Санкт-Петербургский университет МВД России
Кафедра математики и информатики

Специальность: 38.05.01
Экономическая безопасность

Дисциплина: Информатика и информационные технологии в правоохранительной деятельности

Тема 8. Основы защиты информации. Электронная подпись

Лекция 8.1. Основы защиты информации. Электронная подпись

Рассмотрена и одобрена
на заседании ПМС кафедры МиИ
протокол № 11 от 20.05.2021

Доцент кафедры Сибаров К.Д.

Лекция 8.1. Основы защиты информации. Электронная подпись

Вопросы лекции:

1. Основные понятия защиты информации
2. Каналы утечки информации. Меры защиты информации
3. Понятие и виды электронной подписи
4. Основные понятия криптографии с двумя ключами
5. Криптографическая сущность электронной подписи

1. ОСНОВНЫЕ ПОНЯТИЯ ЗАЩИТЫ ИНФОРМАЦИИ

1. Основные понятия защиты информации

Федеральный закон «Об информации, информационных технологиях и о защите информации» № 149-ФЗ от 8 июля 2006 года:

Защита информации — это **меры** по ***предотвращению*** неправомерного доступа, уничтожения, изменения, блокирования, копирования, предоставления, распространения информации, а также деятельность по ***обеспечению*** права на законный доступ к информации

Информационная безопасность – это **состояние** защищённости интересов в информационной сфере

Защита информации как *деятельность* обеспечивает информационную безопасность как *состояние*

Можно говорить об информационной безопасности отдельного человека, сообщества людей, учреждения, общества в целом, государства

1. Основные понятия защиты информации

Что такое интересы в информационной сфере?

Согласно ФЗ, **информационная безопасность** – это обеспечение защищённости, доступности и целостности информации

Защищённость (конфиденциальность) — это предотвращение доступа к информации лиц, которые не имеют на это права

Доступность — обеспечение беспрепятственного доступа к информации для удостоверенных пользователей, имеющих на это право

Целостность — обеспечение достоверности и полноты информации и способов её обработки, предотвращение её изменения без разрешения

1. Основные понятия защиты информации

Кроме защищённости, доступности и целостности информации важны также такие качества, нуждающиеся в обеспечении и защите, как подлинность и подотчётность

Подлинность (аутентичность) – свойство, заключающееся в том, что лицо или источник данных соответствуют заявленным

Подотчётность (идентифицируемость) – возможность ведения учёта действий лица, запросившего доступ к источнику данных

1. Основные понятия защиты информации

Законодательство РФ определяет и защищает следующие **виды тайн**:

- государственная тайна
- тайна следствия и судопроизводства
- налоговая тайна
- служебная тайна
  - коммерческая тайна
  - банковская тайна
- личная и семейная тайна
- тайна переписки, телефонных переговоров, почтовых телеграфных и иных сообщений
  - иная конфиденциальная информация

1. Основные понятия защиты информации

Государственная тайна защищена законом РФ «**О государственной тайне**» № 5485-1 от 21 июля 1993 года

Защиту коммерческой тайны обеспечивает Федеральный закон «**О коммерческой тайне**» № 98-ФЗ от 9 июля 2004 года

Личная информация граждан защищается законом «**О персональных данных**» № 152-ФЗ от 27 июля 2006 года

«**Доктрина информационной безопасности Российской Федерации**» утверждена Указом Президента Российской Федерации № 646 от 5 декабря 2016 года

2. КАНАЛЫ УТЕЧКИ ИНФОРМАЦИИ. МЕРЫ ЗАЩИТЫ ИНФОРМАЦИИ

2. Каналы утечки информации. Меры защиты

Утечка информации – неправомерный тайный перенос сведений ограниченного доступа

Канал утечки информации – путь и способ передачи данных без ведома владельца информации

Каналы утечки информации можно разделить на три основные вида:
– ***люди***, имеющий доступ к информации,
– ***документы***, содержащие информацию,
– ***технические средства*** хранения, обработки и передачи информации

2. Каналы утечки информации. Меры защиты

Люди, имеющие доступ к закрытым сведениям, – главный канал утечки информации

По данным специалистов в области промышленной безопасности, на любом предприятии есть

– честные люди, которые остаются таковыми при любых обстоятельствах (5 – 30%)

– люди, честные или нечестные в зависимости от обстоятельств (50 – 80%)

– люди, ожидающих удобного случая поживиться за счёт предприятия (5 – 30%)

Организационные меры:

– тщательный подбор личного состава

– предельное ограничение круга лиц, допускаемых к закрытым сведениям

– строгие правила работы с закрытыми сведениями

2. Каналы утечки информации. Меры защиты

Второй канал – это **документы** – обычные бумажные документы, а также фотодокументы, видео- и звукозаписи, флеш-карты, CD, DVD

Способы несанкционированного доступа к документам, содержащим закрытые сведения:
– зрительный осмотр (для бумажных документов)
– копирование
– хищение

При осмотре и копировании – скрытность доступа
При осмотре – сложность запоминания
Для копирования – смартфоны и др.

Меры – организационные, т.е. связанные с людьми

2. Каналы утечки информации. Меры защиты

Третий канал – это **технические средства** хранения, обработки и передачи информации: ЭВМ, вычислительные сети и другие телекоммуникационные устройства

Программно-технические способы несанкционированного доступа к электронным документам, содержащим закрытые сведения:

– *преодоление программных средств* защиты (паролей)

– внедрение *программных закладок* (программ-троянов)

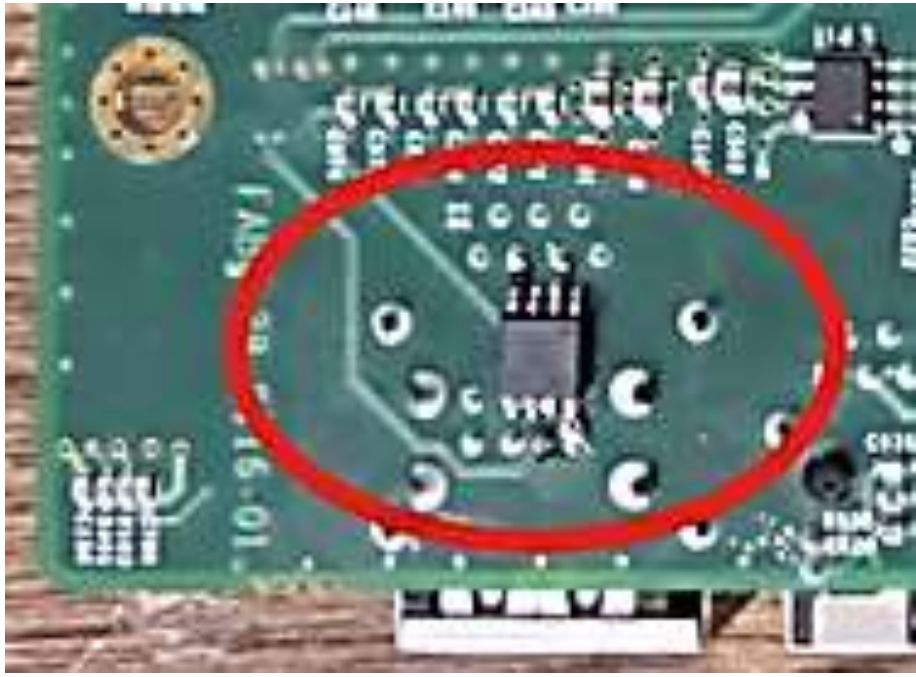
– использование *аппаратных закладок* (подключение устройств для съёма данных)

– *перехват электромагнитных излучений* и наводок (антенны)

2. Каналы утечки информации. Меры защиты

– использование *аппаратных закладок* (подключение устройств для съёма данных)

Съём данных, вводимых с клавиатуры



«Лишняя» микросхема-закладка, отправляющая пакеты в сеть

2. Каналы утечки информации. Меры защиты

Организационные меры защиты данных в ЭВМ и вычислительных сетях:

– исключение пребывания в помещениях посторонних лиц

– наблюдение за посторонними лицами, если их присутствие необходимо

– видеонаблюдение за помещениями

– разработка должностных инструкций пользователей

– ведение учёта пользователей сети

– установка запираемых хранилищ для ключевых носителей данных (*физическая* защита носителей)

– назначение администратора безопасности

2. Каналы утечки информации. Меры защиты

Задачи администратора безопасности:

– учёт и выдача аппаратных средств защиты информации (магнитных или электронных ключей доступа)
– своевременная смена паролей
– проведение инструктажа пользователей
– проверка соблюдения правил информационной безопасности пользователями
– правильная настройка компьютеров пользователей

2. Каналы утечки информации. Меры защиты

Настройка компьютеров пользователей:

– исключение использования режима *автоматического входа* пользователей в операционную систему при её загрузке (только через пароль)

– ведение *журнала событий* в операционной системе

– отключение в CMOC возможности *загрузки* операционной системы с флеш-карты, DVD, по сети

– исключение возможности *удаленного* управления компьютером

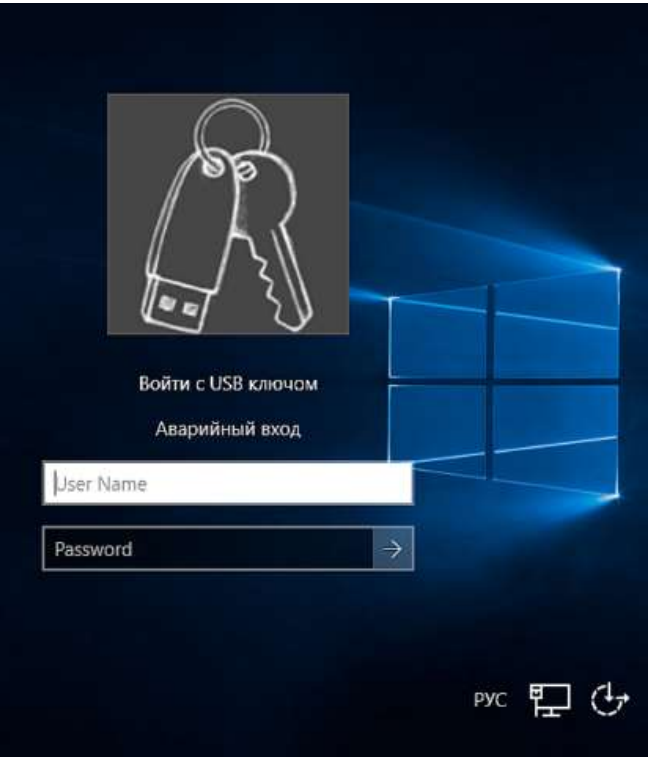
– организация полного *удаления временных* файлов и файлов подкачки

2. Каналы утечки информации. Меры защиты

Программно-технические меры защиты:

1) средства проверки подлинности:

– пароль
– биометрия
– магнитный или электронный ключ

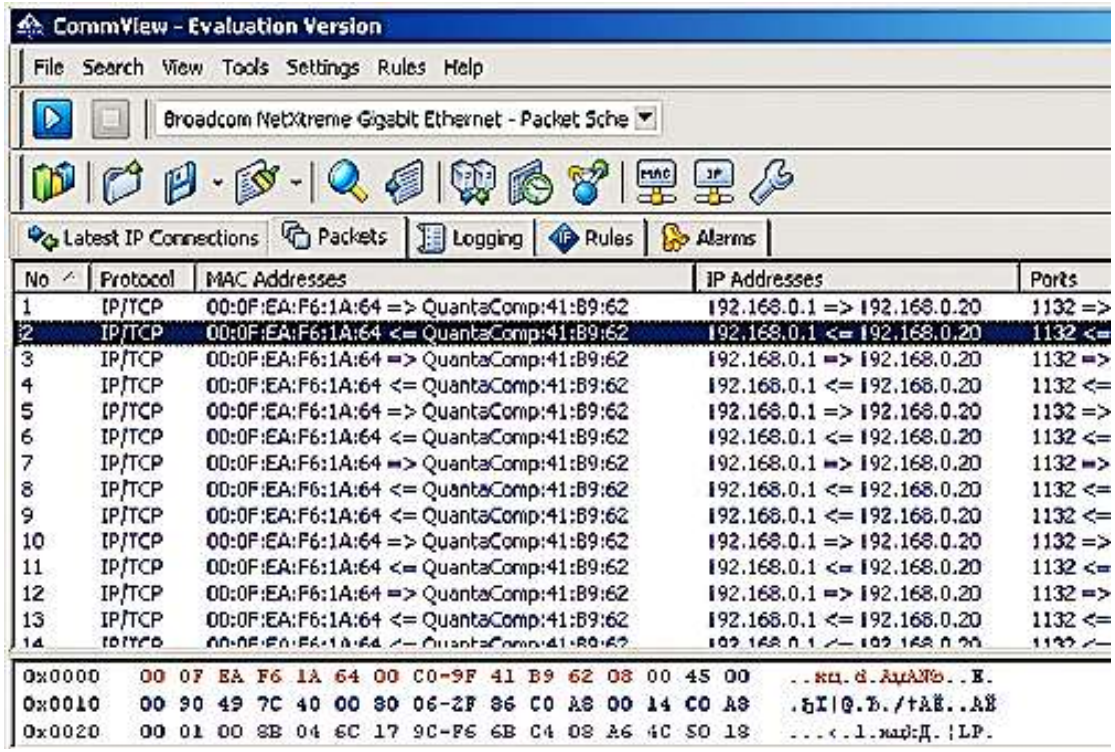


2. Каналы утечки информации. Меры защиты

Программно-технические меры защиты:

2) системы мониторинга сетей:

– межсетевые экраны
– антивирусные и антихакерские программы
– анализаторы протоколов

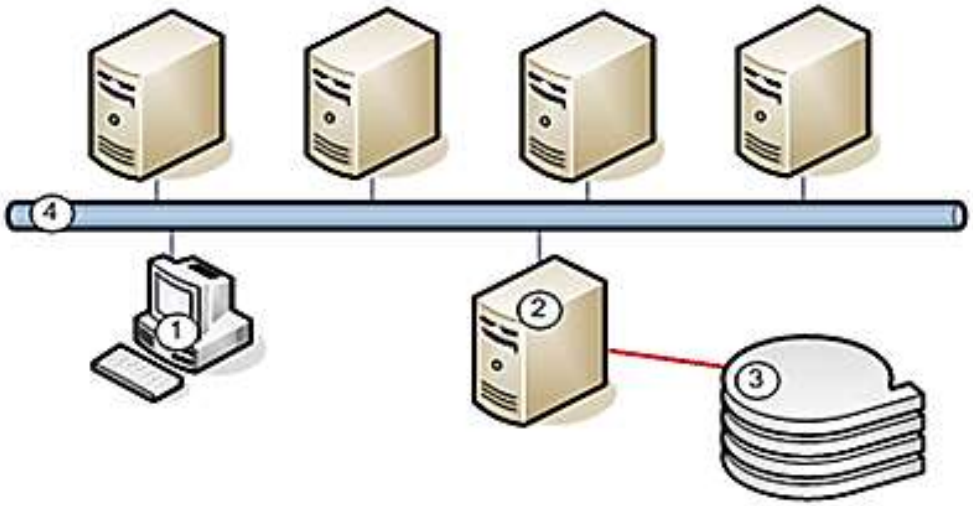


2. Каналы утечки информации. Меры защиты

Программно-технические меры защиты:

3) криптографические средства:
- – шифрование
- – электронная подпись

4) защита информации от непреднамеренного повреждения:
- – резервные накопители данных
- – источники бесперебойного питания



1 – консоль администратора
2 – медиа-сервер
3 – Ленточная библиотека
4 – локальная сеть

— Ethernet LAN
— Fiber Channel или SCSI

3. ПОНЯТИЕ И ВИДЫ ЭЛЕКТРОННОЙ ПОДПИСИ

3. Понятие и виды электронной подписи

Электронная информация — это сведения (набор символов, изображение, звукозапись, видеозапись и т.д.), закреплённые на электронном носителе (=данные)

ГОСТ ИСО 15489-1-2007:

документ – это закреплённая на материальном носителе *удостоверенная* информация, сохраняемая организацией или физическим лицом в качестве доказательства при подтверждении правовых обязательств или деловой деятельности

Сведения в документе – документированная информация

Чтобы **носитель** стал **документом**, а **информация** на нём – **документированной**, должны быть добавлены удостоверяющие и сопроводительные признаки (реквизиты)

3. Понятие и виды электронной подписи

Последовательность знаков сообщения, мысленно оторванных от носителя

Материальный носитель знаков сообщения

Знаки удостоверения сообщения на материальном носителе

Документи-рованная информация

Документ

Реквизиты

3. Понятие и виды электронной подписи

Электронная информация отличается от бумажной тем, что
1) может легко и неотличимо копироваться;
2) не имеет привязки к определённому носителю (хотя какой-то носитель нужен)

Если удостоверять носитель, то пропадают преимущества от лёгкости копирования и электронного обмена

Если носитель не удостоверять, то электронная информация на нём не будет документированной

Как же сделать электронную информацию документированной?

Решение этой задачи дали работы математиков 70-х годов XX столетия:

1. Производится отказ от привязки к первичному носителю
2. Для электронной информации применяется **электронное подписывание**

3. Понятие и виды электронной подписи

Электронная подпись – это электронная информация, добавляемая к сообщению для обеспечения

1) возможности ***установления лица-отправителя*** и
2) уверенности в ***неизменности*** (целостности) ***сообщения*** после его подписания

Как и обычная подпись, обеспечивает **неотказуемость**, т.е. невозможность отказаться от причастности к посылке сообщения

При подписывании электронного сообщения создаётся файл с электронной подписью, который посылается вместе с сообщением или отдельно от него

Материальный носитель подписанного электронного сообщения для целей удостоверения значения не имеет

3. Понятие и виды электронной подписи

Согласно ФЗ № 63 от 2011 года «Об электронной подписи», **виды электронных подписей** следующие:

простая неудостоверенная
простая удостоверенная
усиленная неудостоверенная
усиленная удостоверенная

Простая неудостоверенная – удостоверяет только отправку от определённой учётной записи.

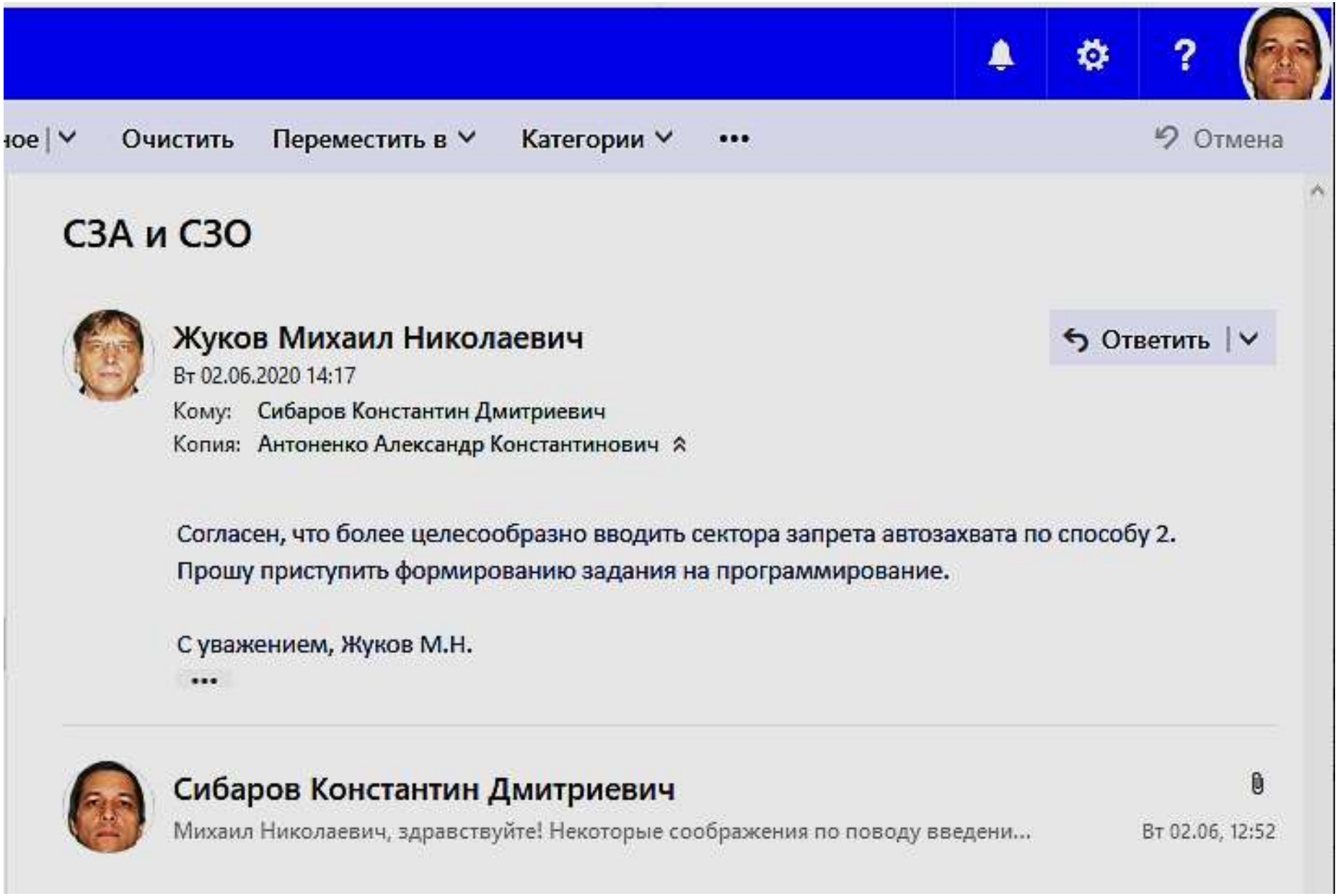
Учётная запись электронной почты создаётся самим пользователем: логин+пароль = имя+ключ

Простая удостоверенная – удостоверяет только лицо.

Код подтверждения высылается на телефонный номер, который получен по паспорту

Электронная почта предприятия – учётные записи у всех сотрудников (подтверждённые, именные)

3. Понятие и виды электронной подписи



3. Понятие и виды электронной подписи

Усиленная неудостоверенная – удостоверяет отправку от определённой учётной записи и неизменность сообщения.

Создаётся с помощью свободно распространяемых криптографических программ подписывания документов, например, Kleopatra

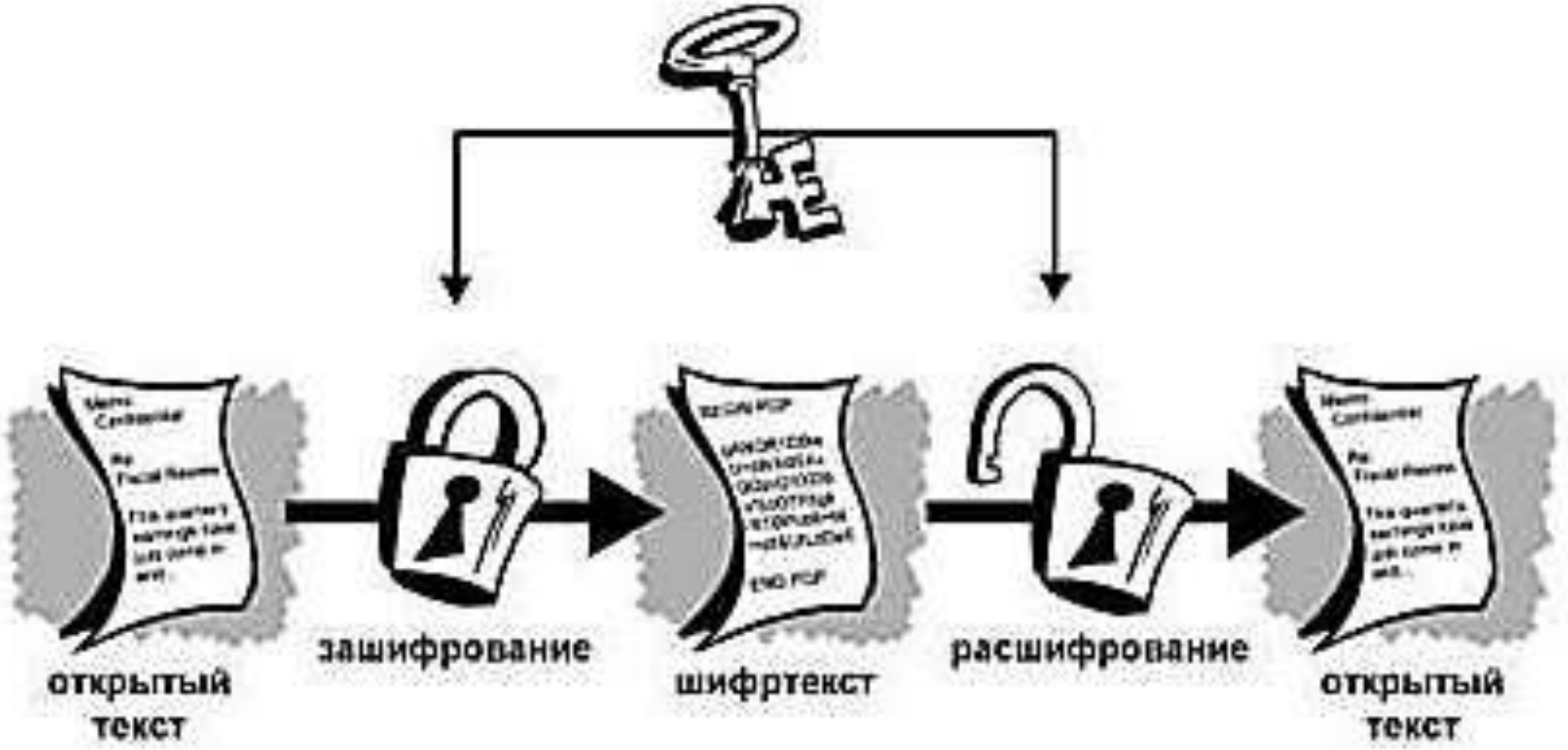
Усиленная удостоверенная – удостоверяет лицо и неизменность сообщения.

Программа и ключ подписи выдаётся *доверенной удостоверяющей службой*

Разрешение на выдачу программ, ключей и ведение учёта обратившихся лиц, выдаёт *Минкомсвязь России* (связи и массовых коммуникаций)

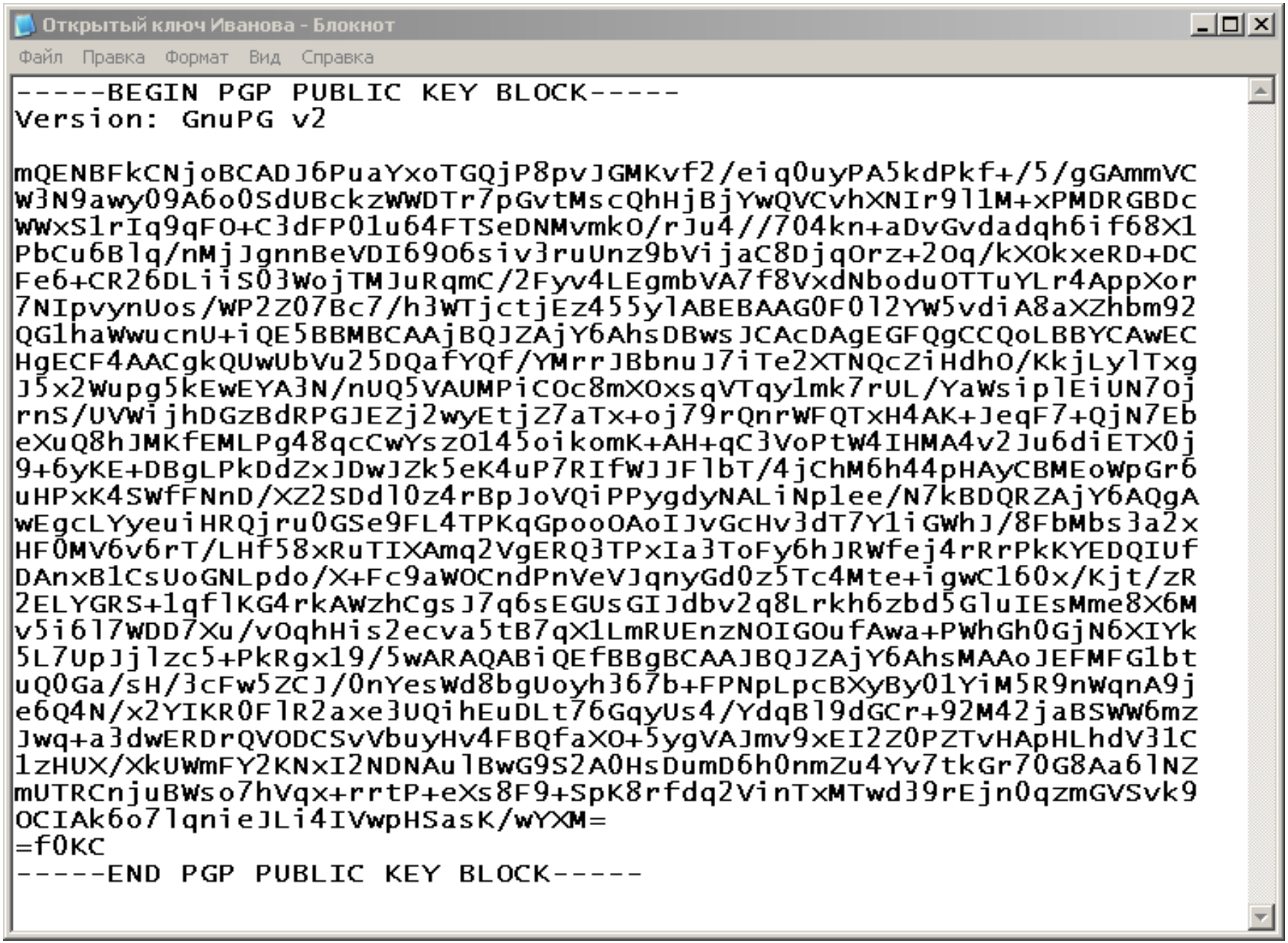
4. ОСНОВНЫЕ ПОНЯТИЯ КРИПТОГРАФИИ С ДВУМЯ КЛЮЧАМИ

КРИПТОГРАФИЯ С ОДНИМ КЛЮЧОМ



КРИПТОГРАФИЯ С ДВУМЯ КЛЮЧАМИ

ОТКРЫТЫЙ КЛЮЧ


Открытый ключ Иванова - Блокнот

Файл Правка Формат Вид Справка

```
-----BEGIN PGP PUBLIC KEY BLOCK-----
Version: GnuPG v2

mQENBFkCNjoBCADJ6PuaYxoTGQjP8pvJGMKvf2/eiq0uyPA5kdPkf+/5/gGAmmVC
W3N9awy09A6o0SdUBckzWWDTr7pGvtMscQhHjBjYwQVCvhXNIr9l1M+xPMDRGBDc
WWxS1rIq9qFO+C3dFP01u64FTSeDNMvmkO/rJu4//704kn+aDvGvdadqh6if68X1
PbCu6Blq/nMjJgnnBeVDI69O6siv3ruUnz9bVijaC8DjqOrz+2Oq/kXOkxeRD+DC
Fe6+CR26DLiiS03WojTMJuRqmC/2Fyv4LEgmbVA7f8VxdNboduOTTuYLr4AppXor
7NIpvynUos/WP2Z07Bc7/h3WTjctjEz455ylABEBAAG0F012YW5vdiA8aXZhbm92
QG1haWwucnU+iQE5BBMBCAAjBQJZAjY6AhsDBwsJCAcDAgEGFQgCCQoLBBYCAwEC
HgECF4AACgkQUwUbVu25DQafYQf/YMrrJBbnuJ7iTe2XTNQcZiHdhO/KkjLylTxg
J5x2Wupg5kEwEYA3N/nUQ5VAUMPiCOc8mXOxsqVTqy1mk7rUL/YaWsiplEiUN7Oj
rnS/UVWijhDGzBdRPGJEZj2wyEtjZ7aTx+oj79rQnrWFQTxH4AK+JeqF7+QjN7Eb
eXuQ8hJMKfEMLPg48qcCwYszO145oikomK+AH+qC3VoPtW4IHMA4v2Ju6diETX0j
9+6yKE+DBgLPkDdZxJDwJZk5eK4uP7RIfWJJFlbT/4jChM6h44pHAyCBMEoWpGr6
uHPxK4SWfFNnD/XZ2SDdl0z4rBpJoVQiPPygdyNALiNp1ee/N7kBDQRZAjY6AQgA
wEgcLYyeuiHRQjru0GSe9FL4TPKqGpooOAoIJvGcHv3dT7Y1iGWhJ/8FbMbs3a2x
HF0MV6v6rT/LHf58xRuTIXAmq2VgERQ3TPxIa3ToFy6hJRWfej4rRrPkKYEDQIUf
DAnxB1CsUoGNLpdo/X+Fc9aWOCndPnVeVJqnyGd0z5Tc4Mte+igwC160x/Kjt/zR
2ELYGRS+1qflKG4rkAWzhCgsJ7q6sEGUsGIJdbv2q8Lrkh6zbd5GluIEsMme8X6M
v5i6l7WDD7Xu/vOqhHis2ecva5tB7qX1LmRUEnzNOIGOufAwa+PWhGh0GjN6XIYk
5L7UpJjlzc5+PkRgx19/5wARAQABiQEfBBgBCAAJBQJZAjY6AhsMAAoJEFMFG1bt
uQ0Ga/sH/3cFw5ZCJ/0nYesWd8bgUoyh367b+FPNpLpcBXyBy01YiM5R9nWqnA9j
e6Q4N/x2YIKR0FlR2axe3UQihEuDLt76GqyUs4/YdqBl9dGCr+92M42jaBSWW6mz
Jwq+a3dwERDrQVODCSvVbuyHv4FBQfaXO+5ygVAJmv9xEI2Z0PZTvHApHLhdV31C
1zHUX/XkUWmFY2KNxI2NDNAulBwG9S2A0HsDumD6h0nmZu4Yv7tkGr70G8Aa6lNZ
mUTRCnjuBWso7hVqx+rrtP+eXs8F9+SpK8rfdq2VinTxMTwd39rEjn0qzmGVSvk9
OCIAk6o7lqnieJLi4IVwpHSasK/wYXM=
=f0KC
-----END PGP PUBLIC KEY BLOCK-----
```

ЗАКРЫТЫЙ КЛЮЧ

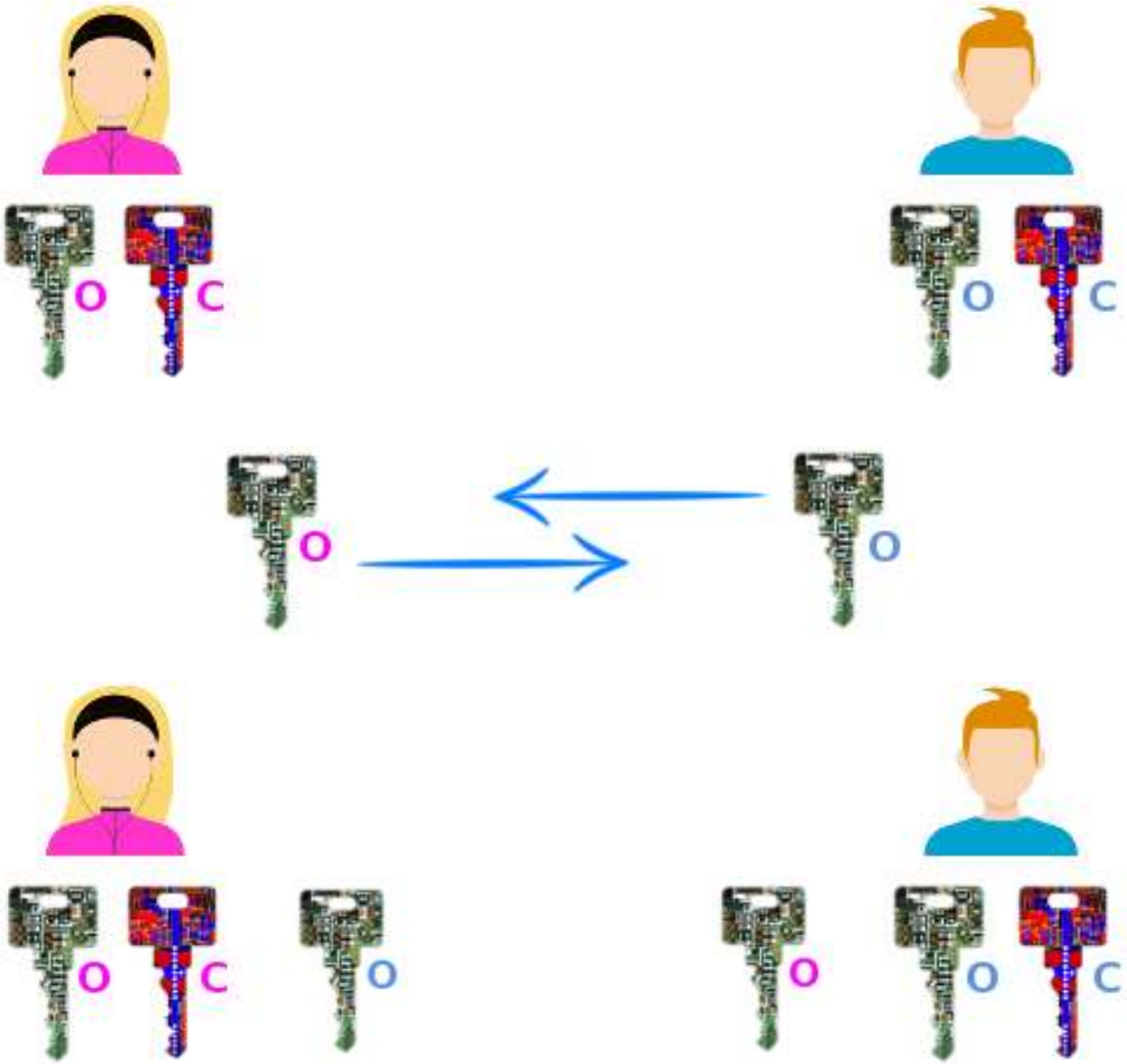
Закрытый ключ Иванова - Блокнот

Файл Правка Формат Вид Справка

```
-----BEGIN PGP PRIVATE KEY BLOCK-----
Version: GnuPG v2

lQO+BFkCNjoBCADJ6PuaYxoTGQjP8pvJGMKvf2/eiq0uyPA5kdPkf+/5/gGAmmVC
WJN9awy09A6o0SdUBckzWWDTr7pGvtMscQhHjBjYwQVCvhXNIr9l1M+xPMDRGBDc
WWxS1rIq9qFO+C3dFP01u64FTSeDNMvmkO/rJu4//704kn+aDvGvdadqh6if68X1
PbCu6Blq/nMjJgnnBeVDI69O6siv3ruUnz9bVijaC8DjqOrz+2Oq/kXOkxeRD+DC
Fe6+CR26DLiiSO3WojTMJuRqmC/2Fyv4LEgmbVA7f8VxdNboduOTTuYLr4AppXor
7NIpvynUos/WP2Z07Bc7/h3WTjctjEz455ylABEBAAH+AwMCfMgI+885nZKunOWA
lHtVMf/d7b/HL0JeAjJ6lPymzsvhJZP8Fw55i5gH6MzbTTen2MukcjNc/xDz+qyp
dXPJKfRg3wp4xFxGayaDrlTI8rNZmrXvuZPgu8UJB/bqouruk7uDO2PO7G9QGiNO
Yb++NcUAAJjIo5uhd9Kxq9E+OJ6LiqTre0z54mbbPTbWH5cg3JWwY9jmy01ycLLm
b9Dx/81cP6SjF6PHmWkTyGsylfnyE3926zlIgONCVOMUA90CMgPz2YT6PAtmFmOw
Z9sV3yb9QZs5LesL9Wes1KcVImQKjMv5yrIzjCx+MVJm38AQcHxO59N2KpWCENZK
2VLk0gMubrmUj82hCNXQA2u80hoRQZADlj4ls0VigKplsguRrFPOH7lDz92z2Gsj
lNZNjxI8CzRxx/4p7kKvHfDdZ4sWIpArvKn8tiG0NoBrX83jIX7lFi8kl8FoTAr4
v8NX5AOgJdhzQyYl5GQ856jk2ccz5Dmd/eYPgBXuq6XAEvv43vz/2ptx3TTKKQRR
ebEIt6Rgvrxcq5oXS7fp9DyulIKFIxE+VrYWZ6hYkRC/RNM+biF5/4c+jQ9C2Yd3
YUVochTmmVPI0dYkdzbSW3f9sVlNIqFlhn8dE+uDoy5jKV9DIq73VJg0mH4CPKlJ
GkAapmdZ/LSLFlyGu4nD3/Wh9zfA54nEXQTDqCw/lG4B/0Q2CEEmJGCecofrOCYF
yErMKdQCD1H3dTUMvVR9LwTXxcyvwDU7WbV+XfJjZgv9TLKYwtFpy5yO65o5va3L
xBbLjzTth2qrZxQOPNhCsId66xBrQ6ktO3YGWrQc2+wMn4cKQU4VQP5NaTuOiouM
hifcjZGGnPC2E2yfuqHsYeFScpNudHWOTq/+6UokKn55hmZS8U0XpBJpw0fc7HDB
s7QXSXZhbm92IDxpdmFub3ZAbWFpbC5ydT6JATkEEwEIACMFAlkCNjoCGwMHCwkI
BwMCAQYVCAIJCgsEFgIDAQIeAQIXgAAKCRBTBRtW7bkNBp9hB/9gyuskFue4nuJN
7ZdMlBxmId2E78qSMvKVPGAnnHZa6mDmQTARgDc3+dRDluBQw+II5zyZc7GypVOr
LWaTutQv9hpayKmUSJQ3s6OudL9RVaKOEMbMF1E8YkRmPbDIS2NntpPH6iPv2tCe
tYVBPEfgAr4l6oXv5CM3sRt5e5DyEkwp8Qws+DjypwLBizM7XjmiKSiYr4Af6oLd
Wg+lbggcwDi/Ym7p2IRNfSP37rIoT4MGAs+QNlnEkPAlmTl4ri4/tEh9YkkWVtP/
iMKEzqHjikcDIIEwShakavq4c/ErhJZ8U2cP9dnZIN2XTPisGkmhVCI8/KB3I0Au
I2nV5783nQO+BFkCNjoBCADASBwtjJ66IdFCOu7QZJ70UvhM8qoamig4Cggm8Zwe
/d1PtjWIZaEn/wVsxuzdrbEcXQxXq/qtP8sd/nzFG5MhcCarZWARFDdM/EhrdOgX
LqElfZ96PitGs+QpgQNAhR8MCfEHUKxSgY0u12j9f4Vz1pY4Kd0+dV5UmqfIZ3TP
lNzgy176KDALXrTH8qOJ/NHYQtgZFL7Wp+UobiuQBbOEKCwnurqwQZSwYgl1u/ar
wuuSHrNt3kaW4gSwyZ7xfoy/mLqXtYMPte7+86qEeKzZ5y9rm0HupfUuZFQSfM04
gY658DBr49aEaHQaM3pchiTkvtSkmOXNzn4+RGDHX3/nABEBAAH+AwMCfMgI+885
nZKug68kkssHB8zqoJtLr8yxJ7HiKFCo+cPOcZRbpGz8EDQSmOtRGHAkal9itaKO
J75TM3qxgXgXM5xW2mFF+GJzB0tsIZFvpF223oEofmOvXE2iGzhoeNH+n9sNt2GI
Xj2mgkedAJjrGKY7mqw2zbPAnpOzFJicTIUlFxib8wkxAW/UEiNbFh+HQ06T3LXv
qY7Cknnb4bE5MXSTmYYPLJHdXUeZ3vnhECypQEqrzfE02RP6yhN35f5zvKmoXAcH
gQGDoG3WG/gRA7ojfsKt/4uEo7ddnSmRuSR1BHGPdDRWfRvUb7jFf5M2bSp7/0L4
6bG7B4toBSp+pysjp9k+LHvr4QrtcbBr6aLSMHFrFsC8k17I0m2QclDEAH8ygxZ0
ZvJ13vSytD4nYKcBFyMW/ArDrNWgzy3qRjjb+PAUnYF4gbQ3kGnmwrqBiH4cSsVJ
SonOJxRX26/hhns9rjLi0UzvvJuHre3hWNoh03giXJyYkgmELeFUuvKSmUc34/fX
EZKrTlJK4Y8rKJ5bLUOUpKaQWCNDWAih/EwnHgxvFbigD5CfEoIWdCCQukGLkTS7
yYqZz7HolEMVTraN4Q4TcdVmdvxNsOAQSW1MC2XcGUkyBbZb9vlHl1WGaATA6EKF
mRQ7QwtRHYHD8NTyxVIMqc6ZMmcozhrVeb0zmjVhWG8njxcP8oh+lNcEt3CMPiGK
LpHkq2Mq0XsahZwHQkglXSK0Yj6d3OROTeyJ6liZmCjR4XGirCvlOuNIzGJyAA7l
YmCw3NKTnlBJS4cSOqF/XD9kwDWoKGViSlqC78GQmkkSm+RZCreZeZ7zjwYlmlzT
wmD3OmglgXarYPSmfFJ08uDL53kmlf5JmQEPd0FDWUt6qOBuLKBu0pUbO/x/Weoj
WKwweroZBIkBHwQYAQgACQUCWQI2OgIbDAAKCRBTBRtW7bkNBmv7B/93BcOWQif9
J2HrFnfG4FKMod+u2/hTzaS6XAV8gctNWIjOUfZ1qpwPY3ukODf8dmCCkdBZUdms
Xt1EIoRLgy7e+hqslLOP2HagZfXRgq/vdjONo2gUllupsycKvmt3cBEQ60FTgwkr
1W7sh7+BQUH2lzvucoFQCZr/cRCNmdD2U7xwKRy4XVd9Qtcx1F/15FFphWNijcSN
jQzQLpQcBvUtgNB7A7pg+odJ5mbuGL+7ZBq+9BvAGupTWZlE0Qp47gVrKO4Vasfq
67T/nl7PBffkqSvK3JatlYp08TE8Hd/axI59Ks5hlUr5PTgiAJOqO5ap4niS4uCF
cKR0mrCv8GFz
=zMLl
-----END PGP PRIVATE KEY BLOCK-----
```

ПРЕДВАРИТЕЛЬНЫЙ ОБМЕН ОТКРЫТЫМИ КЛЮЧАМИ



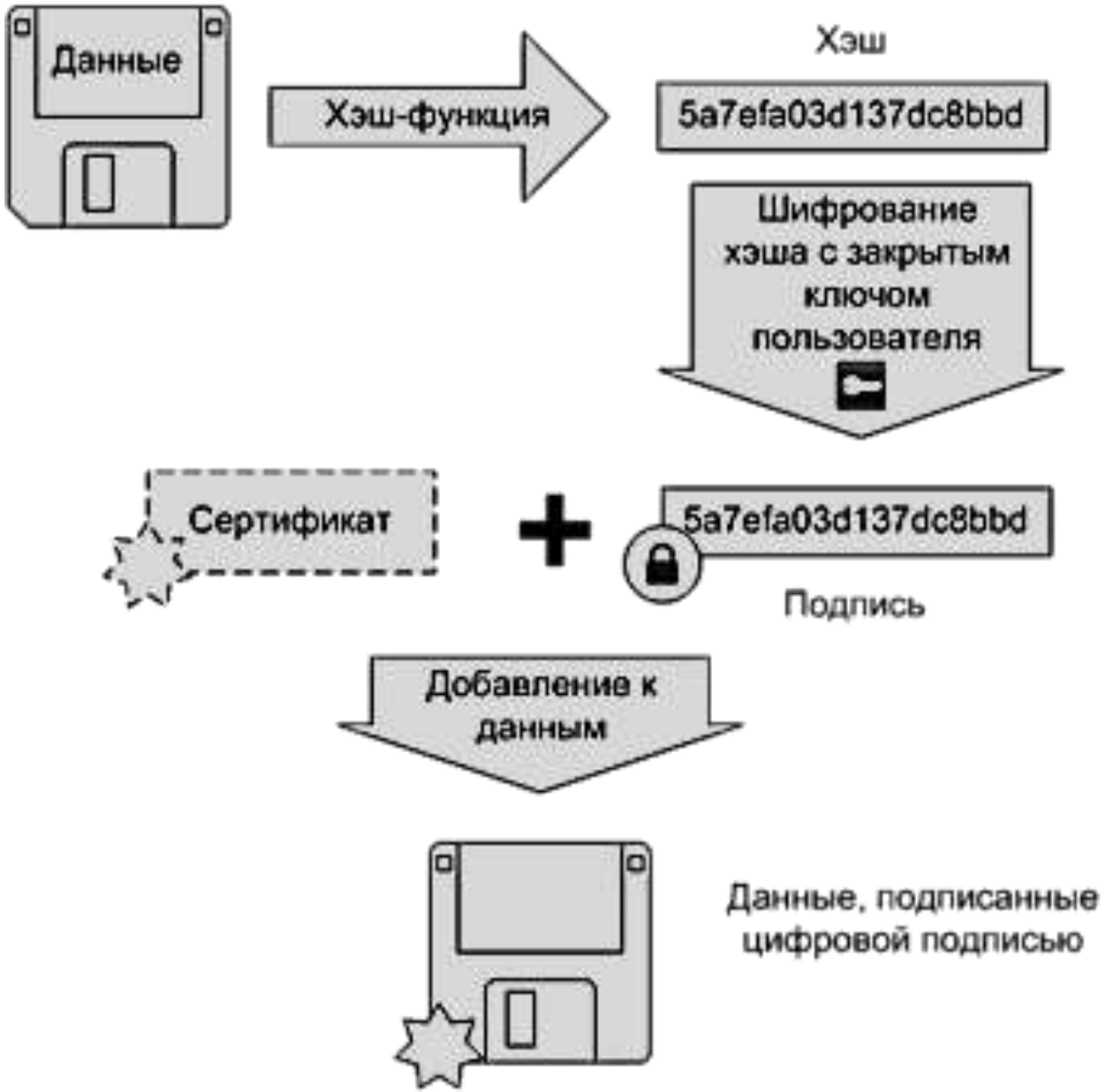
РАЗДЕЛЬНОЕ ШИФРОВАНИЕ СООБЩЕНИЯ И КЛЮЧА

РАСШИФРОВКА КЛЮЧА И СООБЩЕНИЯ

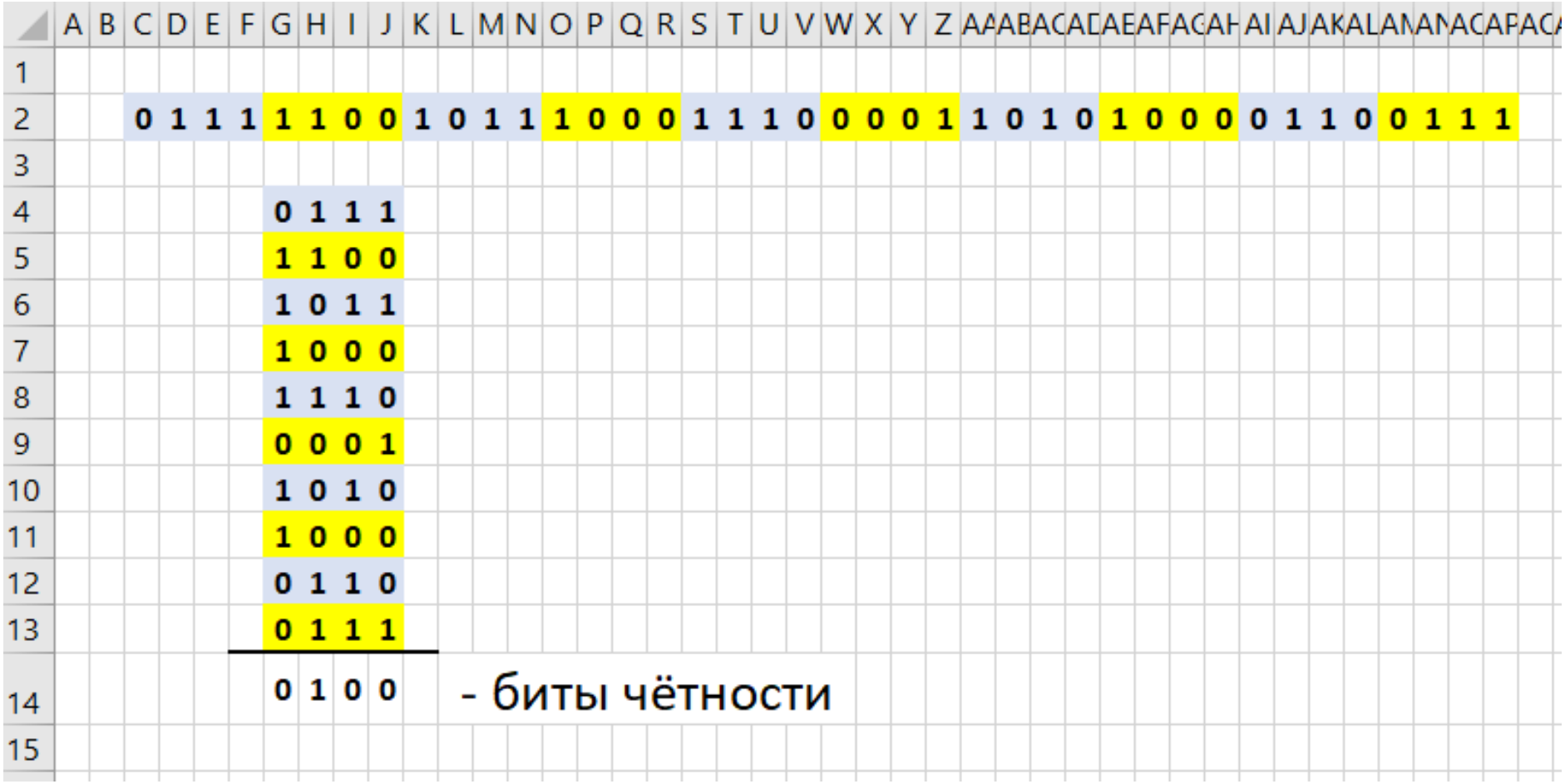
5. КРИПТОГРАФИЧЕСКАЯ СУЩНОСТЬ ЭЛЕКТРОННОЙ ПОДПИСИ

СУЩНОСТЬ ЭЛЕКТРОННОЙ ПОДПИСИ

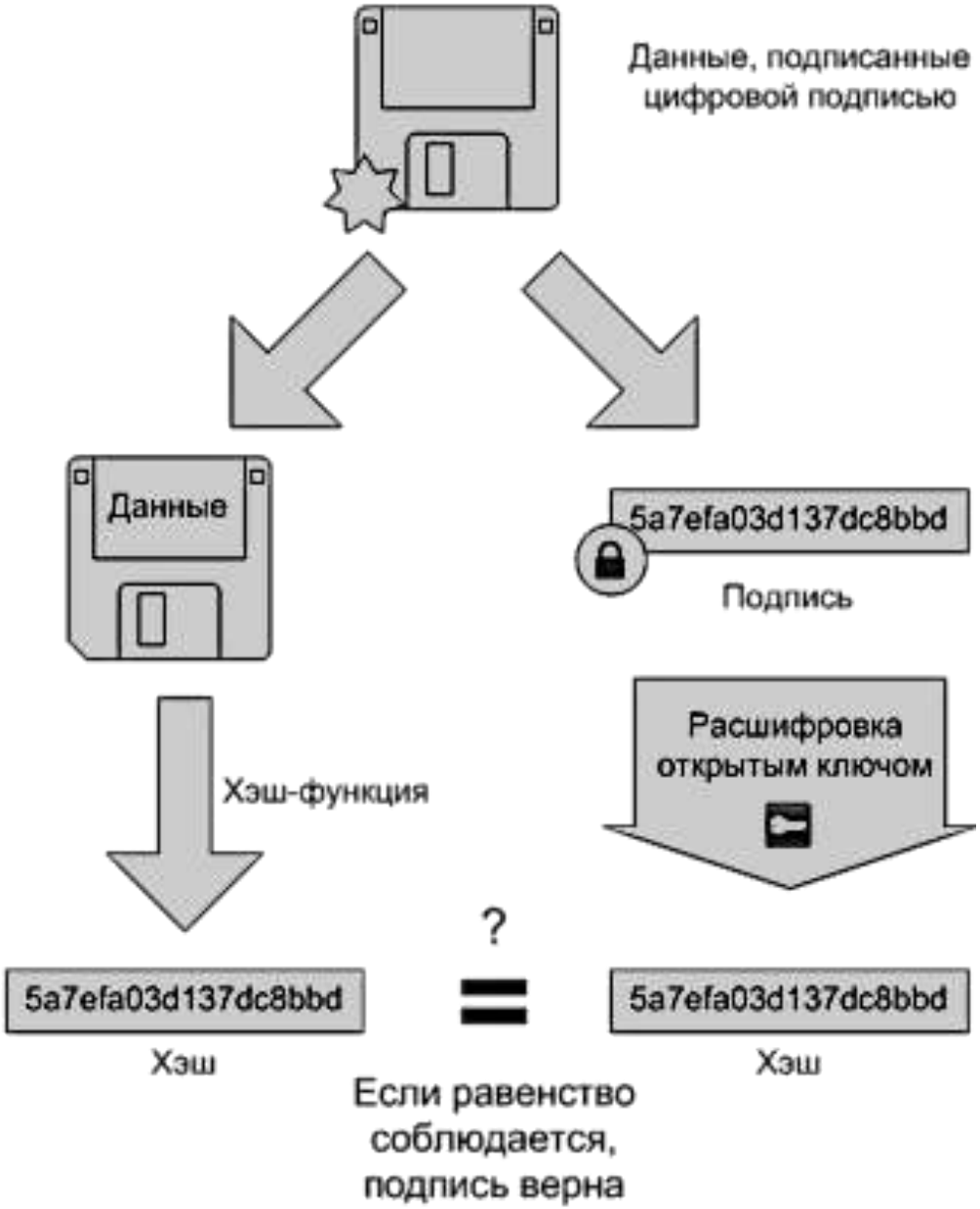
ПОДПИСЫВАНИЕ СООБЩЕНИЯ. ХЭШ



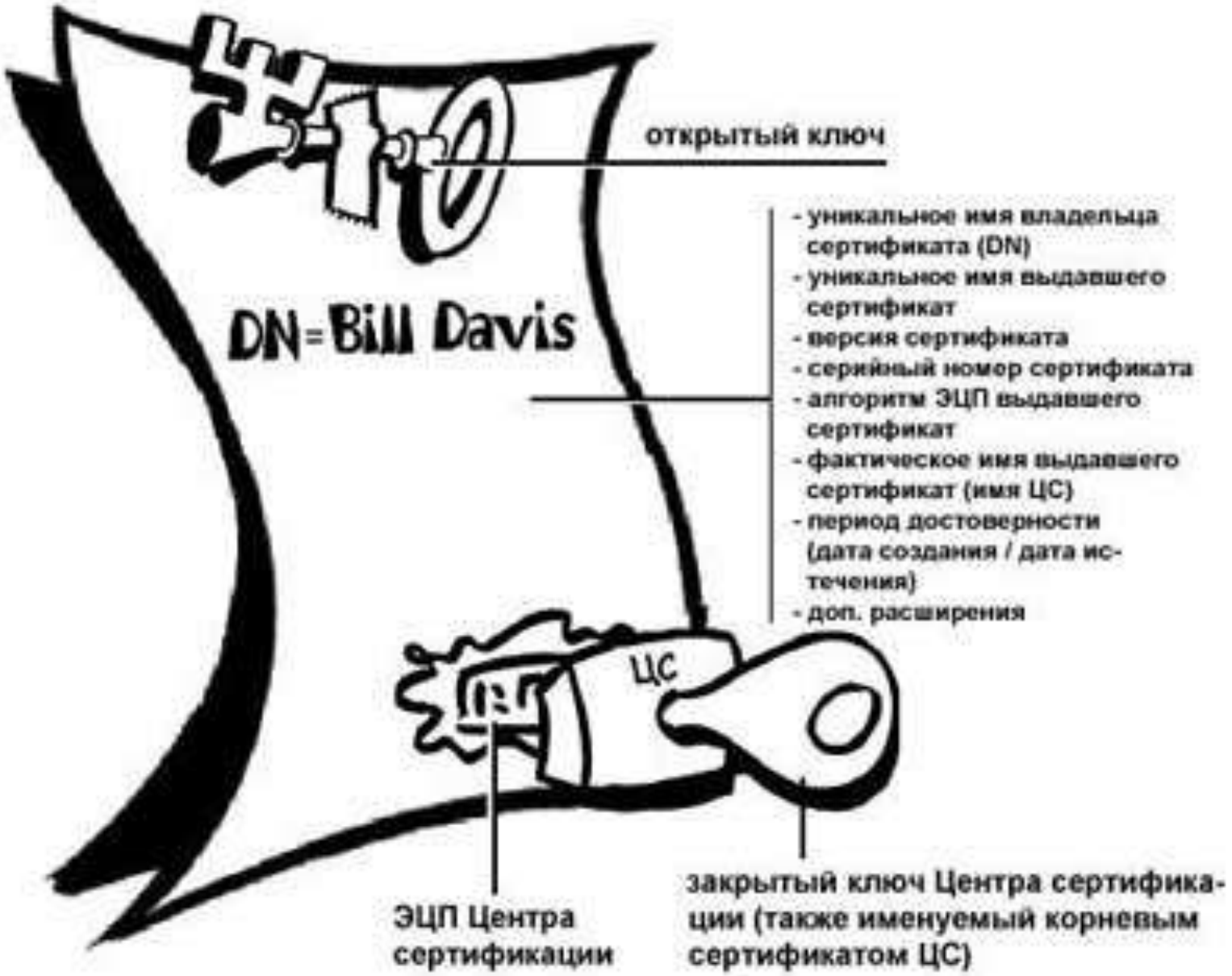
ПРОСТЕЙШИЙ ПРИМЕР ХЭШ – КОНТРОЛЬНАЯ СУММА



ПРОВЕРКА ЭЛЕКТРОННОЙ ПОДПИСИ



Электронный сертификат ключа



Порождение открытого и закрытого ключей

Общий порядок порождения открытого и закрытого ключей *(для общего представления, а не для выучивания):*

Имеется заранее вычисленная последовательность простых чисел вплоть до 2 в 1024-й степени

1. Из неё случайным образом берутся два достаточно больших простых числа
2. Вычисляется произведение этих простых чисел
3. Первое из этих двух чисел подвергается определённому математическому преобразованию с участием ещё одного случайного целого числа
4. Число, полученное по п.3, подвергается своему математическому преобразованию

В итоге получаются два новых целых числа по пп. 3 и 4

Первое новое число вместе с произведением – это открытый ключ

Второе новое вместе с произведением – это закрытый ключ

Порождение открытого и закрытого ключей (пример)

1. Берутся два простых числа:
   $p = 3$ и $q = 5$
2. Вычисляется их произведение:
   $n = p \cdot q = 3 \cdot 5 = 15$
3. Вычисляется функция Эйлера:
   $\Phi(n) = (p - 1) \cdot (q - 1) = 2 \cdot 4 = 8$
4. Подбирается число, взаимно простое с $\Phi(n) = 8$: $e = 9$
   Взаимно простые числа не имеют общих делителей, кроме 1. Условие: $1 < e < n$
5. Подбирается число, обратное к e по модулю $\Phi(n)$: $d = 17$
   d таково, что остаток от деления $(e \cdot d)$ на $\Phi(n)$ равен **1**
   Т.е. $(9 \cdot 17) / 8 = 161/8 = (160+1)/8 = 160/8 + \mathbf{1}/8$, остаток **1**
6. **Открытый** ключ – это пара чисел e и n : {9, 15}
7. **Закрытый** ключ – это пара чисел d и n : {17, 15}

Порядок шифрования и расшифровывания

Шифрование:

Есть исходное сообщение (или его часть) –
длинное двоичное число: x

1. Оно возводится в степень e : x^e
(e – первая часть открытого ключа)
2. Ищется остаток от деления x^e на n : $x^e \bmod n = c$
(n – вторая часть открытого ключа) Остаток(x^e/n) = c

c – зашифрованное сообщение

Расшифровывание:

Есть зашифрованное сообщение – двоичное число: c

1. Оно возводится в степень d : c^d
(d – первая часть закрытого ключа)
2. Ищется остаток от деления c^d на n : $c^d \bmod n = x$

x – расшифрованное исходное сообщение

Вычислительная сложность расшифровывания

Алгоритм вычисления ключей общеизвестен – приведён в Википедии

Программы для их получения выставлены в сети

Алгоритмы шифрования и расшифровывания тоже

Оба ключа математически связаны между собой, т.е. зная открытый ключ, можно вычислить закрытый и расшифровать сообщение или подделать электронную подпись

Однако вычислительная сложность математической задачи определения закрытого ключа по открытому такова, что на её решение требуются годы и даже десятилетия вычислений на множестве компьютеров одновременно

Вследствие этого пропадает смысл в такой расшифровке

Применение криптографии с двумя ключами при передаче данных в Межсети

Протокол защищённой передачи данных https

Два сервера постоянно обмениваются служебными сообщениями о своём состоянии (готовности)

При необходимости передачи данных сервер-отправитель сообщает об этом серверу-получателю и посылает свой открытый ключ

Сервер-получатель в ответ посылает свой открытый ключ

Сервер-отправитель делит длинное передаваемое сообщение на части (содержимое пакетов), и каждую часть шифрует открытым ключом сервера-получателя

Пакеты передаются по открытому каналу связи

Сервер-получатель извлекает содержимое из пакетов и каждую часть расшифровывает своим закрытым ключом

Вопросы для самопроверки

1. Основные понятия защиты информации
2. Понятие и виды электронной подписи
3. Каналы утечки информации. Меры защиты информации
4. Основные понятия криптографии с двумя ключами
5. Криптографическая сущность электронной подписи