**Лабораторная работа № 4.**

Изучение программных средств

защиты информации

1.Постановка задачи:

Цель работы – освоение программных средств защиты информации PGP, предназначенных для:

- шифрования конфиденциальных информационных ресурсов;

- обеспечения целостности информационных ресурсов с помощью механизма;

- электронной цифровой подписи;

- надежного уничтожения остаточной конфиденциальной информации;

- скрытия присутствия в компьютерной системе конфиденциальной информации с помощью виртуального диска.

Результат выполненной работы:

Вопросы:

1) Как обеспечивается случайность выбираемых криптографических ключей

в системе PGP;

Компонент PGP, ответственный за выдачу случайных чисел,

называется генератором (истинно) случайных чисел (ГСЧ), в противовес так

называемым ГПСЧ, алгоритмам, генерирующим детерминированный поток,

похожий на случайные данные. ГСЧ использует гибридный подход: он

обращается к внешним источникам для обеспечения непредсказуемости и

использует функцию хэширования, чтобы сгладить отклонения.

2) Как и где хранится секретный ключ пользователя в системе PGP;

Секретные ключи хранятся в виде "сертификатов ключей", которые включают в

себя идентификатор пользователя владельца ключа (обычно это имя

пользователя), временную метку, которая указывает время генерации пары

ключей, и собственно ключи. Сертификаты секретных ключей — секретные.

Каждый секретный ключ также шифруется с отдельным паролем. Файл ключей,

или каталог ключей ("кольцо с ключами" — "keyring") содержит один или

несколько таких сертификатов. В каталогах секретных ключей

хранятся сертификаты секретных ключей.

3) Как может быть обеспечена в системе PGP возможность восстановления

секретного ключа пользователя при его случайной потере.

Сохранением его резервной копии.

4) Какие дополнительные параметры шифрования могут быть использованы

и в чем их смысл и возможное применение;

• Файл ключа, введите расположение файла PGP ключа, который будет

использоваться для шифрования файлов. Если оставить это поле пустым,

действия файла шифрования PGP используется файл, укажите в папки

Keyring поля. Файлы могут иметь любое расширение имени файла, но \*.asc

является стандартным.

• Папка Keyring, введите расположение папки, содержащей keyring, который

будет использоваться для шифрования файлов. Файл открытого keyring

(\*.pkr) могут быть переименованы с расширением \*.gpg.

• Пользователь, введите имя пользователя, который был указан при создании

ключа шифрования. Это поле является обязательным.

• COMMENT, введите комментарий, который был указан при создании ключа

шифрования. Если это поле был завершен, когда был создан ключ

**Основные функции PGP Desktop Professional:**

1. Шифрование сменных носителей на основе политик. Пользователи PGP Desktop Professional под управлением сервера PGP Universal Server могут автоматически применять шифрование к сменным носителям в соответствии с выбранной политикой.
2. Единый вход в ОС Windows. Система единого входа в ОС MS Windows обеспечивает синхронизацию пароля, обеспечивая надежное применение политики безопасности путем управления политик пароля доменов в Windows без замены существующих правил входа в MS Windows.
3. Несколько способов совместного доступа к данным. Пользователи могут создавать зашифрованные контейнеры для переноса и совместного использования отдельных файлов с помощью приложений PGP® Virtual Disk, PGP® Zip и PGP® Self-Decrypting Archive.
4. Безопасное удаление файлов. Приложения PGP Shredder и PGP Wipe позволяют безвозвратно удалять файлы.
5. Функции управления. Централизованное применение политик безопасности. Политика безопасности электронной почты обеспечивает применение шифрования и цифровых подписей. Данная политика устанавливает принудительное шифрование дисков и сменных носителей, предотвращая расшифровывание данных на дисках и удаление [программного обеспечения](https://pandia.ru/text/category/programmnoe_obespechenie/). Управление текущими каталогами LDAP или [Microsoft](https://pandia.ru/text/category/microsoft/" \o "Microsoft) ActiveDirectory для автоматического назначения политик на основе атрибутов групп пользователей.
6. Протоколирование событий. Ведение информативных протоколов для записи всех операций администрирования и шифрования дисков для проверки и установки передовых методов защиты в организации.
7. Фраза-пароль для восстановления. Автоматическое генерирование и централизованное хранение уникальной фразы-пароля для восстановления позволяет выполнять удаленную поддержку.

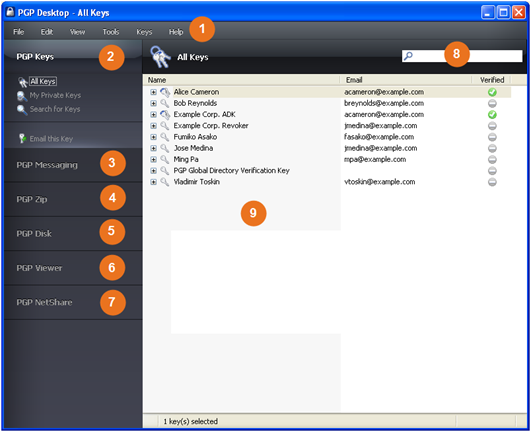
Предоставляет следующие возможности пользователю:

* создание пользователем пары ключей “закрытый - открытый”;
* шифрование файла с возможностью выбора ключа;
* подпись файла ЭЦП;
* шифрование + подпись;
* дешифрование / подтверждение подлинности;
* «необратимое» (безопасное) удаление данных с диска.

PGP Desktop Professional включает в себя пять тесно интегрированных приложений для шифрования электронной почты, управления цифровыми подписями, создания виртуальных дисковых томов с криптозащитой, шифрования данных на уровне жесткого диска и шифрования мгновенных сообщений. Высокая степень автоматизации и согласованность управления всеми пятью модулями достигается за счет использования политик защиты информации, определяемых конечным пользователем.

Запуск программы PGP осуществляется из меню Start/Progpams/Pretty Good Privacy/PGPDesktop. Для того чтобы начать работать с PGP следует создать пару ключей «открытый-закрытый» и распространить открытый ключ по всем абонентам, с которыми вы хотите обмениваться защищенной информацией.

Рассмотрим главный экран PGP Desktop



Главный экран PGP включает:

1. Строка меню. Предоставляет Вам доступ к настольным командам PGP. Меню изменяется в зависимости от того, какой пульт управления выбран.
2. Пульт управления ключами PGP. Дает Вам контроль над ключами PGP.
3. Передающий пульт управления PGP. Дает Вам контроль над передачей сообщений PGP.
4. Пульт управления почтового индекса PGP. Дает Вам контроль над почтовым индексом PGP.
5. Дисковый пульт управления PGP. Дает Вам контроль над диском PGP.
6. Пульт управления зрителя PGP. Дает Вам способность расшифровать, проверить и показать сообщения вне почтового потока.
7. Пульт управления NetShare PGP. Дает Вам контроль NetShare PGP.
8. Настольное рабочее пространство PGP.
9. Рабочая область ключей PGP.

**Создание пары ключей «открытый-закрытый»**

Для создания новой пары ключей необходимо выполнить следующие действия:

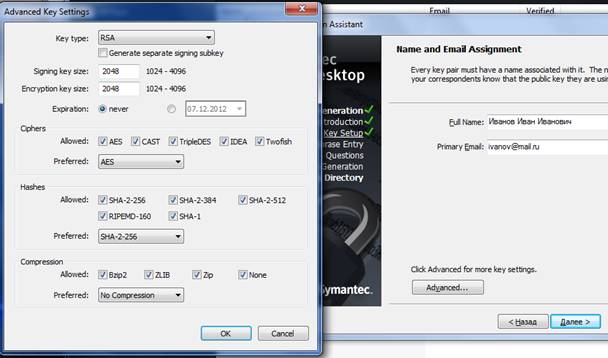
1. В окне PGPkeys выбрать пункт меню File|New PGP Key… для запуска Мастера создания ключей (Key Generation Wizard)
2. Прочитав содержимое окна, нажмите далее для перехода к следующему окну диалога. Помощник генерации ключей попросит вас ввести ваше имя и адрес электронной почты
3. Введите ваше имя в первой строке и ваш адрес электронной почты во второй.

Для того чтобы выбрать тип ключа Diffie-Hellman или RSA, длину ключа и другие свойства необходимо нажать Advanced.

Укажите срок прекращения использования ключей. Вы можете сохранить выбор по умолчанию "никогда" (never), или указать конкретное количество дней, по истечении которых ключи станут недействительными.







4.  Нажмите далее и в следующем окне (Create Passphrase), необходимо задать фразу-пароль, которая должна состоять не менее, чем из 8 символов.



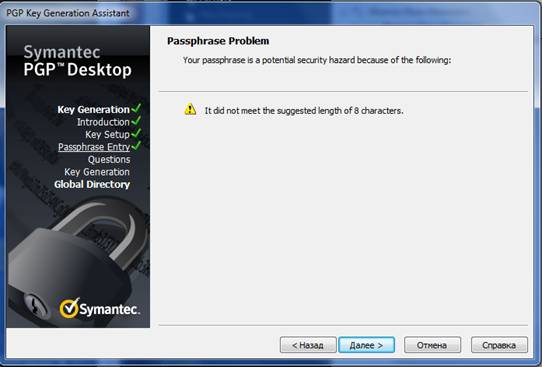
В поле ввода Пароль (Enter Passphrase) введите последовательность символов или слов, которую вы будете использовать для исключительного доступа к своему закрытому ключу. Для подтверждения вашего выбора, переместите курсор нажатием клавиши Tab на следующую строку и введите выбранный пароль еще раз.

Обычно, для обеспечения вашей безопасности, на экране не отображаются вводимые вами символы. Если вы, однако, уверены в том, что за вами никто не подглядывает, и хотите видеть вводимые вами символы пароля, снимите флажок в поле "Show Keystrokes".

Пароль должен содержать несколько слов, и может включать пробелы, цифры и другие печатные символы. Придумайте что-нибудь, что вам легко запомнить, а другим - непросто отгадать, и помните, что в пароле строчные и заглавные буквы различаются. Чем длиннее ваш пароль, и чем шире набор символов, которые он содержит, тем он более надежен. Попытайтесь включить равное количество строчных и заглавных букв, цифр, знаков препинания и т. п.

5.  После задания пароля и нажатия кнопки. Далее на экране появится окно генерации ключей с индикатором хода процесса. Помощник генерации ключей покажет, что он занят генерацией новой пары ключей.

Если вы ввели неадекватный пароль, до запуска генерации ключей появится предупреждающее сообщение, и для продолжения вы должны либо подтвердить использование неудачного пароля, либо ввести новый пароль.



6.  По окончании процесса генерации необходимо нажать кнопку. Далее и в следующем окне кнопку Готово для окончания процедуры создания ключей.



**Обмен ключами**

Распределение открытого ключа

Вы можете передать свой открытый ключ различными способами:

* Издать свой ключ в Глобальном Справочнике PGP.
* Включить свой открытый ключ в электронное письмо.
* Экспортировать свой открытый ключ или скопировать его в текстовый файл.
* Копия со смарт-карты.

Передача открытого ключа на keyserver:

1. Откройте PGP Desktop.
2. Удостоверьтесь, что Пульт управления Ключей PGP активен.
3. Щелкните правой кнопкой мыши на keypair, открытый ключ которого Вы хотите послать на keyserver.
4. Выберите Send и затем выберите keyserver, на который Вы хотите послать открытый ключ из списка.

Как только Вы помещаете копию своего открытого ключа на keyserver, это доступно людям, которые хотят послать Вам зашифрованные данные или проверить Вашу цифровую подпись. Даже если Вы явно не указываете людям на Ваш открытый ключ, они могут получить копию, ища на keyserver Ваше имя или адрес электронной почты.

Другим удобным методом поставки Вашего открытого ключа является включение его в электронное письмо.

Когда Вы посылаете кому-то свой открытый ключ, убедитесь, что подписали его электронной подписью. Таким образом, получатель может проверить Вашу подпись и убедиться, что никто не вмешался в информацию по пути.

Включение открытого ключа в электронное письмо:

1. Активизируйте Пульт управления ключей.
2. Щелкните правой кнопкой мыши на keypair, открытый ключ которого Вы хотите включить в электронное письмо.
3. Выбранный ключ отправить получателю. Ваша почтовая программа откроется в рабочей области.
4. Обратитесь к сообщению и пошлите его.

Если этот метод не работает, Вы можете открыть PGP Desktop, выбрать Ваш keypair правой кнопкой мыши и нажать Copy, открыть электронное письмо и вставить его в тело сообщения.

**Экспорт открытого ключа.**

Имеется три способа экспортировать Ваш открытый ключ:

1. Выберите свой keypair, затем File|Export. Введите имя и местоположение для файла, затем щелкните Save.
2. Нажмите сочетание клавиш Ctrl+click по ключу, который Вы хотите сохранить, выберите Экспорт из списка, введите имя и местоположение для файла, затем щелкните Save.
3. Выберите свой keypair, затем щелкните правой кнопкой мыши и выберите Copy. Откройте редактора текста, вставьте ключевую информацию в текстовый файл и сохраните.

**Получение открытых ключей**

Для того, чтобы послать зашифрованную почту или проверить цифровые подписи, Вы должны получить открытые ключи ваших партнеров.   
Способы получения открытого ключа:

1. Автоматическое восстановление проверенного ключа из Глобального Справочника PGP. Поиск ключа вручную на keyserver.
2. Добавление открытого ключа непосредственно из электронного письма.
3. Импорт открытого ключа из экспортируемого файла.
4. Получение ключа от универсального сервера своей организации PGP.
5. Получение открытого ключа от Keyserver.

Если человек, которому Вы хотите послать зашифрованную почту, является опытным пользователем PGP, вероятно, что копия его открытого ключа находится в глобальном справочнике PGP или в другой общественности keyserver. Это очень удобно, чтобы получить копию самого современного ключа всякий раз, когда Вы хотите послать почту, и также освобождает Вас от необходимости сохранять множество ключей.

Для получения открытого ключа необходимо:

* активизировать пульт управления ключами PGP;
* выбрать поиск ключей, после этого определить свои критерии поиска, а затем выполнить поиск;
* добавить открытый ключ.

**Получение открытого ключа из электронного письма.**

Удобным способом получения копии открытого ключа является приложение данного ключа к электронному письму.

1. открыть электронное письмо;
2. щелкнуть два раза на файл с расширением \*.asc, который содержит открытый ключ;
3. выбрать необходимый открытый ключ;
4. чтобы открыть файл, выберите открытый ключ, который Вы хотите добавить, и щелкните Import.

**Окно свойств ключа**

Окно свойств ключа появляется при выборе ключа в окне PGPkeys и пункта меню Keys|Key Properties. Окно Key Properties содержит:

* значения атрибутов ключа (идентификатор, тип, размер, дата создания, срок действия, используемый шифр);
* цифровой отпечаток ключа (fingerprint), который представляет собой уникальную строку цифр и символов, генерируемую при создании ключа и предназначенную для его аутентификации; уровень доверия к лицу, удостоверяющему ключ (Trust);
* кнопку Change Passphrase… для изменения фразы пароля.



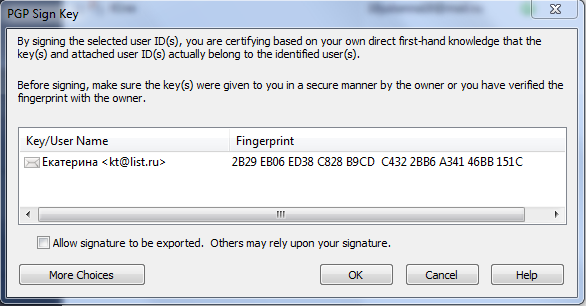
**Подтверждение подлинности открытого ключа другого пользователя**

Когда вы обмениваетесь ключами с кем-то, трудно утверждать, что ключ действительно принадлежит этому человеку. Наилучший путь, который дает полную уверенность, что открытый ключ действительно принадлежит конкретному лицу — это получить копию ключа на флэш-диске лично от владельца данного ключа. Тем не менее, наиболее распространенным способом является получение ключа через e-mail или от общественного сервера ключей.

Если вы уверены, что данный ключ достоверный и действительно принадлежит определенному пользователю, то вы можете подтвердить его подлинность, подписав ключ своим закрытым ключом. Подписывая чей-то общественный ключ своим закрытым ключом, вы удостоверяете, что вы уверены в принадлежности ключа предполагаемому пользователю.

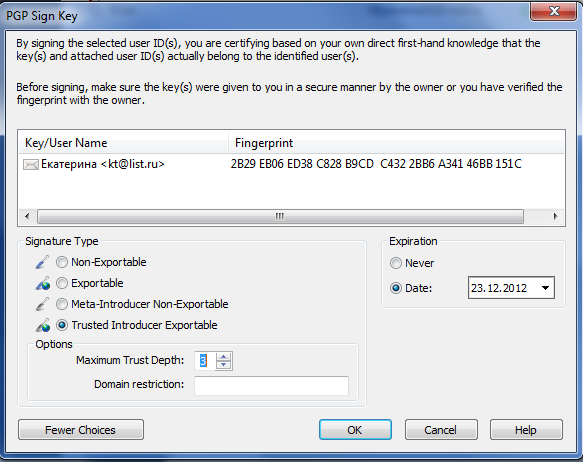
Для того, чтобы подписать ключ, необходимо выполнить следующие действия:

1. В окне PGPkeys выбрать ключ, который нужно подписать.
2. Открыть окно PGP Sign Key (пункт меню Keys|Sign)
3. Для того, чтобы разрешить экспортировать вашу подпись, необходимо включить опцию Allow signature to be exported. Это позволит другим пользователям использовать вашу подпись для определения степени доверия к данному ключу.

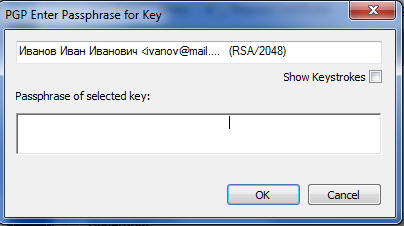


Для более детальной установки свойств подписи, необходимо нажать кнопку More Choices и в появившемся окне определить следующие опции:

* Non-exportable - указывает на невозможность экспорта вашей подписи;
* Exportable - эквивалентна включению опции Allow signature to be exported (см. выше);
* Meta-Introducer Non-Exportable - означает, что вы доверяете не только владельцу данного ключа и его ключам, но и ключам, которые были им подписаны. Данная подпись не может быть экспортирована;
* Maximum Trust Depth - определяет число вложенных уровней доверия, т. е. количество человек, составляющих цепочку: второй пользователь подписывает ключ первого, третий - второго и т. д.
* Trusted Introducer Exportable - данный вид подписи используется, когда вы подтверждаете, что данный ключ достоверен, и что владельцу данного ключа и подписанным им ключам можно полностью доверять. Данный вид подписи является экспортируемым.



1. Для определения ограниченного срока действия ключа необходимо выбрать опцию Date и задать дату окончания срока действия ключа (группа опций Expiration) или включить опцию Never при неограниченном сроке действия ключа.
2. После задания всех опций, нажать кнопку OK и в появившемся окне ввести фразу пароля.



**Средства защиты файлов**

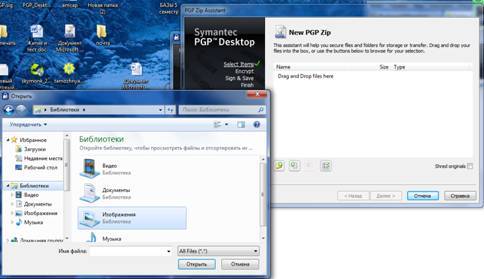
**Шифрование и подпись файлов**

Для зашифровки/подписи файлов необходимо выполнить следующие действия:

1.  Запустить PGP Zip.

2.  Выбрать пункт New PGP Zip

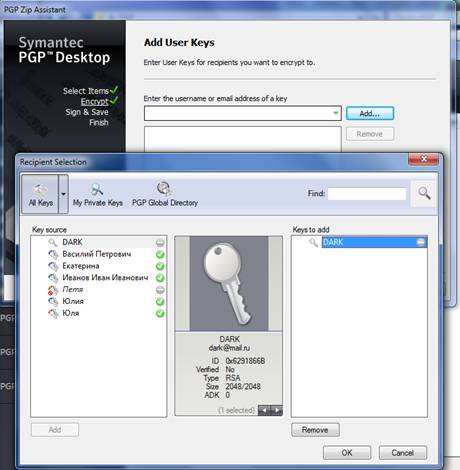
3.  В появившемся окне добавляем файл или папку, которую необходимо зашифровать, нажав кнопу Add files… Нажимаем Далее.



4.  В следующем окне выбрать желаемое действие, выбрав один из пунктов:



5.  Нажимаем Далее. Добавляем открытый ключ получателя, который импортировали ранее



6.  Нажимаем далее и выбираем электронную цифровую подпись, которой будем подписывать шифрованный файл



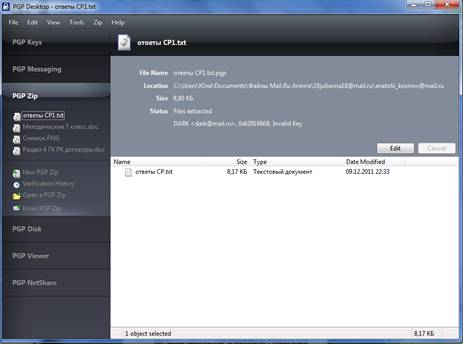
7.  Нажимаем Далее. В появившемся окне видим, что файл зашифрован. Нажимаем Готово.



8.  Теперь можно отправить уже зашифрованный файл получателю, чей открытый ключ использовался.

**Расшифровка файлов и проверка подписи**

Получив зашифрованный файл необходимо открыть его. Если шифрование выполнено правильно, он откроется в PGP Zip



Сохранить файл можно, щелкнув правой кнопкой по файлу и выбрав Extract