

Инструкция по шифрованию писем¹

№09-И

1. Принцип работы

Программа PGP работает на основе асимметричной криптографии, то есть каждый пользователь создаёт и в дальнейшем использует два ключа - публичный, с помощью которого можно зашифровать сообщение, и приватный, для расшифровки сообщений. Для расшифровки требуется приватный ключ, парный публичному, использовавшемуся для шифрования. Для работы с приватным ключом необходимо знать пароль (так называемую ключевую фразу), задаваемый при создании ключа. Таким образом, любой человек, имеющий ваш публичный ключ, может зашифровать им данные, а расшифровать их сможете только вы сами с помощью вашего приватного ключа. Ваш приватный ключ не должен быть доступен никому, кроме вас, как и ключевая фраза!

2. Установка ПО

Бесплатную версию PGP можно скачать с <http://www.pgp.com/downloads/desktoptrial2.php> и установить в соответствии с инструкцией. Не забудьте установить плагин для своего почтового клиента.

3. Создание ключей

Если у вас уже есть ключи PGP, вам следует прислать нам свой публичный ключ. Если нет, надо сначала создать пару ключей, для этого необходимо воспользоваться программой PGPKeys (при этом не рекомендуется оставлять ключевую фразу пустой).

4. Где взять наш ключ и как послать свой

Для работы с ключами служит программа PGPKeys. В ней вы можете сразу импортировать наш ключ с сервера ключей, либо получить его от нас по электронной почте и импортировать из сообщения. Ключи Assist находятся по адресу <https://www.assist.ru/contacts/support@assist.ru.key.pub>. Чтобы передать свой публичный ключ нам, вам следует экспортировать его и переслать по электронной почте.

¹ Это краткая инструкция, подробную документацию см. на <http://www.pgp.com>



5. Отправка и получение писем

Программа PGP интегрируется в большинство популярных почтовых программ. Подробно настроить нужную функциональность вы можете через вкладку Email в настройках PGP. Шифрование/расшифровку писем можно осуществлять как автоматически, так и вручную. В последнем случае в почтовой программе появляются специальные кнопки для этого.

6. Примечание

Более подробную информацию о шифровании писем можно получить по адресу support@assist.ru.