

Самозащита электронной почты от слежки

Массовая слежка нарушает наши фундаментальные права и угрожает свободе слова!

Тем не менее мы способны защитить себя.



Проблема

Пароля, защищающего Вашу электронную почту, недостаточно для защиты Ваших писем от технологий массовой слежки, применяемых секретными службами.

Каждое письмо, отправленное через Интернет, проходит через множество компьютерных систем на пути к адресату. Секретные службы и следящие агентства используют это, чтобы читать миллионы и миллионы электронных писем каждый день.

Даже если Вы думаете, что Вам нечего скрывать: любой, с кем Вы общаетесь с помощью незащищенной почты, также беззащитен.

Шифрование

Верните себе приватность общения с помощью GnuPG! GnuPG шифрует Ваши письма перед отправкой так, что только выбранные Вами получатели смогут прочесть их.

GnuPG платформонезависим. Это значит, что он работает с любыми адресами электронной почты и запускается на подавляющем большинстве компьютеров и современных смартфонов. GnuPG является свободным ПО и распространяется бесплатно.

Тысячи людей уже используют GnuPG как для профессиональных, так и для частных целей. Присоединяйтесь к нам! Каждый присоединившийся делает наше сообщество сильнее и доказывает, что мы готовы дать отпор.

Решение

Даже если письмо, зашифрованное с помощью GnuPG, перехвачено или попало не в те руки, оно окажется бесполезным:

без соответствующего закрытого ключа оно никем не может быть прочитано. Лишь для назначенного получателя, и только для него, письмо будет выглядеть абсолютно обычным.

Отправитель и получатель теперь лучше защищены. Даже в случае, если Ваши письма не содержат никакой частной/личной/секретной информации, последовательное использование шифрования защищает нас от незаслуженной массовой слежки.

Приватное общение через email



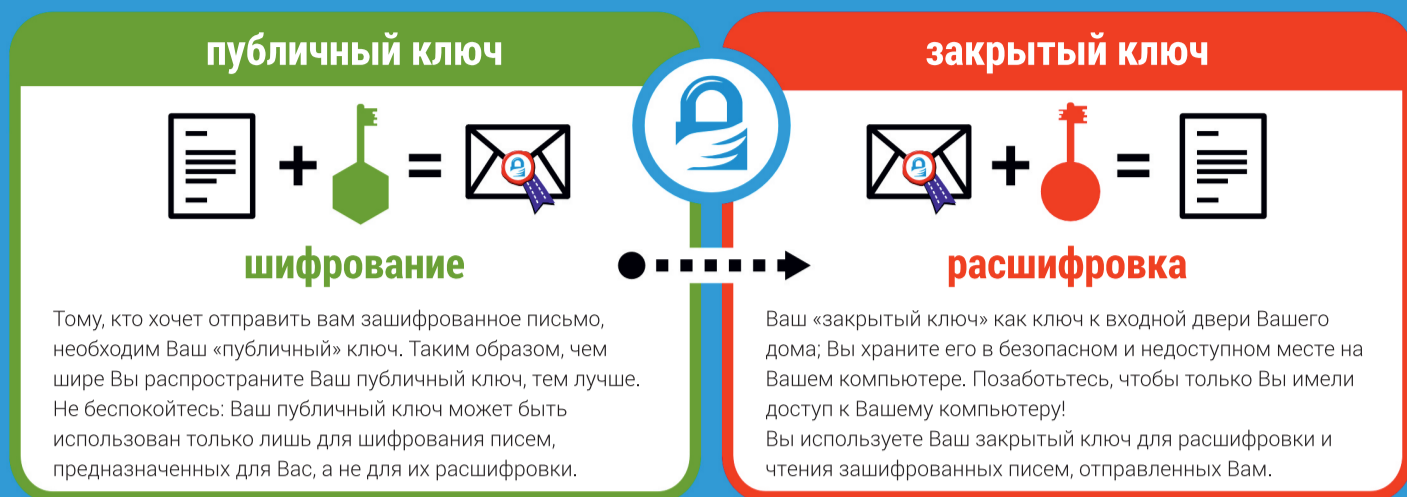
**Верните свою приватность!
Используйте GnuPG!**



- Свободное Программное Обеспечение
- для любых адресов email
- доступен для GNU/Linux, Windows, Mac, Android, ...
- не требует учетной записи или регистрации
- распространяется бесплатно

Как работает GnuPG

Чтобы использовать шифрование GnuPG Вы создаете уникальную пару, состоящую из публичного и закрытого «ключей». Эти ключи используются следующим образом



Что делает GnuPG безопасным?

GnuPG является **Свободным ПО** и использует **Открытые Стандарты**. Это важно для уверенности в том, что ПО действительно способно защитить нас от слежки, поскольку в проприетарном ПО и форматах различные действия могут происходить вне Вашего контроля.

Если никто не допущен к просмотру исходного кода программы, то никто не может быть уверен, что программа не содержит нежелательное шпионское ПО — так называемые «бэкдоры». Если ПО не показывает, как оно работает, мы не можем слепо доверять ему.

В противоположность этому, фундаментальным условием Свободного ПО является публикация исходного кода: Свободное ПО разрешает и поддерживает независимую проверку и публичный обзор кода программы каждым. Предоставляя эту прозрачность, бэкдоры могут быть обнаружены и удалены.

Большинство Свободного ПО находится в руках сообщества, которое работает вместе над созданием безопасного ПО для каждого. Если Вы хотите защитить себя от слежки, Вы можете доверять только Свободному ПО.

Что такое Свободное ПО

Свободное ПО может быть использовано кем угодно для любых целей. Эта возможность включает в себя свободное распространение, просмотр исходного кода и возможность улучшать или адаптировать ПО под Ваши нужды (так называемые «четыре свободы»).

Если Вы хотите только лишь использовать программу, то Вы все равно в выигрыше от этих свобод, поскольку они гарантируют, что Свободное ПО останется в руках нашего сообщества и что его дальнейшая разработка не будет управляться интересами частных компаний или государств.

Узнайте больше об этом и о том, как Свободное ПО способно привести нас к Свободному Обществу:

fsfe.org/freesoftware

Практический совет

Технология, на которой основан GnuPG, предоставляет первоклассную защиту. Следующие указания помогут Вам убедиться в том, что Ваша зашифрованная переписка не скомпрометирована по иным причинам:

Чтобы расшифровать электронные письма, Вам необходим Ваш закрытый ключ и Ваш **пароль**. Этот пароль должен состоять, как минимум, из 8 символов, содержать цифры, специальные символы, буквы как нижнего, так и верхнего регистра. Кроме того, никто, обладающий различными сведениями о Вас, не должен угадать Ваш пароль.

Создавайте резервные копии Вашего ключа! Если Ваш жесткий диск ломается, вам не придется создавать новый ключ и Вы не потеряете свои данные.

Шифруйте как можно больше! Благодаря этому, Вы препятствуете пониманию другими того, когда и с кем Вы общаетесь конфиденциальной информацией. Таким образом, чем чаще Вы шифруете сообщения, тем менее подозрительными они становятся.

Имейте в виду, что **тема письма передается незашифрованной!**

Руководство

Вы можете найти простое руководство по самозащите электронной почты с помощью шифрования GnuPG здесь:

EmailSelfDefense.FSF.org

Или найти так называемые **Криптопати** в Вашем регионе. На этих мероприятиях Вы можете встретить людей, которые будут рады помочь Вам с установкой и использованием GnuPG или других средств шифрования безвозмездно.

2016-04-04



Эта листовка - компиляция, выполненная ЕФСПО, основанная на оригинальной графике ФСПО и Journalism++, доступной по адресу: emailselfdefense.fsf.org

О ФСПО

Эта листовка была создана Европейским Фондом Свободного Программного Обеспечения (ЕФСПО), некоммерческой организацией, направленной на продвижение Свободного ПО и работающей над построением свободного цифрового общества.

Доступ к ПО определяет то, как мы можем принимать участие в нашем обществе. Поэтому ЕФСПО борется за справедливый доступ к нему и за участие каждого в стремлении к цифровой свободе в информационный век.

Никто никогда не должен быть принужден к использованию ПО, которое не предоставляет свободы **использования, изучения, распространения и улучшения ПО**. Мы должны иметь право видоизменять технологии под наши нужды.

Работа ЕФСПО поддерживается сообществом людей, преданных этой идее. Если Вы желаете присоединиться к нам и/или помочь нам в достижении наших целей, то существует множество способов сделать это. Неважно, какова Ваша подготовка и образование. Вы можете узнать больше об этом, а также помочь нашей работе по ссылке ниже:

fsfe.org/contribute

Становитесь членом Содружества!

Пожертвования критичны для продолжения нами работы и гарантии нашей независимости. Вы можете поддержать нашу деятельность самым лучшим образом, став членом поддержки ЕФСПО — «членом Содружества». Этим Вы напрямую поддерживаете нас в нашей всесторонней борьбе за Свободное ПО.

fsfe.org/join

Вы можете заказать эту листовку бесплатно:

fsfe.org/promo

Free Software Foundation Europe e.V.
Schönhauser Allee 6/7
10119 Berlin
Germany
<https://fsfe.org>

