отправки самоуничтожающихся сообщений, использование секретных чатов, установление ограничений на уровне устройства (блокировка создания скриншотов или записи экрана), а также установка ограничений на поверхность использования. В то же время подобные меры могут вызывать неудобства для пользователей.

Основным результатом проведенного обзора являются выводы о преимуществах и недостатках рассмотренных систем, которые могут быть использованы организациями для выбора подходящего решения. Данная работа является начальным этапом исследования, целью которого является изучение возможностей построения защищённого корпоративного

мессенджера. Результаты обзора могут быть полезны для организаций, которые стремятся усовершенствовать обеспечение безопасности своих информационных ресурсов и данных, а также обеспечить конфиденциальность данных своих сотрудников и клиентов.

2. Анализ критериев безопасности корпоративных мессенджеров

Мессенджер – это средство для обмена сообщениями в режиме реального времени с другими людьми через сеть Интернет и отслеживания хода данного разговора [3]. Мессенджеры позволяют пользователям отправлять текстовые сообщения, фотографии, видео, аудиофайлы и другие виды контента [4]. Они могут быть доступны через различные платформы, такие как приложения для мобильных устройств, компьютерные программы, веб-браузеры. Мессенджеры обеспечивают удобство и скорость коммуникации, что делает их популярными среди пользователей и организаций.

Однако использование мессенджеров также имеет свои ограничения и недостатки, связанные с безопасностью данных. Некоторые мессенджеры могут собирать и передавать данные пользователей третьим лицам, что может представлять угрозу для конфиденциальности. Кроме того, мессенджеры могут быть подвержены различным видам кибератак. Мессенджеры являются важной частью повседневной жизни современного человека, но их использование требует осознанного подхода к безопасности и приватности данных.

Одним из главных критериев на текущий момент является защищенность личной информации, чем является, в частности, переписка между пользователями. Когда идет речь о рабочей коммуникации, следует учитывать принцип «work-life balance», который указывает на необходимость разграничения зон программного обеспечения (далее – ПО). Это означает необходимость определения границ использования рабочего и личного ПО.

Например, в некоторых компаниях запрещено использовать личные мессенджеры для рабочих целей. Применение популярных мессенджеров, таких как Telegram или WhatsApp для обмена рабочей информацией не позволяет организациям контролировать циркуляцию рабочих данных, что может привести к рискам ИБ, таким как утечка конфиденциальной информации, нарушение политик безопасности организации и кибератакам. Из этого можно сделать вывод, что вышеперечисленные средства коммуникации не полностью подходят для корпоративной коммуникации, так как компаниям в текущее время стремительной цифровизации крайне важно сохранить конфиденциальность данных. Данные системы коммуникации в рабочем процессе не рекомендуется использовать.

Основное различие между персональными и корпоративными мессенджерами заключается в их функциональности. Различия возникают в механизмах аутентификации, методах авторизации, контроле доступа к данным и других возможностях, которые в личных коммуникациях обычно не используются. Из основных функций корпоративных средств обмена сообщениями можно выделить следующие:

1. Аутентификация пользователей. Имеются различные способы подтверждения личности пользователя: телефон, внутренний домен, внутренняя система аутентификации. Обязательным пунктом является второй фактор, как правило, это одноразовые коды OTP (One time password).

2. Контроль доступа. Закрытие доступа после увольнения сотрудника, ограничение времени жизни сессии, контроль доступа по геолокации, контроль доступа по типу сети.

3. Наличие средств контроля за утечками информации (DLP – Data Leakage Protection).

4. Наличие встроенных антивирусных проверок передаваемых медиа файлов для защиты внутренней инфраструктуры

5. Централизованное хранение данных на серверах компании. Хранение на внешних сервисах создаёт риск неправомерного доступа к информации со стороны третьих лиц.

6. Интеграции с вспомогательным ПО, например, календарь и платформы разработки.

Сформулируем критерии защищенности применительно к трем группам объектов: защищаемые данные, обеспечиваемые качества и вспомогательные функции. Рассмотрим каждую группу подробнее.

Защищаемые данные в мессенджере – это информация, которую организация хочет защитить от несанкционированного доступа или использования. Такой информацией может быть рабочая переписка, фотографии, видео, документы и другие файлы, которые работник отправляет через мессенджер. Также к защищаемым данным относятся метаданные, ключи шифрования и другая техническая информация, используемая приложением. Для защиты этих данных используются различные методы, такие как шифрование, двухфакторная аутентификация, парольная защита и другие. Таким образом, к защищаемым данным относятся:

1.Ключевые данные. К этой группе данных относятся криптографические ключи и данные, необходимые для функционирования криптографической подсистемы корпоративного мессенджера.

2.Полезная нагрузка. К этой группе данных относится рабочая переписка, файлы, медиа-данные и т.д.

3.Вспомогательные данные. Под вспомогательными данными подразумевается техническая информация, используемая приложением (метаданные, команды протокола, технические данные).

Мессенджер должен обладать определенными качествами, чтобы обеспечивать защищенность пользователей и данных. Выделим основные качества безопасности и рассмотрим подробнее каждое из них:

1.аутентификация:

a) аутентификация данных (целостность данных);

b) аутентификация пользователей;

2. конфиденциальность:

a) шифрование данных при пересылке;

b) шифрование данных при хранении;

c) конфиденциальность данных при аутентификации и авторизации пользователей.

Аутентификация – это обеспечение гарантии того, что заявленные характеристики субъекта или объекта являются подлинными (*ПНСТ 799-2022 Информационные технологии. Криптографическая защита информации. Термины и определения*). Данный процесс может осуществляться с помощью аутентифицирующей информации пользователя, например, пароля, одноразового кода, отпечатка пальца [5]. В контексте информационных технологий аутентификация происходит при проверке личности пользователя при входе в систему или при выполнении определённых действий.

Аутентификация данных – это проверка и подтверждение того, что набор данных (сообщение, документ) был создан именно заявленным источником. Подразумевается как проверка целостности данных, так и проверка их источника. Для аутентификации данных используются различные методы, такие как электронные подписи, функции хэширования, режимы работы шифров, предназначенные для выработки имитовставки, аутентифицированное шифрование и другие. Эти методы позволяют

убедиться в том, что данные не были изменены или подделаны, а также в том, что они получены от доверенного источника.

Аутентификация пользователей – это проверка одной из сторон того, что взаимодействующая с ней сторона именно та, за которую себя выдаёт. Существуют различные методы аутентификации пользователей, такие, как пароль, отпечаток пальца, сканирование лица и другие. Каждый метод имеет свои преимущества и недостатки, и выбор метода зависит от требований безопасности и удобства использования. Стоит учесть, что аутентификация только устанавливает, правильно ли было заявлено утверждение идентичности и не предполагает, что аутентифицированная сторона может делать [6]. Аутентификация в мессенджерах является важнейшим элементом защиты данных, так как позволяет предотвратить несанкционированный доступ к личной информации пользователей.

Также отдельно можно выделить критерий – вспомогательные функции безопасности. Некоторые решения предоставляют своим пользователям функции, которые призваны улучшить безопасность данных, например, самоуничтожающиеся сообщения, ограничения на уровне устройства (запреты скриншотов, записи экрана), ограничения поверхности пользования, но в то же время могут причинять неудобства пользователям.

На рис. 1 приведена диаграмма рассматриваемых в данной статье критериев защищенности корпоративных мессенджеров.

3.Анализ популярных решений для корпоративной коммуникации на соответствие выделенным критериям безопасности

Задачей данного раздела является анализ популярных корпоративных мессенджеров на соответствие критериям, описанным в разделе 2 и изображенным на рис. 1.

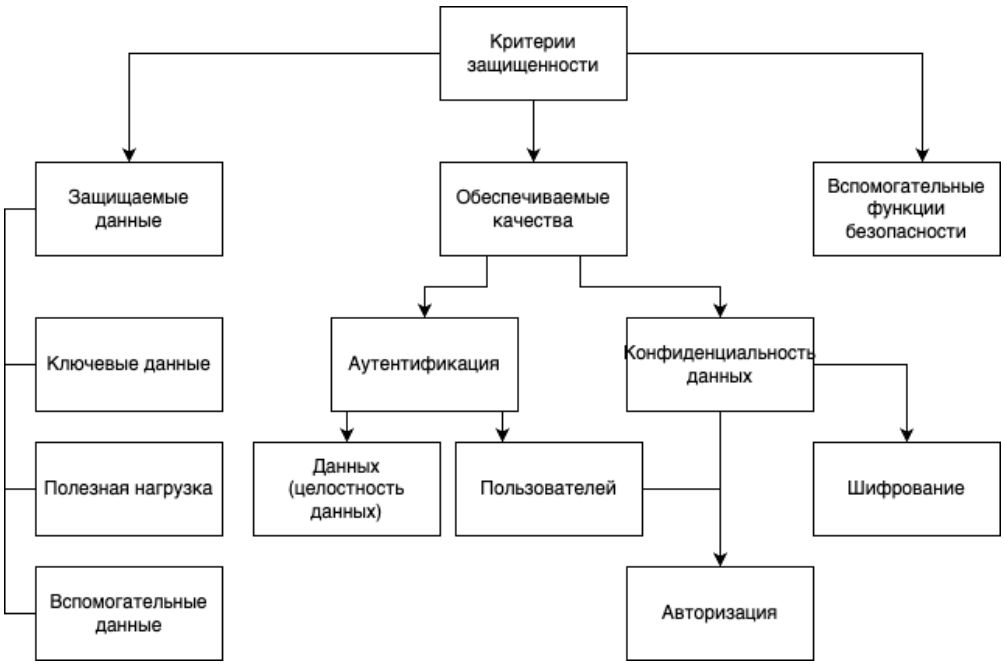

Рис. 1. – Диаграмма критериев защищенности корпоративных мессенджеров

3.1 Обзор Rocket.Chat

Корпоративный мессенджер Rocket.Chat – это ПО, предназначенное для обмена сообщениями и файлами между сотрудниками компании. Размещение Rocket.Chat возможно как в облачной инфраструктуре, так и на собственных серверах организации. Для шифрования данных при передаче используется сквозное (end-to-end) шифрование.

Приложение использует следующие ключевые данные:

1.Ключевая пара клиента RSA-OAEP, длина 2048 бит (RSA-OAEP стандартизирован в RSA PKCS #1 версии 2.1 и является частью стандартов ANSI X9.44, IEEE P1363, ISO 18033-2 и SET [7, 8]).

2.Мастер-ключ AES-CBC, длина 256 бит, 1000 итераций применения криптографического преобразования к паролю, сгенерированному клиентским приложением.

3.Ключ сессии AES-CBC, длина 128 бит [8].

При входе в систему клиент автоматически генерирует пароль для выработки мастер-ключа и просит пользователя сохранить его. Также при

первом входе в приложение клиент генерирует ключевую пару, предварительно проверяя ее наличие в базе данных сервера. Если такая пара по идентификатору пользователя уже существует – она не генерируется, а берётся из базы данных. Если нет – закрытый ключ зашифровывается с помощью мастер-ключа, а затем ключевая пара клиента (зашифрованный закрытый ключ и открытый ключ) отправляется на сервер и сохраняется в базе данных. На рис. 2 изображена схема генерации ключей при первом входе в приложение Rocket.Chat.

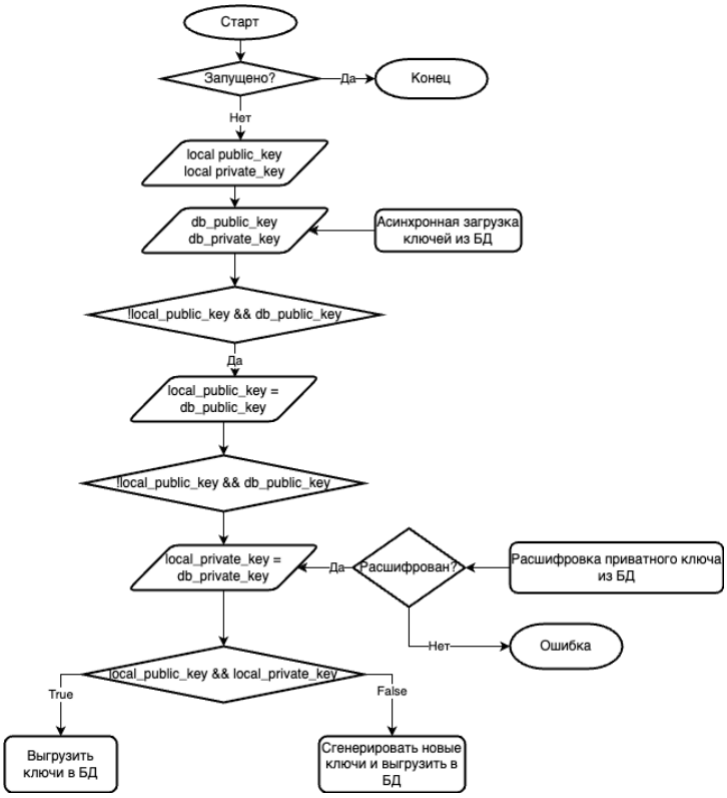

Рис. 2. – Схема генерации ключей при первом входе в Rocket.Chat

Загруженный открытый ключ используется как есть, а зашифрованный закрытый ключ сначала расшифровывается с помощью мастер-ключа на стороне клиента. Если мастер-ключ не был расшифрован на стороне клиента, то пользователю предлагается создать мастер-ключ повторно. Открытый ключ используется для шифрования с помощью алгоритма RSA-OAEP-2048 постоянного ключа сессии, из которого вырабатываются сессионные ключи,

используемые непосредственно для шифрования переписки с помощью алгоритма AES-128 в режиме CBC. Сквозное шифрование в Rocket.Chat работает как для peer-to-peer (чата с пользователем), так и для групповых чатов. Это связано с тем, что в реализации приложения все чаты являются групповыми и чат с пользователем – это групповой чат с двумя участниками [8].

Для обеспечения аутентификации пользователей поддерживаются следующие методы:

1. Базовая аутентификация – создание учётной записи с помощью электронной почты и пароля.

2. Облегчённый протокол доступа к каталогам LDAP (Lightweight Directory Access Protocol). Протокол обеспечивает простой доступ к информации о пользователях. Обычно он используется в организациях, где необходима централизованная аутентификация и авторизация [9, 10].

3. Security Assertion Markup Language (SAML). Это открытый стандарт, позволяющий осуществлять единый вход (SSO – Single Sign-On) для нескольких приложений с одним набором учётных данных [10].

4. Open Authorization (OAuth). Открытый протокол, использующий токены для предоставления доступа к сторонним сервисам без раскрытия учетных данных пользователя [10].

5. OpenID Connect: уровень идентификации поверх OAuth 2.0, обеспечивающий единый вход для различных веб-приложений [10].

6. Внешняя аутентификация: Для прямого входа с веб-сайта или стороннего приложения [10].

Ко всему вышеперечисленному имеется возможность подключения многофакторной аутентификации (MFA – Multifactor authentication), что является преимуществом для организаций, так как позволяет исключить возможность подключения к корпоративной переписке лиц, не состоявших в

компании. Это достигается путём использования различных факторов аутентификации, например, одноразовый пароль, отпечаток пальца или аппаратный токен.

Из дополнительных возможностей можно отметить, что для конфиденциальности “чувствительной” информации в приложении предусмотрена система предотвращения утечки данных (под “чувствительной” понимается информация, которая может нанести ущерб компании или её сотрудникам, в случае, если она станет доступна третьим лицам). Данная функциональность предотвращения утечек может быть сконфигурирована с помощью наборов правил, которые будут срабатывать при отправке сообщений.

К преимуществам Rocket.Chat также относится возможность его размещения на собственных серверах организации.

Недостатками данного мессенджера (исходя из отзывов компаний) являются: проблемы со стабильностью работы и сложность адаптации под корпоративные цели (сложность кастомизации) [11].

3.2 Обзор Mattermost

Mattermost – платформа с открытым исходным кодом, которая обеспечивает безопасную совместную рабочую коммуникацию команд. Данное приложение разработано для использования в организациях и предоставляет им полный контроль над своими данными. Приложение Mattermost стало популярно в РФ и является качественным аналогом другого зарубежного решения – Slack [12]. Mattermost предлагает множество функций, помогающих обеспечить безопасность коммуникаций.

Защиту передаваемой информации между сервером и клиентом обеспечивает протокол TLS 1.2. По умолчанию в конфигурации определены следующие криптонаборы:

1.TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256

2. TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384

3. TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256

4. TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384

5. TLS_RSA_WITH_AES_128_GCM_SHA256

6. TLS_RSA_WITH_AES_256_GCM_SHA384

Обеспечение безопасности хранимых на сервере или локально данных достигается средствами программного и аппаратного шифрования диска [13]. Сквозное шифрование приложение не поддерживает.

Доступность пользовательских данных по умолчанию обеспечивается за счёт хранения полной истории, включая удаление и редактирование сообщений. Дополнительно можно сконфигурировать политики хранения истории переписки под требования организации.

По умолчанию приложение Mattermost не имеет встроенной защиты от пересылки вредоносного программного обеспечения (ВПО). Тем не менее, администраторы могут использовать дополнительные плагины для интеграции антивирусных систем в мессенджер. Это поможет защитить пользователей от потенциальных угроз, связанных с пересылкой ВПО. Однако стоит отметить, что использование сторонних плагинов может представлять определенные риски, связанные с использованием устаревших антивирусных баз данных.

Дополнительно предоставляются возможности для контроля исполнения внутренних требований компаний, например, конфигурирование текста push-уведомлений для исключения из них конфиденциальной информации [14].

Безопасная аутентификация пользователей обеспечивается технологиями Active Directory, LDAP или SSO (Single Sign-On). Для более надёжной защиты имеется возможность подключения многофакторной

аутентификации (MFA). Вторым фактором в данном случае выступает одноразовый код, генерируемый с помощью специальных программных средств генерации OTP (One time password). Для усиления безопасности и предотвращения неправомерного доступа имеется возможность конфигурирования политик контроля и разграничения доступа: расширенные требования к паролям и адресу электронной почты, разграничение доступов определённых команд к тем или иным группам или каналам, ограничение пересылки файлов [15]. На рис. 3 изображена схема архитектуры Mattermost [16].

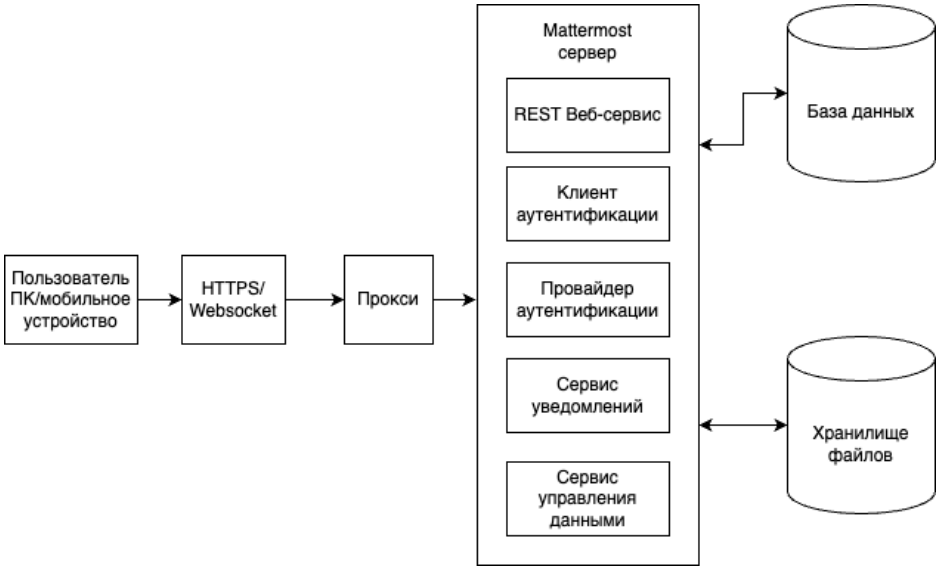

Рис. 3. – Архитектура Mattermost

3.3 Обзор Slack

Приложение Slack считается одним из самым популярных в командах разработки. Популярность оно приобрело из-за обширной интеграции с различными сервисами, используемыми в жизненном цикле разработки ПО. Также Slack имеет широкую функциональность для коммуникации, отправки файлов, планирования рабочего времени. Приложение доступно на всех популярных платформах (Web, Windows, macOS, Linux, iOS, Android).

С точки зрения безопасности передаваемых данных, по словам разработчика, программа направлена на предотвращение несанкционированного доступа к данным клиентов [17].

При передаче все данные в трафике Slack защищаются с помощью протоколов TLS 1.2 с использованием алгоритма шифрования AES-256 и алгоритма хэширования SHA2. Для защиты данных любого типа, хранимых локально, применяется стандарт FIPS 140-2. Стоит отметить, что шифрование применятся ко всем типам данных, в том числе к локальным базам данных и резервным копиям.

Как заявляет разработчик, все криптографические ключи хранятся на сервере в изолированной сети с ограниченным доступом. Также заявлено, что в приложение внедрены меры обеспечения ИБ при выработке, хранении и передаче ключевых данных [17]. В дополнение к базовой системе безопасности данных, разработчик предоставляет возможность подключения ещё одного слоя защиты при использовании Enterprise версии приложения. Расширенная версия позволяет использовать собственные криптографические ключи организации, вместо базовых ключей приложения. Это позволяет администраторам полностью контролировать данные, вносит прозрачность в процессы зашифрования и расшифрования сообщений (вся информация фиксируется), а также производить отзыв и замену ключей, когда это необходимо [18].

Доступность данных достигается регулярным резервным копированием. В то же время все данные хранятся в нескольких разных центрах хранения информации для того, чтобы обеспечивать доступность даже в случае инцидента [17].

Для аутентификации разработчик приложения рекомендует использовать технологию OAuth 2.0. Дополнительно с помощью плагинов можно подключить интеграцию с Active Directory и различными SSO

провайдерами. Имеется возможность подключения двухфакторной аутентификации с помощью приложения для генерации одноразовых кодов, либо с помощью SMS.

Одним из главных преимуществ, отличающих Slack от других решений, является большое разнообразие интеграций с другими сервисами, как связанных с безопасностью, так и обычных утилит для удобства работы пользователей.

Среди недостатков приложения Slack следует отметить: отсутствие поддержки сквозного (E2E) шифрования в криптографической подсистеме и невозможность размещения приложения на собственных серверах компании, что означает зависимость от разработчика.

Исходя из пользовательского опыта, минусом также является отсутствие возможности настройки внешнего вида приложения под стиль организации. Стоит также отметить, что в настоящий момент оплата корпоративной лицензии в РФ недоступна.

3.4 Сравнение рассмотренных приложений

Результат сравнения мессенджеров, рассмотренных в 3.1-3.3, на соответствие критериям, описанным в разделе 2, представлен в таблице 1.

Таблица 1 – Результат сравнения мессенджеров.

	Rocket.Chat	Mattermost	Slack
	1	2	3
Защищаемые данные	Все данные, как ключевые так и вспомогательные, зашифровываются и локально, и при передаче		
Целостность данных	Нет информации	Целостность обеспечивается посредством протокола TLS [19].	
Доступность данных	Обеспечивается за счёт хранения данных в локальных БД. Имеется возможность создания резервных копий.		Все данные хранятся на серверах Slack, без

	Данные можно		возможности
	1	2	3
	локализовать на собственных серверах.		развёртывания на серверах компании. Проводится регулярное резервное копирование.
Конфиденциальность данных	Возможность подключить DLP плагин.	Контроль доступа к данным с помощью настроек политик конфиденциальности компании.	Возможность подключения DLP плагинов. В Enterprise версии имеются расширенные настройки безопасности данных
Аутентификация пользователей	Basic, LDAP, SSO, OAuth, OpenID, External, MFA	ActiveDirectory, LDAP, SSO, MFA	OAuth 2.0, LDAP (с помощью плагинов), MFA
Шифрование	Имеется поддержка E2EE. AES-CBC-256 с RSA-OAEP-2048 + AES-CBC-128 для ключа сессии	AES-256 с 2048-битным RSA + дополнительное шифрование для разных функций + TLS. Нет поддержки E2EE	TLS 1.2 + AES-256 + SHA2. Нет поддержки E2EE

Вспомогательные функции	OpenSource Множество интеграций Встроенные механизмы внутреннего контроля безопасности	OpenSource Множество интеграций DLP плагин Плагины для интеграции антивирусных систем	Закрытый исходный код Множество интеграций Богатый SDK для создания ботов

Заключение

В данной статье рассмотрены популярные решения для корпоративной коммуникации – приложения Rocket.Chat, Mattermost, Slack. Выделены критерии безопасности, которым по мнению авторов должны соответствовать корпоративные мессенджеры.

Из вышеперечисленных приложений оптимальным решением с точки зрения ИБ по мнению авторов является Rocket.Chat, за счёт грамотно спроектированной криптографической подсистемы, возможности конфигурирования и размещения на собственных серверах организации. Но следует учитывать, что данное решение является довольно молодым, и имеет недостатки, такие, как отсутствие вспомогательных функций безопасности и сложность кастомизации.

Наиболее удобным в плане взаимодействия пользователей является приложение Slack. Данное решение существует довольно давно и заслужило репутацию удобного мессенджера за счёт всевозможных интеграций, простоты работы, администрирования и настройки. Однако данное решение не подходит для организаций на территории РФ из-за невозможности оплаты лицензий. Кроме того, Slack не полностью соответствует рассмотренным критериям безопасности, в частности, не поддерживает локализацию на серверах компании. Альтернативным решением является Mattermost,

который во многом похож на Slack, но обладает более гибкими возможностями настройки и развёртывания в корпоративной среде.

Выполненный обзор и анализ являются начальным этапом исследования, целью которого является изучение возможностей построения отечественного защищённого корпоративного мессенджера. Результаты данного обзора могут быть полезны для организаций при выборе корпоративного мессенджера.

Список литературы:

1. Путято М.М., Макарян А.С. Классификация мессенджеров на основе анализа уровня безопасности хранимых данных // Прикаспийский журнал: управление и высокие технологии. 2019. №4 (48). URL: cyberleninka.ru/article/n/klassifikatsiya-messendzherov-na-osnove-analiza-urovnya-bezopasnosti-hranimyh-dannyh (дата обращения: 07.04.2024).

2. Положий Г.А., Тосунова А. Р., Сафарьян О. А., Черкесова Л. В. Сравнительный анализ систем мгновенного обмена сообщениями // Молодой исследователь Дона. 2020. №4 (25). URL: cyberleninka.ru/article/n/sravnitelnyy-analiz-sistem-mgnovennogo-obmena-soobscheniyami (дата обращения: 07.04.2024).

3. Бордукова В.С. Мессенджер // Большая российская энциклопедия: научно-образовательный портал – URL: bigenc.ru/c/messendzher-320bdd/?v=8402770. – Дата публикации: 29.06.2023. – Дата обновления: 15.09.2023

4. Манапова О.Н., Подин М.С. Современные мессенджеры в учебном процессе профессиональной образовательной организации: Сильные и слабые стороны // Инновационное развитие профессионального образования. 2021. №3 (31). URL: cyberleninka.ru/article/n/sovremennye-messendzhery-v-uchebnom-protsesse-professionalnoy-obrazovatelnoy-organizatsii-silnye-i-slabye-storony (дата обращения: 17.03.2024).

5. Иванов В.В., Лубова Е.С., Черкасов Д.Ю. Аутентификация и авторизация // Проблемы Науки. 2017. №2 (84). URL: cyberleninka.ru/article/n/autentifikatsiya-i-avtorizatsiya (дата обращения: 17.03.2024).

6. Акушуев Р.Т. Аутентификация и идентификация как метод защиты информации // E-Scio. 2020. №1 (40). URL: cyberleninka.ru/article/n/autentifikatsiya-i-identifikatsiya-kak-metod-zaschity-informatsii (дата обращения: 17.03.2024).

7. Болдырева А. Strengthening security of RSA-OAEP // Cryptographers' Track at the RSA Conference. - Берлин: Heidelberg: Springer Berlin Heidelberg, 2009. - pp. 399-413.

8. End-to-End Encryption Specifications // Rocket.Chat URL: docs.rocket.chat/customer-center/security-center/end-to-end-encryption-specifications#algorithms-used (дата обращения: 24.03.2024).

9. LDAP // Rocket.Chat. URL: docs.rocket.chat/use-rocket.chat/authentication/ldap (дата обращения: 24.03.2024).

10. Authentication // Rocket.Chat. URL: docs.rocket.chat/use-rocket.chat/authentication (дата обращения: 24.03.2024).

11. Лучшие корпоративные мессенджеры 2024. // Корпоративный мессенджер современных команд URL: pachca.com/blog-posts/luchshie-korporativnye-messendzhery-2024 (дата обращения: 24.03.2024).

12. Mattermost overview // Mattermost Documentation. URL: /docs.mattermost.com/about/product.html (дата обращения: 17.03.2024).

13. Transmission security // Mattermost Documentation. URL: docs.mattermost.com/about/security.html#transmission-security (дата обращения: 17.03.2024).

14. Integrity and audit controls // Mattermost Documentation. URL: docs.mattermost.com/about/security.html#integrity-and-audit-controls (дата обращения: 17.03.2024).

15. Authentication safeguards // Mattermost Documentation. URL: docs.mattermost.com/about/security.html#authentication-safeguards (дата обращения: 17.03.2024).

16. Architecture overview // Mattermost Documentation. URL: docs.mattermost.com/getting-started/architecture-overview.html#architecture-overview (дата обращения: 24.03.2024).

17. Protecting Customer Data // Security at Slack. URL: a.slack-edge.com/80588/marketing/downloads/security/Security_White_Paper_2019.pdf (дата обращения: 24.03.2024).

18. Enterprise Key Management comes to Slack Enterprise Grid // Slack is your productivity platform | Slack URL: slack.com/blog/transformation/introduction-enterprise-key-management-for-security (дата обращения: 14.04.2024).

19. The Transport Layer Security (TLS) Protocol Version 1.1 // The RFC Series URL: rfc-editor.org/rfc/rfc4346#section-1 (дата обращения: 14.04.2024).

References

1. Putyato M.M., Makaryan A.S. Prikaspiiskii zhurnal: upravlenie i vysokie tekhnologii. 2019. №4 (48). URL: cyberleninka.ru/article/n/klassifikatsiya-messendzherov-na-osnove-analiza-urovnya-bezopasnosti-hranimyh-dannyh (date assessed: 07.04.2024).

2. Polozhii G. A., Tosunova A. R., Safar'yan O. A., Cherkesova L. V. Molodoi issledovatel' Dona. 2020. №4 (25). URL: cyberleninka.ru/article/n/sravnitelnyy-analiz-sistem-mgnovennogo-obmena-soobscheniyami (date assessed: 07.04.2024).

3. Bordukova V. S. Messenger Bol'shaya rossiiskaya entsiklopediya: nauchno-obrazovatel'nyi portal. URL: bigenc.ru/c/messendzher-320bdd/?v=8402770. Data publikatsii: 29.06.2023. date assessed: 15.09.2023

4. Manapova O.N., Podin M.S. Innovatsionnoe razvitie professional'nogo obrazovaniya. 2021. №3 (31). URL: cyberleninka.ru/article/n/sovremennye-messendzhery-v-uchebnom-protsesse-professionalnoy-obrazovatelnoy-organizatsii-silnye-i-slabye-storony (date assessed: 17.03.2024).

5. Ivanov V.V., Lubova E.S., Cherkasov D.Yu. Problemy Nauki. 2017. №2 (84). URL: cyberleninka.ru/article/n/autentifikatsiya-i-avtorizatsiya (date assessed 17.03.2024).

6. Akushuev R.T. E-Scio. 2020. №1 (40). URL: cyberleninka.ru/article/n/autentifikatsiya-i-identifikatsiya-kak-metod-zaschity-informatsii (date assessed: 17.03.2024).

7. Boldyreva A. Cryptographers' Track at the RSA Conference. Berlin: Heidelberg: Springer Berlin Heidelberg, 2009. pp. 399-413.

8. Specifications Rocket.Chat. URL: docs.rocket.chat/customer-center/security-center/end-to-end-encryption-specifications#algorithms-used (date assessed: 24.03.2024).

9. Rocket.Chat. URL: docs.rocket.chat/use-rocket.chat/authentication/ldap (date assessed: 24.03.2024).

10. Rocket.Chat. URL: docs.rocket.chat/use-rocket.chat/authentication (date assessed: 24.03.2024).

11. Korporativnyi messendzher sovremennykh komand [The best corporate messengers of 2024]. URL: pachca.com/blog-posts/luchshie-korporativnye-messendzhery-2024 (date assessed: 24.03.2024).

12. Mattermost Documentation. URL: docs.mattermost.com/about/product.html (date assessed: 17.03.2024).

13. Mattermost Documentation. URL: docs.mattermost.com/about/security.html#transmission-security (date assessed: 17.03.2024).

14. Mattermost Documentation. URL: docs.mattermost.com/about/security.html#integrity-and-audit-controls (date assessed: 17.03.2024).

15. Mattermost Documentation. URL: docs.mattermost.com/about/security.html#authentication-safeguards (date assessed: 17.03.2024).

16. Mattermost Documentation. URL: docs.mattermost.com/getting-started/architecture-overview.html#architecture-overview (date assessed: 24.03.2024).

17. Slack. URL: a.slack-edge.com/80588/marketing/downloads/security/Security_White_Paper_2019.pdf (date assessed: 24.03.2024).

18. Slack. URL: slack.com/blog/transformation/introduction-enterprise-key-management-for-security (date assessed: 14.04.2024).

19. The RFC Series. URL rfc-editor.org/rfc/rfc4346#section-1 (date assessed: 14.04.2024).

Дата поступления: 5.06.2024

Дата публикации: 18.07.2024