


# Средства ЭЦП

**PGP**

**Pretty Good Privacy**




Одной из **ВАЖНЕЙШИХ** задач в автоматизированных системах (АС) является обеспечение надежности передаваемой, хранимой и обрабатываемой информации.

# НАДЕЖНОСТЬ ИНФОРМАЦИИ В АС –

это показатель, характеризующий качество информации с точки зрения:

- **Физической целостности**, т. е. наличия или отсутствия искажений или уничтожения элементов этой информации;
- **Доверия к информации**, т. е. наличия или отсутствия в ней подмены (несанкционированного изменения) её элементов при сохранении целостности;
- **Безопасности информации**, т. е. наличия или отсутствия несанкционированного получения её лицами или процессами, не имеющими на это соответствующих полномочий;



**НИЦ «Прикладная логистика»  
рекомендует использовать следующие  
криптографические системы:**

- **«Крипто Офис» ЛАН Крипто (РФ)**
- **«Верб» МО ПНИЭИ (РФ)**
- **«PGP» Network Associates inc.  
(USA)**
- **«Priva Seal» (USA)**

# ИСТОРИЯ

**PGP** была разработана американским программистом и гражданским активистом **Филом Зиммерманном**, обеспокоенным нарушением личных прав и свобод в информационную эпоху. В 1991 г. в США существовала реальная угроза принятия закона, запрещающего использование стойких криптографических средств, не содержащих "черного хода", используя который, спецслужбы и связанные с ними группировки могли бы беспрепятственно читать зашифрованные сообщения. Тогда Зиммерманн бесплатно распространил PGP в Интернет.

В результате, **PGP** стал **самым** популярным криптографическим пакетом в мире (свыше 2 млн. используемых копий), а Зиммерманн подвергся трехлетнему преследованию властей по подозрению в "незаконном экспорте вооружений".

# PGP - Pretty Good Privacy

**Почти Полная Приватность** - это семейство программных продуктов, которые используют самые стойкие из существующих криптографических алгоритмов (алгоритмов шифрования) и предназначены для защиты приватности файлов и сообщений электронной почты в глобальных вычислительных и коммуникационных средах.

**PGP** реализует технологию, известную как "криптография с открытыми ключами". Она позволяет безопасно обмениваться сообщениями и файлами по каналам открытой связи без наличия защищенного канала для обмена ключами. Эта технология также позволяет накладывать на сообщения и файлы цифровую подпись, с помощью которой можно проверить, были ли они посланы номинальным отправителем и не претерпели ли модификации в пути.

# Электронно- цифровая подпись (ЭЦП)

# Определения - 1

**Электронный документ** - документ, в котором информация представлена в электронно - цифровой форме;

**Электронная цифровая подпись** - реквизит электронного документа, предназначенный для защиты данного электронного документа от подделки. Позволяет идентифицировать владельца сертификата ключа подписи, а также установить отсутствие искажения информации в электронном документе;



## Определения - 2

**Закрытый ключ** – строка символов сгенерированная для конкретного пользователя (уникальная строка). Хранится у пользователя – "как зеница ока".

**Открытый ключ** – строка символов сгенерированная для конкретного человека (уникальная строка) и связанная с Закрытым ключом. Хранится в БД.

**Результат проверки подписи** – утверждение Да/Нет полученное в результате криптопреобразования из Файла с ЭЦП и Открытого ключа

# Общепризнанная схема ЭЦП охватывает три процесса

**1. Генерация ключей (открытый и закрытый)**

**2. Формирования подписи**

**3. Проверка подписи**

Таким образом цифровая подпись является средством **авторизации** и **контроля целостности данных** и позволяет:

- ✓ Осуществить контроль целостности хранимого и передаваемого подписанного сообщения.
- ✓ Подтвердить авторство лица, подписавшего сообщение.
- ✓ Защитить сообщение от возможной подделки.

Кроме того, ЭЦП несёт **принцип неотречения**, который означает, что отправитель не может отказаться от факта своего авторства подписанной им информации.

# Шифрование в PGP

Реализовано по принципу открытого ключа.

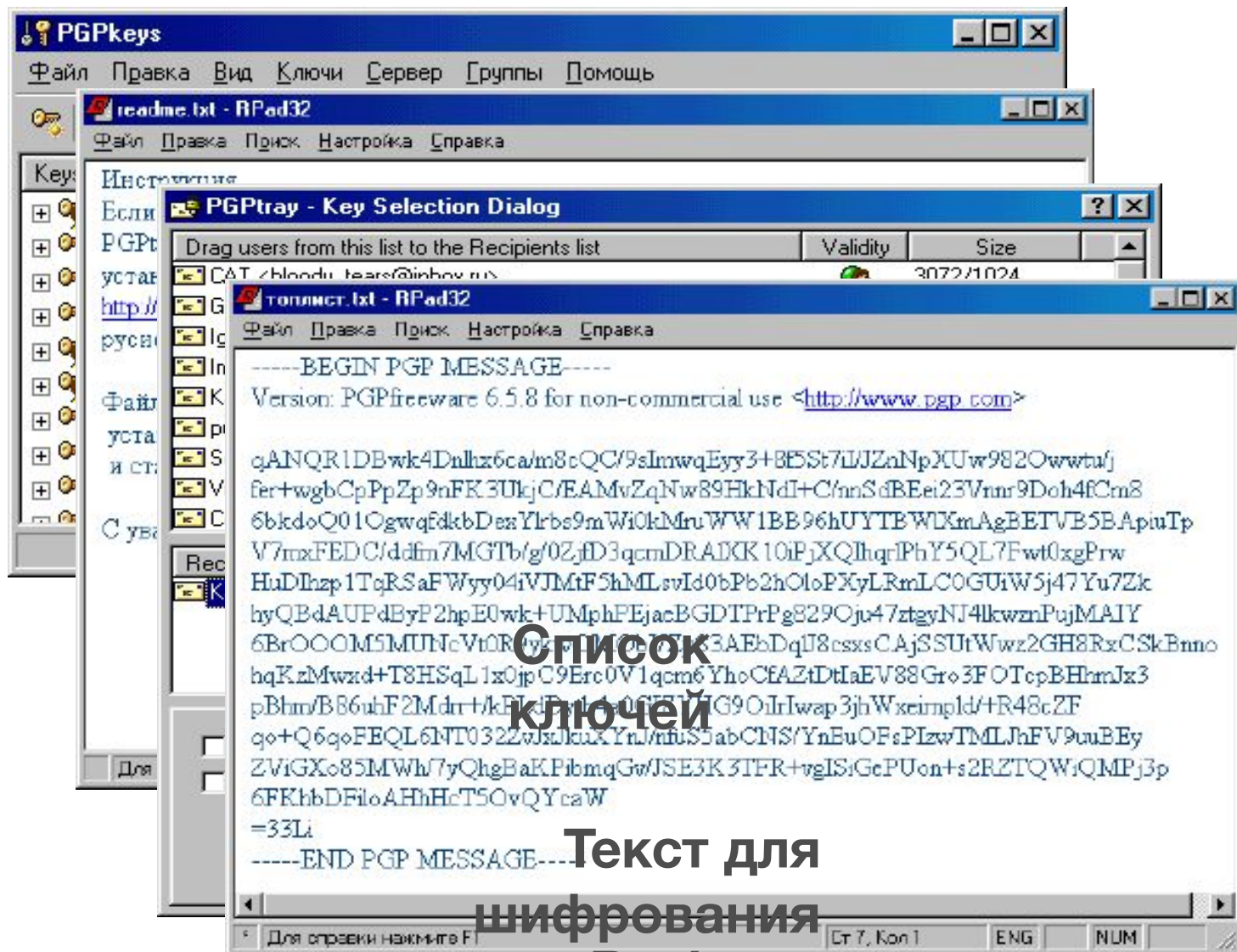
## □ Частный ключ

- расшифровать сообщение, зашифрованные вашим Общественным ключом;
- подписать документ

## □ Общественный ключ.

- зашифровать сообщение тому, чей это ключ;
- проверить подпись владельца ключа

# 4 шага шифрования



Список  
ключей

Текст для  
шифрования

Выбор ключа для  
зашифрованного  
текста

# Окно цифровой подписи

Не измененный документ -

оригинал



Name	Signer	Validity	Signed
 проба.doc	Rouslan <Roosel@mail.ru>		23.12.2004 4:40:41

..После изменения  
документа



Name	Signer	Validity	Signed
 проба.doc	Rouslan <Roosel@mail.ru>		Bad Signature

# Версии PGP:

***PGP Freeware:*** Бесплатная версия PGP для частного некоммерческого (прежде всего, домашнего) использования.

***PGP Workgroupesktop:*** Имеет всё то же, что и PGP Personal, но предназначена в первую очередь для небольших организаций (10-50 человек), поскольку поддерживает корпоративные мэйл-системы MS Exchange Server, Novell GroupWise и Lotus Notes

***PGP Corporate Desktop:*** Комплект поставки для корпоративных пользователей и организаций из 50-5 тыс. пользователей. Включает дистрибутивы PGP Workgroup Desktop, PGP Corporate Disk, PGPadmin, PGP Keyserver.

# Версии PGP:

## *PGP Universal:*

- ✓ Самоуправляемый серверный комплекс информационной безопасности для средних и крупных организаций (от 500 пользователей до 50 тыс.).
- ✓ Автономность функционирования (самостоятельно формируя политику безопасности).
- ✓ Криптографические операции могут производиться на центральном сервере, либо на машинах пользователей.
- ✓ Защищает всю переписку организации и внешних пользователей, независимо от протоколов передачи сообщений.



**PGP** имеет ряд преимуществ перед большинством программ и стандартов (таких, как S/MIME) криптографической защиты информации:

- ✓ Используется по всему миру уже более десяти лет (первая версия была опубликована в 1991 г.).
- ✓ Основана на шифровании открытым ключом, что исключает необходимость передавать адресату секретный пароль (как при обычном шифровании).
- ✓ Лежащий в её основе стандарт OpenPGP был принят организацией IETF в качестве интероперативного стандарта Интернета, и сегодня используется во множестве различных программ, обеспечивая их полную совместимость.
- ✓ Пользователь самостоятельно генерирует свои пары открытых / закрытых ключей и выбирает используемые алгоритмы шифрования.
- ✓ Обеспечивает сквозное шифрование и безопасную связь с пользователями любой операционной системы, email-клиента и почтовой службы.

- ✓ Криптографическое ядро PGP SDK версии 3.0.3, реализованное в PGP 8.1 и выше и в ряде других продуктов, сертифицировано Национальным институтом стандартов и технологий США (NIST) на соответствие нормам безопасности FIPS PUB 140-2.
- ✓ Поддерживает электронные цифровые подписи (ЭЦП), позволяющие заверить авторство и целостность передаваемой информации.
- ✓ Имеет официальные и неофициальные плагины для большинства популярных email-клиентов. Функция работы с активным окном позволяет легко использовать PGP в любых мыслимых приложениях.
- ✓ Система имеет некоторые дополнительные функции в виде шреддера для уничтожения файлов и очистки свободного пространства дисков от остатков удалённой информации, а также PGPdisk для хранения больших объёмов данных на зашифрованных логических дисках.



## Стандарты форматов PGP:

**RFC2440bis:**      Формат      обмена сообщениями PGP (PGP Message Exchange Formats)

**RFC2015:** Стандарт PGP/MIME (MIME Security with Pretty Good Privacy (PGP))

Стандарты описывают форматирование, синтаксис, нотацию и кодировку пакетов **PGP**, а также стандартно используемые алгоритмы. Используя эти открытые спецификации, любой разработчик имеет возможность написать программу, совместимую со всеми иными, основанными на этом стандарте.