Часто задаваемые вопросы

О Mailvelope

- Что такое Mailvelope?
- Какие почтовые сервисы поддерживает Mailvelope?
- Я могу обмениваться зашифрованными письмами только с другими пользователями Mailvelope?
- Работает ли Mailvelope на мобильных устройствах?

Опции шифрования email

- Мой провайдер веб-почты не настроен для работы с Mailvelope. Можно ли всё-таки пользоваться Mailvelope?
- Как настроить новый домен для работы с Mailvelope?
- Как отключить домен от работы с Mailvelope?
- Умеет ли Mailvelope шифровать почтовые вложения?
- Зачем нужна электронная подпись? Как её использовать?
- Как проверить подпись сообщения?
- Что случится, если я сменю адрес email?
- Поддерживает ли Mailvelope функцию N? Если нет, будет ли поддержка в будущем?

Расширенные функции

- Можно ли использовать Mailvelope для шифрования других данных, кроме email?
- Зачем использовать GnuPG, если уже есть OpenPGP.js?
- Как использовать зашифрованные формы с Mailvelope?
- Что такое Web Key Directory? Как его использовать?
- Что такое Autocrypt, как его использовать?

Управление ключами

- Что такое ключ «по умолчанию» в Mailvelope?
- Как импортировать ключ PGP в Mailvelope?
- Как экспортировать мой ключ PGP из Mailvelope?

Сервер ключей

- Что такое сервер ключей Mailvelope? Как его использовать?

Mailvelope Business

- Мы – некоммерческая организация. Можем ли мы воспользоваться Mailvelope Business?
- Нужно ли покупать лицензии всем пользователям в нашей организации?
- Зачем для бизнес-версии Mailvelope нужно соглашение об обработке данных?

Безопасность

- Насколько безопасен Mailvelope?
- Где хранятся мои ключи?
- Насколько защищены закрытые ключи? Может ли кто-то с доступом к моему компьютеру получить доступ и к моему закрытому ключу?
- Как выбрать надёжный пароль для закрытого ключа?
- Как создать резервную копию моих ключей?
- Что делать, если я забыл пароль?
- Как сменить пароль к закрытому ключу?
- Устанавливаю расширение и вижу, что оно хочет доступ к посещённым сайтам, браузерным вкладкам и всем моим действиям в браузере. Это правда необходимо? Зачем?

Ошибки в программе

- Что делать, если Mailvelope не работает должным образом?
- Что включать в отчёт об ошибке?
- Я получил зашифрованное письмо, но вижу только два вложения. Mailvelope не предлагает автоматическую расшифровку.
- Сообщение об ошибке: для зашифрованного письма не найден закрытый ключ
- Mailvelope не удалось распознать установленную версию GnuPG.

Определенные провайдеры веб-почты

- (WEB.DE и GMX) Сервис просит «код восстановления». Где его взять? Из Mailvelope?
- Чтобы выполнить интеграцию с Mailvelope, Google требует дополнительные права доступа для Gmail API. Как Mailvelope обрабатывает мои данные?

Установка

- Как установить Mailvelope?
- Можно ли установить Mailvelope в другие браузеры, кроме Chrome и Firefox?
- Как удалить Mailvelope?

О Mailvelope

Что такое Mailvelope?

Mailvelope – расширение для браузера (в Firefox его иногда называют «дополнением»). Mailvelope добавляет в браузеры Firefox и Chrome шифрование email с помощью технологии PGP.

Mailvelope не требует менять привычную среду, чтобы шифровать email. Если вы используете веб-почту, можно остаться с тем же почтовым провайдером и адресом. Это большой плюс.

Интерфейс Mailvelope дополняет интерфейс веб-почты в браузере. Ваша конфиденциальная информация недоступна почтовому провайдеру. Данные шифруются и расшифровываются на вашем компьютере. Ваш закрытый (секретный) ключ никогда не покидает ваш компьютер. Конфиденциальные письма всегда находятся на серверах провайдера в зашифрованном виде. Вы можете прочесть полученное шифрованное письмо только на своем компьютере и только после ввода пароля к закрытому ключу.

Какие почтовые сервисы поддерживает Mailvelope?

Mailvelope – очень гибкий и настраиваемый инструмент. Он работает с разными почтовыми провайдерами, включая Gmail, Яндекс и др.

Mailvelope появился в 2012 году. С тех пор многие провайдеры веб-почты адаптировали свои сервисы для поддержки Mailvelope API. Благодаря этому шифрование email сильно упростилось. В частности, есть интеграция с немецкими провайдерами WEB.DE, GMX, Posteo, проектом «De-Mail», 1&1, Deutsche Telekom.

Если вы хотите использовать Mailvelope вместе с одним из этих провайдеров, лучше обратиться к справочной системе провайдера. У разных компаний интеграция выполнена по-разному.

Страницы справки (шифрование email с помощью PGP/Mailvelope):

- GMX
- Posteo
- WEB.DE

Авторизованные провайдеры:

- Gmail
- mail.ru
- Outlook.com
- Yahoo
- Zoho Mail

Другие авторизованные провайдеры с поддержкой API:

- mailbox.org
- riseup.net
- Roundcube

Добавить провайдера/сайт всегда можно вручную. См. Как настроить новый домен для работы с Mailvelope?

Я могу обмениваться зашифрованными письмами только с другими пользователями Mailvelope?

Mailvelope использует открытый стандарт OpenPGP. Многие годы ему доверяют как безопасному. Вы можете общаться не только с пользователями Mailvelope, но и со всеми, кто применяет PGP-совместимые программы.

Примеры совместимых программ:

- Enigmail дляThunderbird (macOS, Windows, GNU/Linux)
- Gpg4win для Windows (например, для Outlook)
- GPGtools для mac OS (вместе с Mail, почтовым приложением по умолчанию)

Работает ли Mailvelope на мобильных устройствах?

В настоящее время Mailvelope не работает на мобильных устройствах под управлением Android и iOS. Mailvelope создавался как расширение браузера. Мобильные браузеры имеют ограничения, которые не позволяют Mailvelope функционировать должным образом. Впрочем, некоторые почтовые клиенты поддерживают стандарт OpenPGP для отправки и получения зашифрованных сообщений на Android и iOS.

Сегодня это:

Android:

- FairEmail в связке с OpenKeychain
- K-9 Mail в связке с OpenKeychain
- SqueakyMail в связке с PGP KeyRing
- MailDroid в связке с Flipdog Crypto Plugin

iOS:

- iPGMail
- Canary Mail

Созданные/используемые в Mailvelope ключи можно легко экспортировать и импортировать. Вы сможете пользоваться Mailvelope с тем же email и теми же ключами на своём мобильном устройстве, что и на компьютере. На своей странице помощи провайдер Posteo.de предлагает инструкцию о том, как настроить мобильное PGP-шифрование на Android-устройстве с помощью приложений Squeaky Mail и PGP KeyRing.

Пожалуйста, помните: использование PGP на вашем мобильном устройстве несёт дополнительные риски. Если угрозы серьёзные, лучше не использовать PGP на мобильных устройствах. Особенно это касается Android-устройств. Они часто оказываются без должных обновлений.

Особенности

Мой провайдер веб-почты не настроен для работы с Mailvelope. Можно ли всё-таки пользоваться Mailvelope?

Mailvelope – гибкий инструмент. Если ваш провайдер веб-почты не настроен для использования Mailvelope по умолчанию, его можно настроить вручную. См. также следующий вопрос.

Как настроить новый домен для работы с Mailvelope?

В разделе «Какие почтовые сервисы поддерживает Mailvelope?» говорится, что многие популярные почтовые сервисы настроены на работу с Mailvelope по умолчанию. Ниже сказано, как выполнить эту настройку вручную.

Откройте веб-сайт, который хотите настроить для работы с Mailvelope. Нажмите значок Mailveope в панели браузера. В главном меню выберите «Добавить этот домен». Откроется диалог Mailvelope для настройки нового домена.

В большинстве ситуаций поля «Включено», «Домен» и «API» можно оставить без изменений. После нажатия кнопки «OK» Mailvelope сохранит данные сайта в списке настроенных доменов. Перезагрузите сайт, чтобы активировать Mailvelope.

Как отключить домен от работы с Mailvelope?

Перейдите в раздел «Домены» (из главного меню -> «Панель управления» -> «Настройки»). Наведите курсор на соответствующий домен. Появится значок мусорной корзины. Нажмите на значок и подтвердите удаление. Если вы просто выберете домен, откроется окно с настройками домена. Первый рыжачок позволяет включить или (временно) отключить интеграцию сайта с Mailvelope.

Умеет ли Mailvelope шифровать почтовые вложения?

Да. С помощью соответствующей опции Mailvelope можно легко зашифровать любой файл, а потом отправить его как почтовое вложение. Файл следует шифровать тем же открытым ключом адресата, что и текст письма. Объем файла в настоящее время ограничен 50 Мб, поскольку отправка более крупных файлов обычно не поддерживается почтовыми провайдерами.

Шифрование файлов

Выберите значок Mailvelope в правом верхнем углу браузера. В главном меню выберите «Шифрование файлов». В первом поле нужно указать email получателя. Затем выберите файл(ы) через диалог «Выбрать файл» или перетащите файлы в окно Mailvelope. Когда нажмёте кнопку «Зашифровать», файлы будут зашифрованы для выбранного получателя. Теперь можно скачать файлы, а потом прикрепить их к email как вложения. Зашифрованные файлы можно выбирать как по отдельности, так и с помощью кнопки «Скачать все».

Внимание: при шифровании с помощью Mailvelope файл меняет формат и временно получает расширение для зашифрованных файлов GnuPG (.gpg). После расшифровки файл восстановится в исходном формате.

Расшифровка файлов

Для расшифровки файлов нужно пройти похожие шаги, как для шифрования. В главном меню выберите «Шифрование файлов», а потом в верхнем горизонтальном меню выберите «Расшифровать». Затем выберите файлы через диалог «Выбрать файл» или перетащите файлы в окно Mailvelope. После ввода пароля к закрытому (секретному) ключу будут показаны расшифрованные файлы. Их можно скачать.

Зачем нужна цифровая подпись? Как её использовать?

Цифровая подпись под сообщением гарантирует его аутентичность: вы можете быть уверены, что письмо действительно написал этот человек.

Если в редакторе сообщений Mailvelope нажать кнопку «Настройки», можно увидеть опции для цифровой подписи. Выберите ключ, которым хотите подписать сообщение. Тогда оно будет сначала подписано соответствующим закрытым (секретным) ключом, а после зашифровано.

По ссылке «Добавлять к сообщениям цифровую подпись» можно перейти в настройки Mailvelope и включить подписывание всех исходящих сообщений.

Можно отправлять не зашифрованные, а только подписанные сообщения. Выберите ключ, Mailvelope создаст цифровую PGP-подпись и присоединит её непосредственно к тексту сообщения. Пожалуйста, имейте в виду: содержание письма шифроваться не будет.

Как проверить подпись сообщения?

Если у сообщения есть цифровая подпись, а Mailvelope может определить адрес отправителя, Mailvelope проверит подпись. Тогда в нижней части расшифрованного сообщения появятся надпись «Подписано» и сама цифровая подпись.

Что случится, если я сменю адрес email?

Ваш email (как и ваше имя) служит идентификатором вашего ключа PGP. Но если у вас изменится email, текущий PGP-ключ менять необязательно

менять необязательно.

В этой ситуации у вас есть два основных варианта:

- Можете создать новый ключ для своего адреса email. Откройте управление ключами (главное меню -> «Ключи»), нажмите кнопку «Создать». Продолжайте так, словно используете Mailvelope впервые. Если нужно, обратитесь к нашей документации.
- Можете добавить новый адрес к существующему ключу. Откройте управление ключами (главное меню -> «Ключи») и выберите ключевую пару, для которой хотите добавить адрес email. Под заголовком «Пользовательские ID» вы увидите все почтовые адреса, которые связаны с этим ключом. Нажмите кнопку «Добавить новый» в правой части окна. Можете добавить имя и почтовый адрес. Если нужно, можете удалить ID пользователя старого адреса email.

  Наконец, можно синхронизировать новую запись с сервером ключей, так что ваши собеседники смогут увидеть вас с новым адресом.

Поддерживает ли Mailvelope функцию N? Если нет, будет ли поддержка в будущем?

Если у вас есть предложения, просто напишите сюда: support@mailvelope.com. Мы с радостью рассмотрим их в работе над следующими версиями.

Расширенные возможности

Можно ли использовать Mailvelope для шифрования других данных, кроме email?

Mailvelope можно использовать по-разному. Можно обмениваться PGP-шифрованными файлами или текстами, включая любые вложения, необязательно почтовые. Можно сохранять шифрованные файлы или тексты, например, на USB-флешках или картах памяти, на сайтах или в облачных сервисах. Можно обмениваться шифрованными сообщениями в мессенджерах. Это также неплохой способ избавиться от метаданных.

Если вы хотите использовать Mailvelope таким образом, зайдите в главное меню и выберите «Шифрование файлов». Обратите внимание на кнопку с вопросом «Хотите также зашифровать текст?». Подробнее здесь: «Умеет ли Mailvelope шифровать почтовые вложения?».

Зачем использовать GnuPG, если уже есть OpenPGP.js?

Начиная с версии 3.0 Mailvelope также может работать с программой GnuPG, если та установлена на компьютере (например, в составе пакетов Ggp4win или GPGTools). В главном меню выберите «Панель управления» -> «Настройки» -> «Общие настройки») и выберите ваш вариант OpenPGP. Чтобы использовать «внешнюю» версию PGP в Mailvelope, она должна быть установлена на вашем устройстве.

Для работы с ключами и шифрования пользователь может выбрать OpenPGP.js или установленную на устройстве программу GnuPG. Если возникли проблемы с выбором, пожалуйста, обратите внимание на раздел «Mailvelope не удалось распознать установленную версию GnuPG». Управление ключами со стороны GnuPG может повысить безопасность Mailvelope. В этом случае закрытые ключи будут защищены, если браузер подвергнется атаке. Существует и поддержка токенов безопасности, таких как смарт-карты.

Как использовать зашифрованные формы с Mailvelope?

Mailvelope предлагает веб-разработчикам специальные правила создания форм, согласно которым данные могут быть прочитаны только определённым получателем. Браузерное расширение Mailvelope Browser обеспечивает шифрование и упаковку данных форм в защищённом сообщении OpenPGP.

Техническую документацию по шифрованным формам можно найти в Mailvelope Wiki.

Что такое Web Key Directory? Как его использовать?

Перед тем, как вести шифрованную OpenPGP-переписку, собеседники должны обменяться открытыми ключами. По умолчанию Mailvelope использует для этого собственный сервер ключей. Это упрощает и даже частично автоматизирует обмен ключами.

Web Key Directory – новый стандарт обмена ключами, опирающийся на принцип децентрализации. Ключи можно запрашивать непосредственно у почтового провайдера (если тот поддерживает стандарт). Подробнее см. GnuPG Wiki.

Что такое Autocrypt, как его использовать?

Перед тем, как вести шифрованную OpenPGP-переписку, собеседники должны обменяться открытыми ключами. По умолчанию Mailvelope использует для этого собственный сервер ключей. Это упрощает и даже частично автоматизирует обмен ключами.

Autocrypt – новый способ, при котором для обмена ключами используются заголовки электронных писем. Отправитель автоматически включает свой открытый ключ в заголовок сообщения. Подробнее см. сайт разработчиков Autocrypt.

Управление ключами

Что такое ключ «по умолчанию» в Mailvelope?

Первый ключ, который вы создаёте в Mailvelope сразу после установки, автоматически становится ключом по умолчанию. В списке ключей он так и будет отмечен: «По умолчанию». Ключ по умолчанию можно сменить. Это легко сделать, если выбрать соответствующую пару ключей в списке.

Как импортировать ключ PGP в Mailvelope?

Выберите «Управление ключами», а затем «Импорт».

Есть два варианта:

- **Импорт ключа из файла.** Выберите на диске файл с ключом (расширение *.asc) и импортируйте его в Mailvelope.
- **Импорт ключа из текста.** Скопируйте ключ (можно импортировать несколько ключей сразу) в буфер памяти. Не забудьте включить в свой выбор строки `-----BEGIN PGP PUBLIC KEY BLOCK-----` и `-----END PGP PUBLIC KEY BLOCK-----` . Нажмите кнопку «Импорт ключа из буфера». Ключ появится в локальной связке ключей.

Автоматизация импорта открытых ключей

- **Ключи в сообщениях email.** Mailvelope автоматически распознает открытые ключи в сообщениях электронной почты, если почтовый сервис поддерживает предварительный просмотр вложений. Если Mailvelope распознает ключ, то помечает его значком закрытого конверта. Нажатие на значок открывает диалог импорта, и ключ автоматически добавляется в связку ключей.
- **Ключи на сайтах.** Подобным образом Mailvelope проверяет все сайты в настроенном домене (подробнее см. Как настроить новый домен для работы с Mailvelope?). Mailvelope ищет PGP-ключи, которые могут быть на этих сайтах. Если вы хотите добавить в Mailvelope собеседника (или нескольких), чей ключ опубликован на сайте, настройте соответствующий домен, а затем импортируйте все ключи с сайта, которые Mailvelope способен разобрать.

Как экспортировать мой ключ PGP из Mailvelope?

С помощью функции «Экспорт» ключи можно экспортировать, а затем отправить или сохранить в качестве резервных копий. Эту функцию можно использовать для публикации открытого ключа или хранения копии ключевой пары (открытый + закрытый ключи) в безопасном месте. Мы предлагаем вашему вниманию самые распространённые ситуации. Если вы выберете экспорт ключа через буфер памяти, не забудьте при выборе включить строки `-----BEGIN PGP PUBLIC KEY BLOCK-----`и `-----END PGP PUBLIC KEY BLOCK-----`. Если вы используете в Mailvelope установленную программу GnuPG, пожалуйста, обратите внимание на последний пункт в этом FAQ_.

Экспорт открытого ключа

Выберите «Управление ключами», затем ваш ключ по умолчанию, а потом «Экспорт». Выберите «Открытый» и, если требуется, укажите имя файла. Нажмите «Сохранить», и ваш открытый ключ будет сохранён на компьютере как файл с расширением `.asc`. Этот формат понимают все программы, работающие с PGP. Как вариант, вы можете скопировать ключ в буфер обмена, нажав на одноимённую кнопку. Теперь открытый ключ можно отправить вашему собеседнику, загрузить на сервер ключей, выложить на ваш собственный веб-сайт.

Сохранение своей пары ключей

Найдите в списке ключей вашу ключевую пару по умолчанию. Её можно узнать благодаря метке «По умолчанию». Выберите эту пару, затем выберите «Экспорт», затем «Все». Введите имя файла и сохраните. Ваша ключевая пара сохранится на компьютере как файл с расширением `.asc`. Пожалуйста, обратите внимание на советы по безопасности в разделе «Резервное копирование».

Резервное копирование всей связки ключей

Откройте окно «Управление ключами». Если у вас несколько связок ключей, в правом верхнем углу окна вы увидите опцию выбора; укажите нужную связку. Выберите «Экспорт» в левой части горизонтального меню. Вы можете сохранить все открытые ключи, все закрытые ключи или всю связку ключей («Все»). Укажите имя файла. Нажмите «Сохранить», и связка ключей будет сохранена на вашем устройстве в виде файла с расширением `.asc`. Если в связке есть закрытые ключи, пожалуйста, обратите внимание на рекомендации по безопасности здесь.

Особый случай: использование связки ключей GnuPG

Если для работы с ключами вы используете GnuPG, пожалуйста, имейте в виду: по соображениям безопасности Mailvelope поддерживает экспорт только открытых ключей. Хотите экспортировать ключевую пару или закрытый ключ из GnuPG – используйте сторонние программы.

Сервер ключей

Что такое сервер ключей Mailvelope? Как его использовать?

У Mailvelope есть свой сервер ключей. Это база PGP-ключей с открытым доступом. Представьте, что вам нужно отправить зашифрованное сообщение вашему собеседнику, но у вас нет его ключа. Тогда вы можете поискать ключ на специальном сервере ключей. Более того, вы можете сохранить там свой собственный открытый PGP-ключ, чтобы облегчить жизнь тем, кто хочет вам писать. У сервера ключей Mailvelope есть преимущество: все адреса email, которые там хранятся, уже фактически были проверены. Это неплохая защита от потенциальной кражи личности.

Автоматический поиск ключей

Иногда Mailvelope использует сервер ключей в фоновом режиме. Например, каждый раз, когда вы создаёте новую ключевую пару, Mailvelope загружает ваш открытый ключ на сервер ключей. (Вы можете отключить эту опцию при создании ключей). Когда вы указываете email в поле «Кому» при отправке сообщения, Mailvelope ищет соответствующий открытый ключ на сервере ключей. Если ключ обнаружен, Mailvelope подсветит его зелёным цветом, а если нет – красным.

Эта поисковая опция включена по умолчанию, но её тоже можно отключить. Выберите в настройках «Сервер ключей» и снимите галочку в поле «Использовать сервер ключей Mailvelope».

Загрузка или скачивание ключа вручную

Если вы хотите загрузить ваш ключ вручную или найти ключ другого пользователя, Mailvelope предлагает веб-интерфейс для своего сервера ключей.

Загрузка ключа на сервер

Скопируйте нужный открытый ключ в буфер обмена. Убедитесь, что выбраны строкя - - - - BEGIN PGP PUBLIC KEY BLOCK - - - - и - - - - - END PGP PUBLIC KEY BLOCK - - - -. Вставьте ключ в поле ввода и выберите «Загрузить».

Поиск ключей на сервере ключей

Введите адрес электронной почты или идентификатор ключа (идентификатор ключа делает каждый ключ PGP уникальным). Например, идентификаторы ключей можно найти в разделе Управление ключами в столбце «Идентификатор ключа». Наконец, выберите «Поиск».

Удаление ключа с сервера ключей

Введите email ключа, который хотите удалить, и выберите «Удалить» Учитывайте регистр, иначе ключ можно и не найти. Обратите внимание: при попытке удалить ключ с сервера ключей вы получите письмо со ссылкой. Нужно использовать эту ссылку для завершения удаления.

Mailvelope Business

Мы – некоммерческая организация. Можем ли мы воспользоваться Mailvelope Business?

Для некоммерческих организаций у нас есть тарифный план Mailvelope Nonprofit . Он даёт право бесплатного ипользования Mailvelope группам до **4** человек. У Mailvelope Nonprofit тот же набор функций, что у Mailvelope Business, но без опций для предприятий, которые включены в план Business.

Пожалуйста, обратите внимание:

- Тарифный план Mailvelope Nonprofit ориентирован на **организации**, которые работают в **некоммерческих целях.**
- Во время регистрации, пожалуйста, укажите **доменное имя** вашей организации. Под этим именем должен быть доступен **веб-сайт, открытый для публичного доступа.** По веб-сайту должен чётко прослеживаться некоммерческий характер деятельности вашей организации.
- План Mailvelope Nonprofit активируется сразу после регистрации. Проверка домена происходит позже и может занять некоторое время. Мы оставляем за собой право удалить регистрацию, если она не соответствует нашим правилам.

Регистрация Mailvelope Nonprofit

Нужно ли покупать лицензии всем пользователям в нашей организации?

Нет. В лицензии определено максимальное число пользователей домена, связанного с GSuite. В начале каждого месяца первые залогиненные пользователи автоматически получат бесплатные лицензии. Это позволяет более гибко подходить к максимальному числу лицензий, приобретаемых ежемесячно. Таким образом, вам нужны лицензии только для тех людей, которые активно используют Mailvelope. Если вам понадобится больше лицензий, вы можете увеличить их число в настройках вашего аккаунта Chargebee.

Зачем для бизнес-версии Mailvelope нужно соглашение об обработке данных?

Сквозное шифрование в Mailvelope происходит в программе-клиенте. Соответственно, важные данные покидают ваше устройство уже зашифрованными. Чтобы обеспечить удобство и лёгкость работы с открытыми ключами, мы полагаемся на сервер ключей Mailvelope Key. Если вы выбрали загрузку ключей на наш сервер, туда попадут и ваши персональные данные, которым по закону требуется защита, например, имя и email address. На этот случай у нас есть соглашение о защите данных (mailvelope.com/en/dpa). Там определены роли и ответственность обработчиков данных. Соглашение в подписанном виде может быть предоставлено вашей организации по запросу; достаточно написать на support@mailvelope.com. Пользователи Mailvelope Business также регистрируют аккаунты на платёжной платформе Chargebee.

Безопасность

Насколько безопасен Mailvelope?

Mailvelope обеспечивает сквозное шифрование. Приложение гарантирует (в пределах установленных технических ограничений) защиту важных данных при передаче с одного устройства на другое по потенциально уязвимому каналу, например, по email.

Во время профессиональных аудитов безопасности были протестированы разные сценарии угроз. (Список аудитов Mailvelope)

Аудиторы пришли к выводу, что Mailvelope предлагает безопасное сквозное шифрование. Однако безопасность при работе с Mailvelope зависит от того, насколько защищено ваше устройство. Поэтому мы рекомендуем такие меры безопасности, как регулярное обновление браузера и операционной системы. Мы также советуем использовать надёжные пароли (см. «Как выбрать надёжный пароль для закрытого ключа?»).

Где хранятся мои ключи?

Папка, где Mailvelope хранит ключи, зависит от того, что указано в настройках: «Общие настройки» -> «Настройки OpenPGP».

Вариант по умолчанию (OpenPGP.js)

Mailvelope хранит ключи в файле. Он находится в локальной папке браузера, или в папке пользовательских данных Chrome, или в папке профиля Firefox. Если вы очистите временные данные браузера, ключи Mailvelope не пострадают. Однако если удалить расширение Mailvelope из Chrome или Firefox, ключи будут также удалены из системы.

Если ключами управляет GnuPG

Если в качестве шифровального средства вы выбрали программу GnuPG на своём компьютере («Общие настройки» -> «Настройки OpenPGP»), управлять ключами будет эта программа. Обычно это происходит в связи с установкой GPG4Win или GPGTools).

Насколько защищены закрытые ключи? Может ли кто-то с доступом к моему компьютеру получить доступ и к моему закрытому ключу?

Mailvelope хранит и экспортирует закрытые ключи только в зашифрованном виде. Поэтому закрытый ключ всегда защищён паролем. Все действия, для которых требуется закрытый ключ (например, расшифровка или подпись сообщения), требуют наличия обоих компонентов: закрытого ключа **и** пароля. Даже после экспорта закрытого ключа он всегда зашифрован и защищён паролем.

Mailvelope по умолчанию гарантирует вашим закрытым ключам высокий уровень безопасности. Вы можете поднять его ещё выше, если в качестве шифровального средства выберете GnuPG («Общие настройки» -> «Настройки OpenPGP»).

Примечания

- Стандарт OpenPGP допускает использование закрытых ключей без пароля. На практике это случается редко. Мы не рекомендуем использовать ключи без паролей в Mailvelope.
- Если злоумышленник получит доступ к закрытому ключу и применит метод перебора, стойкость защиты полностью зависит от сложности и длины пароля. Пожалуйста, обратите внимание на примечания в следующем разделе этого FAQ_.
- Как и всякая программа со сквозным шифрованием, Mailvelope полагается на безопасность отправителя и получателя. Если один из этих компьютеров имеет уязвимости (например, на нём не установлены обновления операционной системы или браузера), надёжность шифрования оказывается под вопросом. Обычные меры защиты важны, но надо особенно следить, чтобы третьи лица не получили доступ к вашему компьютеру.
- GPG использует аналогичную модель безопасности для закрытых ключей. Шифруется не «связка ключей», а лишь отдельные части ключа. Любой пользователь с правами локального доступа может скопировать закрытый ключ из файловой системы. Но для работы с закрытым ключом нужен пароль.
- По умолчанию браузеры Chrome и Firefox автоматически отправляют статистику использования и отчёты о сбоях своим разработчикам. Если возникнет ошибка, не исключено, что вместе с прочими данными разработчику будет отправлен закрытый ключ. Поэтому мы рекомендуем отключить автоматическую отправку статистики и отчётов в настройках Chrome (в разделе «Конфиденциальность и безопасность»). В Firefox вы также можете найти соответствующую опцию настройках (раздел «Приватность и защита» -> «Сбор и использование данных Firefox»).

Как выбрать надёжный пароль для закрытого ключа?

Для защиты данных нужно использовать надёжные пароли. Представьте, что злоумышленник получил доступ к вашему закрытому ключу и старается подобрать пароль методом перебора. При такой атаке в течение короткого времени перебирается множество вариантов паролей. В конечном счете эффективность вашего шифрования зависит, с одной стороны, от длины пароля, с другой стороны, от случайности (энтропии) комбинации символов.

Надёжный пароль получится, если комбинировать буквы верхнего и нижнего регистров, цифры и специальные символы. Такие пароли бывает сложно запомнить. Другой вариант – придумать сценку или картинку, которую вы можете описать несколькими случайными словами. Эти слова и составят ваш пароль (пример здесь).

Как создать резервную копию моих ключей?

Если хотите сделать резервную копию ключей, обратитесь к инструкции в разделе «Как экспортировать мой ключ PGP из Mailvelope?»

Если хотите защитить закрытый ключ, позаботьтесь о безопасности. Закрытый ключ и после экспорта остаётся зашифрованным и запароленным, но его всё равно не стоит оставлять без присмотра на диске.

Если риск для информации высок, лучше держать файл в безопасном офлайновом хранилище. Например, хранить закрытый ключ на USB-флешке (если у неё есть аппаратная или программная парольная защита, этого может быть достаточно). Найдите для флешки безопасное место.

Что делать, если я забыл пароль?

Увы, Mailvelope не поможет восстановить пароль. Сообщения, которые были присланы вам и зашифрованы вашим открытым ключом, окажутся недоступны. Останется только удалить старый ключ. Это нужно сделать и на сервере ключей Mailvelope, если вы предварительно загружали ключ туда. Создайте новую ключевую пару. Поскорее оповестите своих собеседников о том, что вы сменили открытый ключ.

Когда Mailvelope используется для почты WEB.DE и GMX , можно восстановить пароль с помощью так называемого «кода восстановления». Подробнее см. «(WEB.DE и GMX) Сервис просит «код восстановления». Где его взять? Из Mailvelope?».

Как сменить пароль к закрытому ключу?

Откройте окно со связкой ключей Mailvelope (главное меню -> «Ключи»). Выберите ключевую пару, для которой хотите сменить пароль, и обратите внимание на детали ключа. В левом нижнем углу – поле «Пароль». Нажмите кнопку «Изменить». Укажите старый пароль, потом новый пароль.

Устанавливаю расширение и вижу, что оно хочет доступ к посещённым сайтам, браузерным вкладкам и всем моим действиям в браузере. Это правда необходимо? Зачем?

Эти права нужны для корректной работы Mailvelope по следующим причинам:

- Mailvelope должен иметь возможность искать PGP-шифрованные сообщения на сайтах. Для этого Mailvelope нужен доступ к данным сайтов.
- Mailvelope по умолчанию настроен для ряда популярных почтовых сервисов. Но можно настроить Mailvelope для работы с любыми сайтами. Поскольку Mailvelope не знает априори, какие провайдеры добавляются, ему нужен доступ ко всем сайтам.
- Иначе Mailvelope не сможет добавлять свои элементы управления в интерфейсы сайтов.

Mailvelope – программное обеспечение с открытым исходным кодом. Его проверили на многих сайтах. Мы гарантируем, что Mailvelope не будет злоупотреблять разрешениями.

Определенные провайдеры веб-почты

(WEB.DE и GMX) Сервис просит «код восстановления». Где его взять? Из Mailvelope?

Если пользователь забудет пароль к своему ключу или потеряет сам ключ, сервисы GMX и WEB.DE (и только они) попросят код восстановления. Этот 26-значный код генерируется при настройке шифрования email. Его лучше распечатать, чтобы потом можно было использовать для восстановления доступа к ключу.

Если у вас все ещё есть личный ключ PGP и пароль, вы можете распечатать новый код восстановления.

В настоящий момент у WEB.DE нет сайта техподдержки на английском языке, поэтому можете использовать ссылку ниже для обоих сервисов. Последовательность действий одинаковая.

Помощь GMX: создание нового документа восстановления

Если вы потеряли/забыли свой закрытый ключ или пароль к нему и не распечатали код восстановления, зашифрованное сообщение прочесть не получится. PGP-функцию вашего аккаунта GMX или WEB.DE придется перезапустить. Вы не сможете это сделать ни вручную, ни через Mailvelope. Нужно обратиться на горячую линию поддержки GMX или WEB.DE:

- Поддержка GMX
- Поддержка WEB.DE

Чтобы выполнить интеграцию с Mailvelope, Google требует дополнительные права доступа для Gmail API. Как Mailvelope обрабатывает мои данные?

Mailvelope может работать в связке с Gmail даже без использования API. Однако с API получается гораздо проще

отправлять сообщения и вложения.

Если вы включите в настройках опцию «Gmail API», то в почтовом интерфейсе Gmail появятся новые элементы. При первой попытке использования этих функций Google предложит пошаговую авторизацию.

Таким образом браузерное расширение Mailvelope получит доступ к вашей электронной почте в аккаунте Gmail. Ни при каких условиях ваши письма не будут использованы в несогласованных целях или не будут пересылаться посторонним людям. Mailvelope получает не больше прав, чем любая программа электронной почты, установленная на вашем компьютере.

Код Mailvelope открыт и доступен публично. Мы полностью прозрачны в том, что касается обработки ваших данных. Кроме того, безопасность регулярно оценивается аудиторами. Наши руководящие принципы обработки данных изложены в Политике приватности.

Ошибки в программе

Мне кажется, Mailvelope работает неправильно. Что делать?

Mailvelope – браузерное расширение. Для его корректной работы нужно, чтобы и браузер работал корректно. Если вы всё ещё видите ошибки, проверьте, не устарела ли ваша операционная система. Возможно, вам пора обновить браузер до последней версии. Если ошибки останутся, попробуйте следующее.

Firefox:

- Сначала отключите прочие расширения браузера. Перезапустите Firefox. Порой одно расширение мешает работе другого.
- Firefox предлагает функцию очистки. Инструкции доступны в материале «Очистка Firefox – сброс дополнений и настроек».

Google Chrome:

- Сначала отключите прочие расширения браузера. Перезапустите Chrome. Порой одно расширение мешает работе другого.
- Если вы обнаружите, что другие расширения мешают Mailvelope (это изредка случается в Chrome), можете создать специальный пользовательский профиль, в котором Mailvelope будет единственным расширением.

Что включать в отчёт об ошибке?

Перед отправкой сообщения об ошибке, пожалуйста, перезапустите браузер. Убедитесь, что проблема исчезла. Часто проблемы возникают с самим браузером, а не с Mailvelope. Если вы используете устаревшую версию браузера или операционной системы, пожалуйста, обновите программы и проверьте, исчезла ли проблема. Если нет, пожалуйста, отправьте нам отчёт об ошибке: support@mailvelope.com.

В отчёте следует указать, как минимум:

- Краткое описание проблемы
- Тип и версию операционной системы

Если у вас Google Chrome:

- Версию браузера (введите about:version в адресной строке)
- Если Mailvelope не показывает сообщение об ошибке, можете найти соответствующую информацию в журнале
- Во вкладке браузера, где открыт сайт вашего почтового провайдера, выберите Ctrl + Shift + J (Windows/Linux) или ⌘ + alt/Option + J (Mac). Добавьте выделенные красным ошибки в свой отчёт.
- Далее, откройте страницу расширения (*chrome:extensions* в адресной строке)
- Активируйте режим разработчика в правом верхнем углу страницы
- Нажмите ссылку «фоновая страница» в разделе «Mailvelope»
- Откроется новое окно браузера. Убедитесь, что вкладка «Консоль» включена, и добавьте в отчёт об ошибке все ошибки, отмеченные красным цветом

Если у вас Firefox:

- Как узнать версию браузера, рассказано здесь
- Если Mailvelope не показывает сообщение об ошибке, можете найти соответствующую информацию в журнале
  - Перезапустите браузер

- Попробуйте воспроизвести проблему
- В главном меню Firefox выберите «Дополнения». В правом верхнем углу нажмите на значок шестерёнки («Инструменты для всех дополнений»). В выпадающем меню выберите пункт «Отладка дополнений». Появится список расширений. Нажмите кнопку «Исследовать», которая находится в разделе Mailvelope. Выберите вкладку «Консоль». Вставьте содержимое окна консоли в свой отчёт об ошибке.

Я получил зашифрованное письмо, но вижу только два вложения. Mailvelope не предлагает автоматическую расшифровку.

Когда такое может произойти? Например, PGP-программа вашего собеседника зашифровала письмо в формате PGP/MIME, а ваш почтовый провайдер по умолчанию не включил функцию предпросмотра вложений. Тогда Mailvelope не сможет добраться до расшифрованных данных по техническим причинам. Соответственно, Mailvelope не сможет предложить автоматическую расшифровку.

Решение

- Если такая ситуация возникает часто, вашему собеседнику лучше научиться впредь переключаться с PGP/MIME на PGP/INLINE. Это самое простое решение.
- Вы можете расшифровать оба вложения вручную с помощью Mailvelope. Сначала сохраните файлы на компьютер. Нажмите правой кнопкой мыши на файле, выберите «Открыть с помощью», выберите простой текстовый редактор на вашем компьютере (например, «Textedit» в Mac OS или «Блокнот» в Windows). Выберите код PGP в текстовом редакторе. Не забудьте включить в своё выделение заголовки `-----BEGIN PGP PUBLIC KEY BLOCK-----` и `-----END PGP PUBLIC KEY BLOCK-----`. Скопируйте в буфер памяти. Выберите «Шифрование файлов» в главном меню Mailvelope, затем «Расшифровать» в верхнем горизонтальном меню. Нажмите кнопку «Хотите также расшифровать текст?» Вставьте содержимое буфера в открывшееся окно и подтвердите кнопкой «Расшифровать». Как только вы увидите расшифрованное письмо, можете скопировать его из окна и использовать в другом месте.

Mailvelope говорит, что для сообщения не найден закрытый ключ (а нужен другой ключ с определённым ID).

Эта ошибка возникает, если вы получили зашифрованное сообщение, но Mailvelope не может найти в вашей связке ключей соответствующий закрытый ключ. Такое бывает, когда ваш собеседник по ошибке использует для шифрования не ваш открытый ключ, а чей-то чужой. Тогда у Mailvelope не получится расшифровать письмо. Если вы не знакомы с PGP, советуем почитать о принципах работы Mailvelope в нашей документации. Это поможет вам лучше понять, как работает ассимметричное шифрование.

Закрытый ключ может отсутствовать по разным причинам. Например, вы обменялись открытыми ключами с собеседником, а потом забыли пароль к своему закрытому ключу. Чтобы это исправить, вы создали новую ключевую пару, а старую удалили. Теперь нужно отправить собеседнику ваш новый открытый ключ. Важно, чтобы собеседник не продолжал пользоваться вашим старым открытым ключом – иначе вы не сможете расшифровать полученные письма и увидите вот такие сообщения об ошибке.

Другой пример: ваш собеседник использовал устаревший открытый ключ с сервера ключей Mailvelope (или другого сервера ключей). Старый ключ, который вы забыли удалить с сервера после создания нового. Обратите внимание: пока этот старый ключ доступен людям, каждый может отправить вам зашифрованное письмо и при этом не увидит никакого сообщения об ошибке. Вы не сможете открыть это письмо, поскольку в Mailvelope нет соответствующего ключа для расшифровки.

Mailvelope не видит установленную программу PGP

Может случиться, что вы установили GnuPG, но Mailvelope не видит эту программу. Или вы не можете выбрать GnuPG в качестве шифровального средства в настройках Mailvelope. Использование GnuPG оптимизировано не для всех операционных систем. Более подробную информацию можно найти в нашем wiki на GitHub: Mailvelope GnuPG Integration.

Установка

Как установить Mailvelope?

Установка Mailvelope в Chrome и Firefox выполняется почти одинаково. Инструкции есть в нашей документации.

Можно ли установить Mailvelope в другие браузеры, кроме Chrome и Firefox?

Да. Есть много браузеров, построенных на основе «движков» Chromium и Mozilla. Mailvelope прекрасно работает в этих браузерах. Однако рынок постоянно меняется, и у нас нет возможности проверять работу Mailvelope во всех существующих браузерах. Можем, впрочем, порекомендовать браузер Brave, основанный на Chromium. У этого браузера много функций, ориентированных на приватность.

Для Opera существует расширение, которое позволяет устанавливать в этом браузере расширения Chrome. Мы не проверяли, насколько корректно работает Mailvelope в Opera.

Как удалить Mailvelope?

- Удаление Mailvelope из Chrome.
- Удаление Mailvelope из Firefox.

Благодарим волонтёров localizationlab.org за участие в переводе этого материала!

Команда Mailvelope