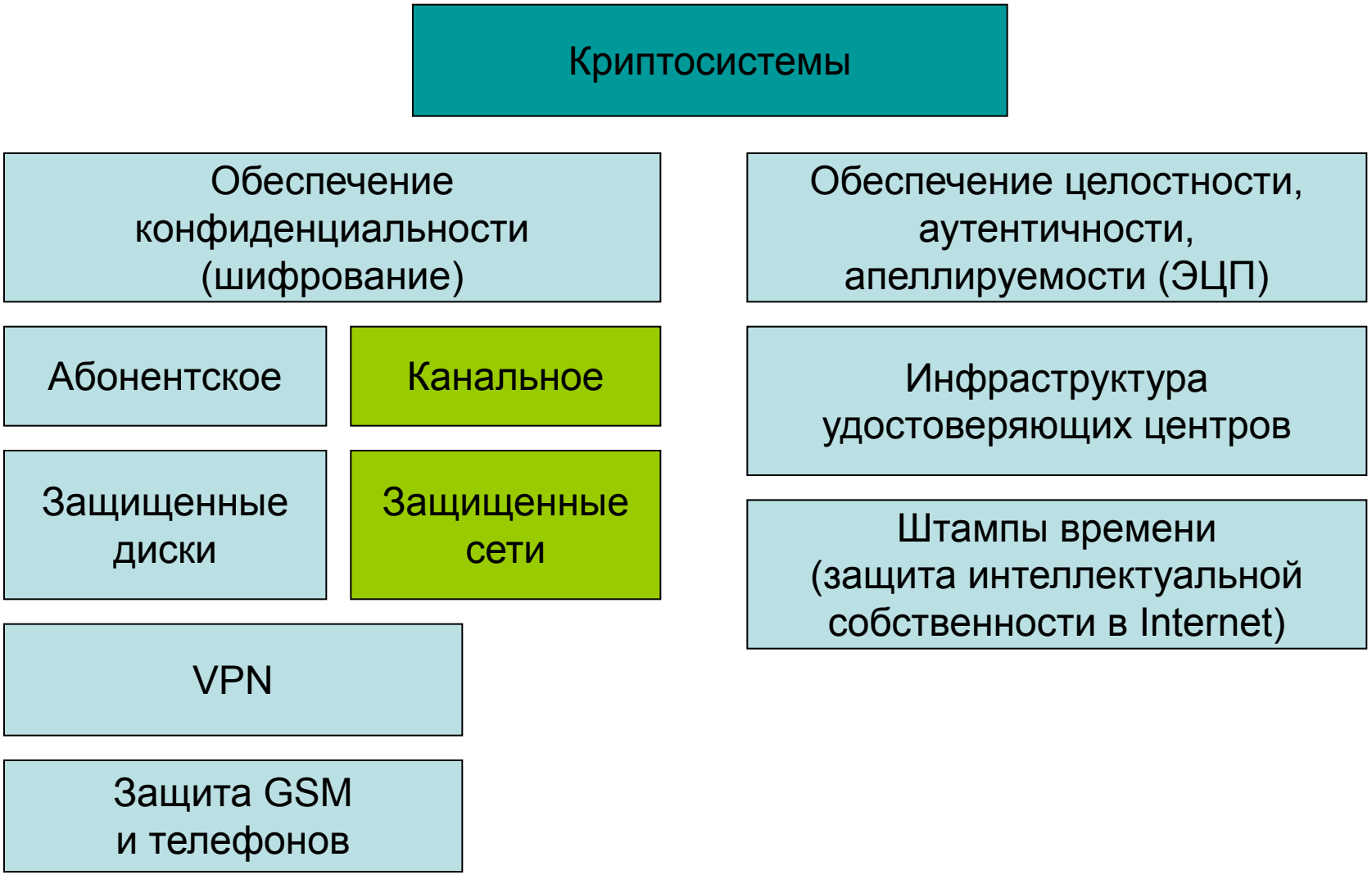
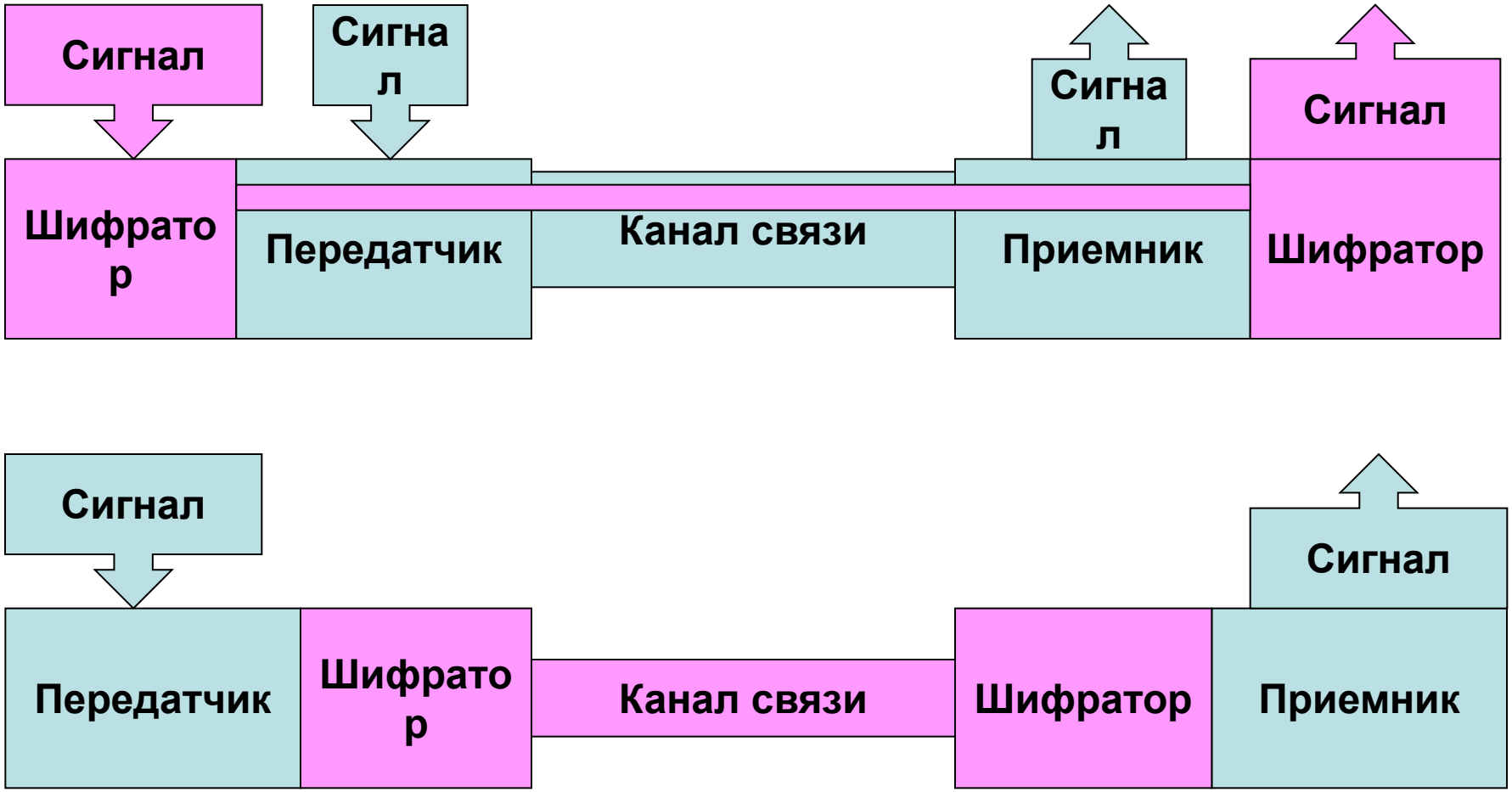
Криптографические методы защиты информации.

Перспективные направления разработок.

Современные направления



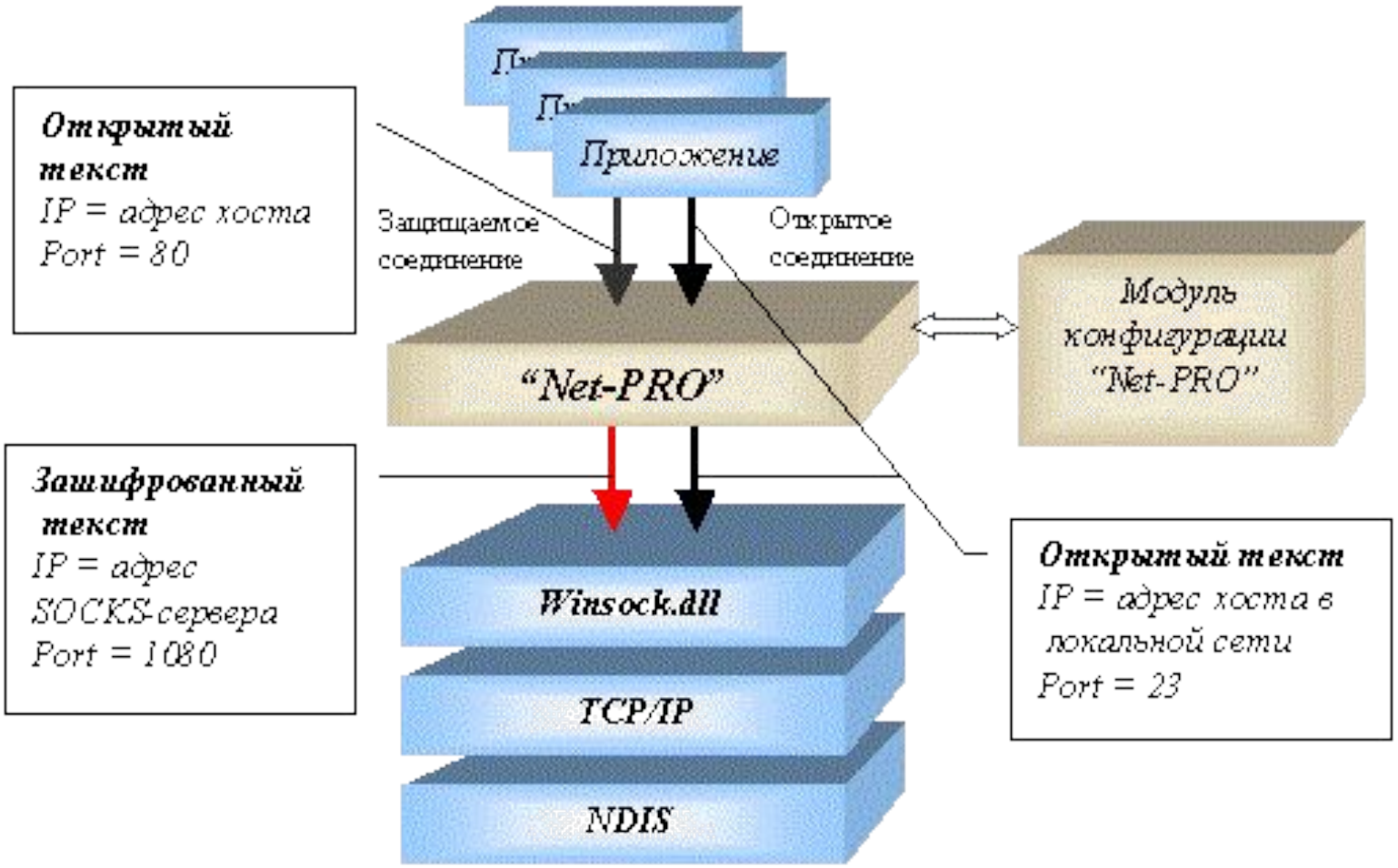
Абонентское vs. канальное



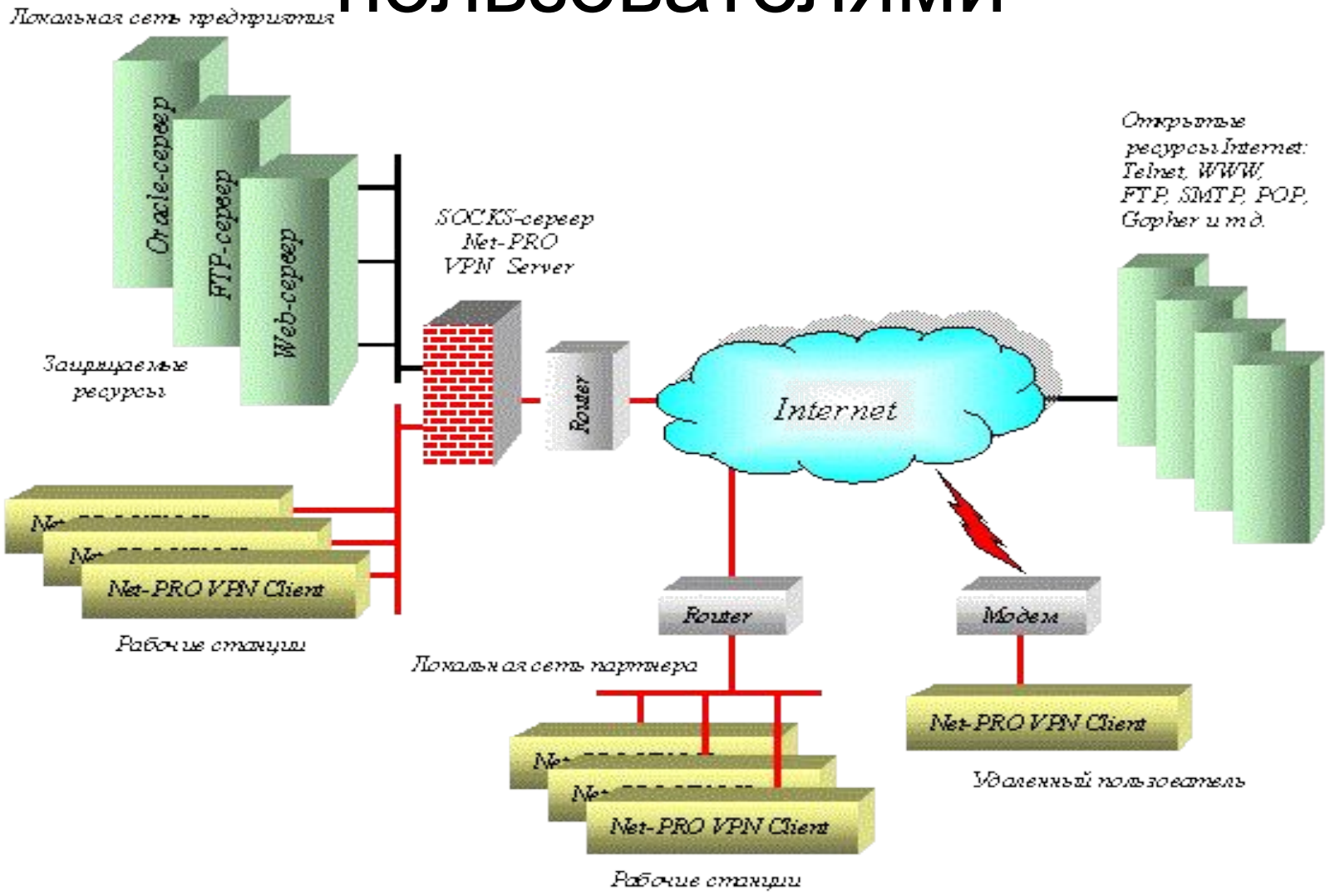
Абонентское шифрование

	Защита диска	Защита файла
Достоинства	**Доступ ко всему содержимому диска по одному ключу.** **Невозможность аналитической оценки содержимого.** **«Прозрачность» шифрования.**	**Гибкость работы с файлами.** **Возможность использовать любой режим и алгоритм шифрования.** **Экономия вычислительной мощности.**
Недостатки	**Рационально использовать только режим шифрования «Электронно-цифровой книги».** **Большие затраты вычислительной мощности.** **Негибкость работы.**	**Шифрование каждого файла на своем ключе.** **Возможность аналитической оценки содержимого дисков.** **«Непрозрачность» шифрования.**

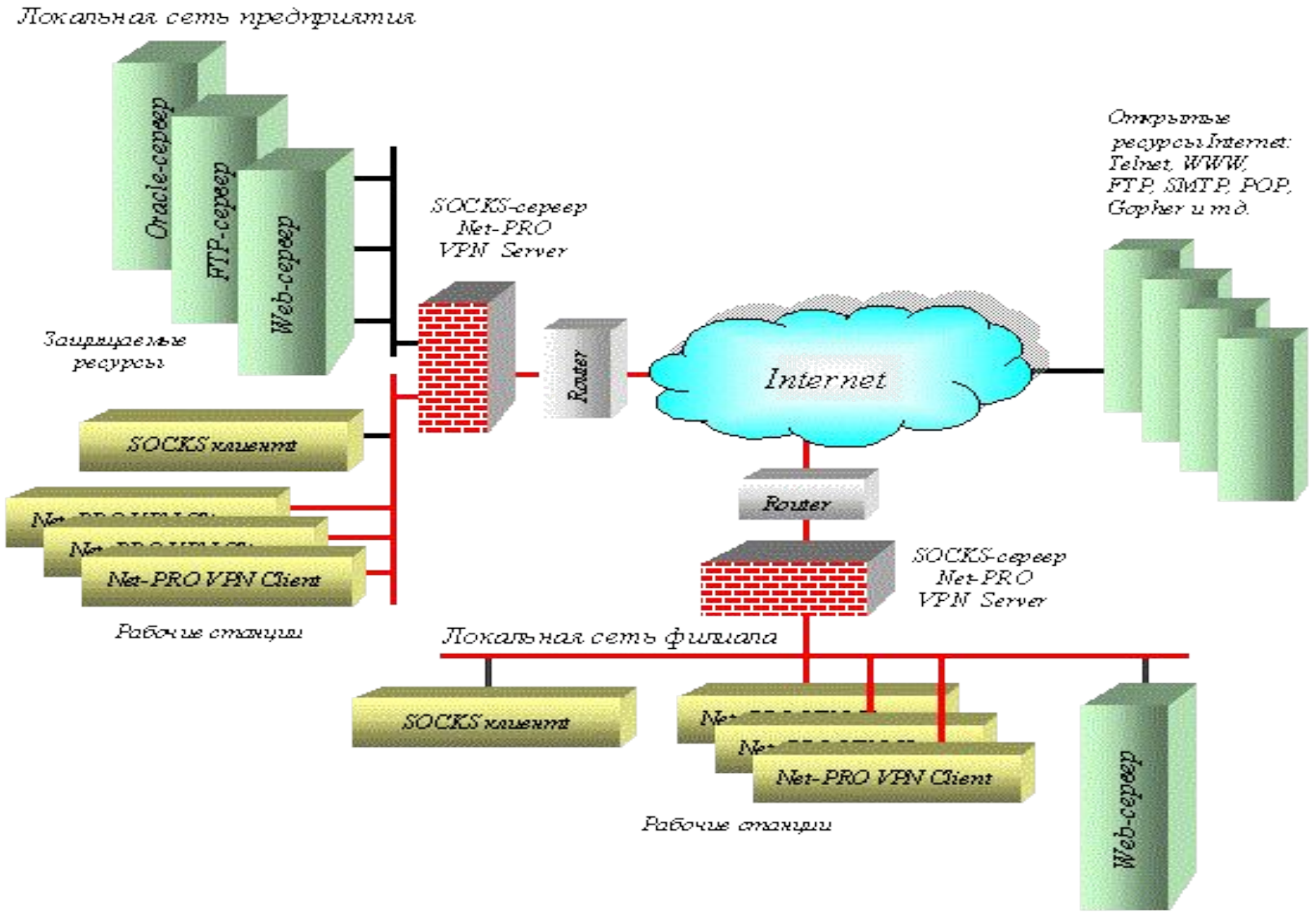
SOCKS-ИФИКАЦИЯ



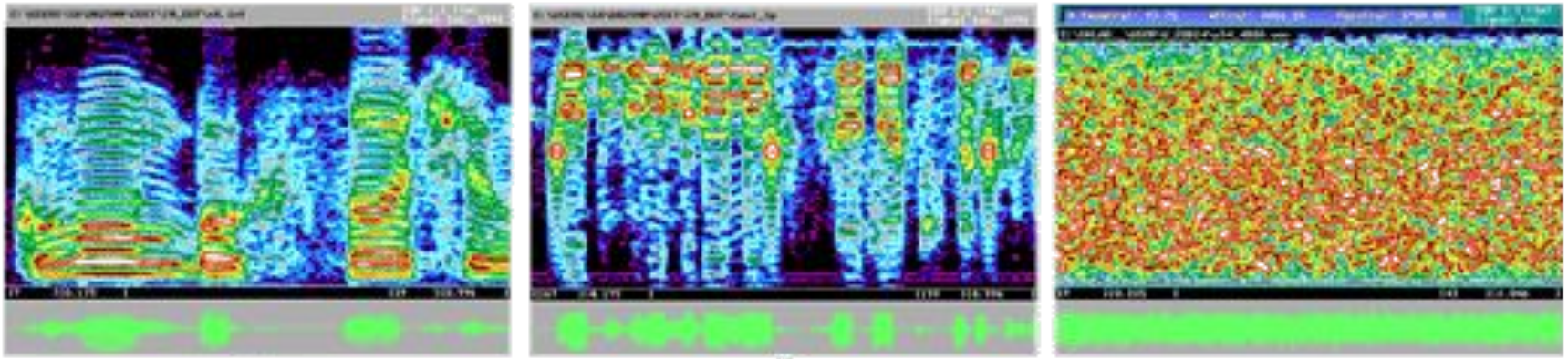
Работа с удаленными пользователями



Работа с филиалами



Виды сигналов ТС



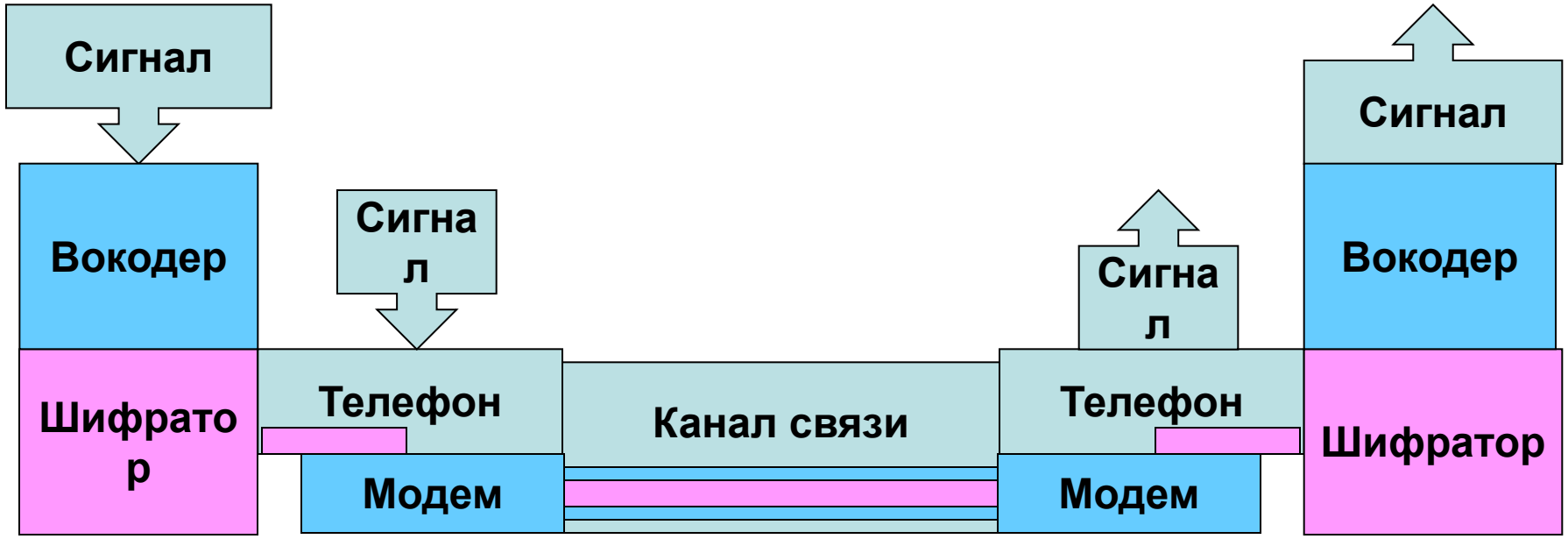
а б в

а) Аналоговый сигнал

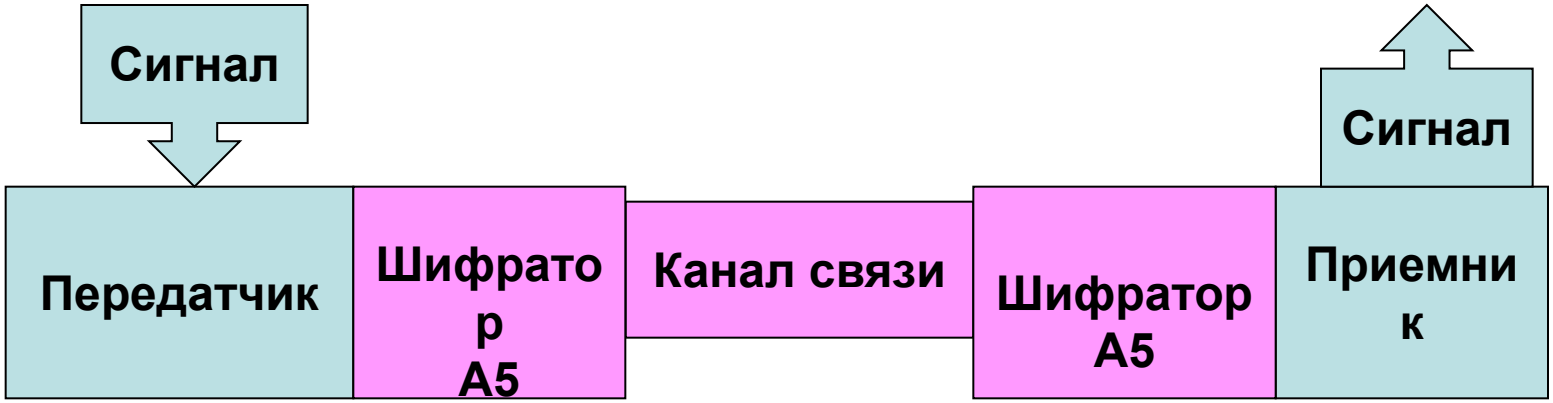
б) Скремблированнный аналоговый сигнал

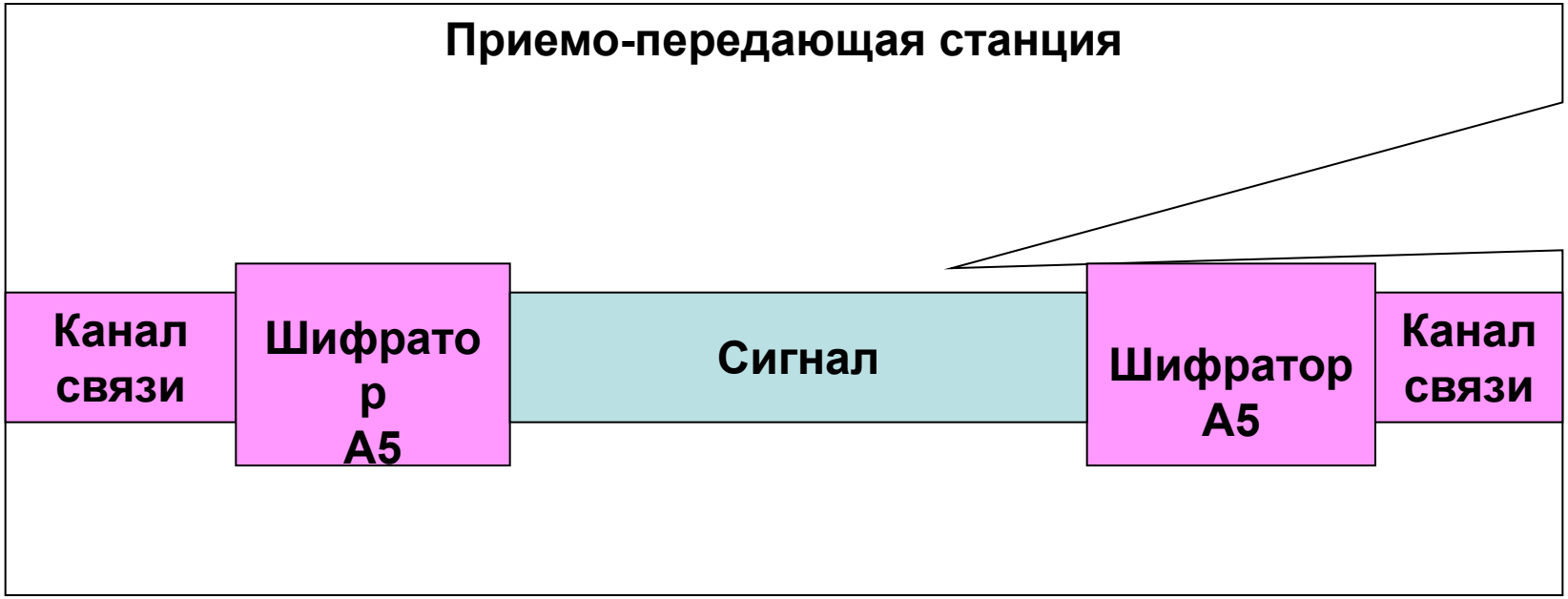
в) Цифровой сигнал (кодированный или шифрованный)

Защита ТС

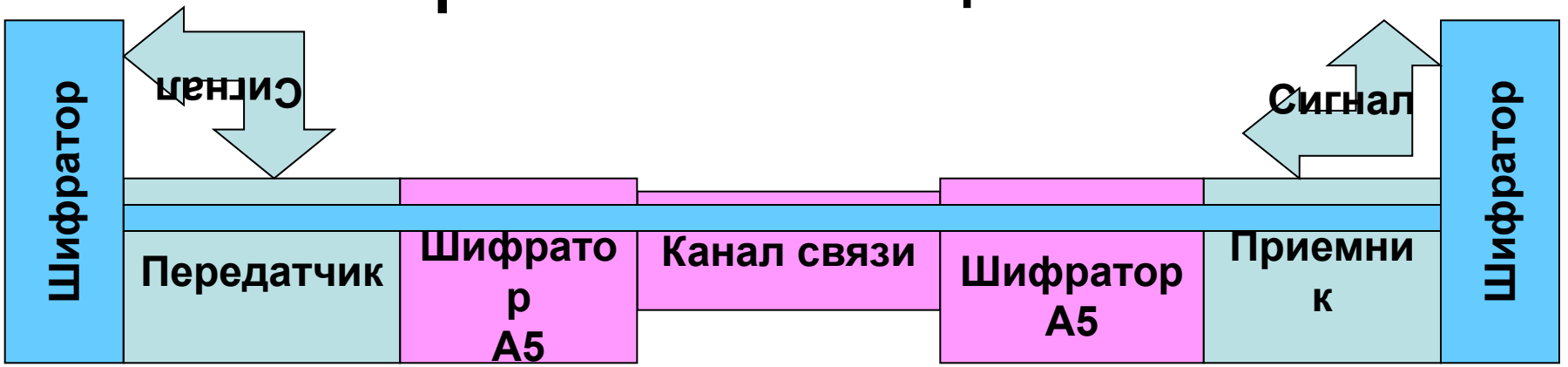

Сигнал
Вокодер
Шифратор
Сигнал
Телефон
Модем
Канал связи
Сигнал
Телефон
Модем
Сигнал
Вокодер
Шифратор

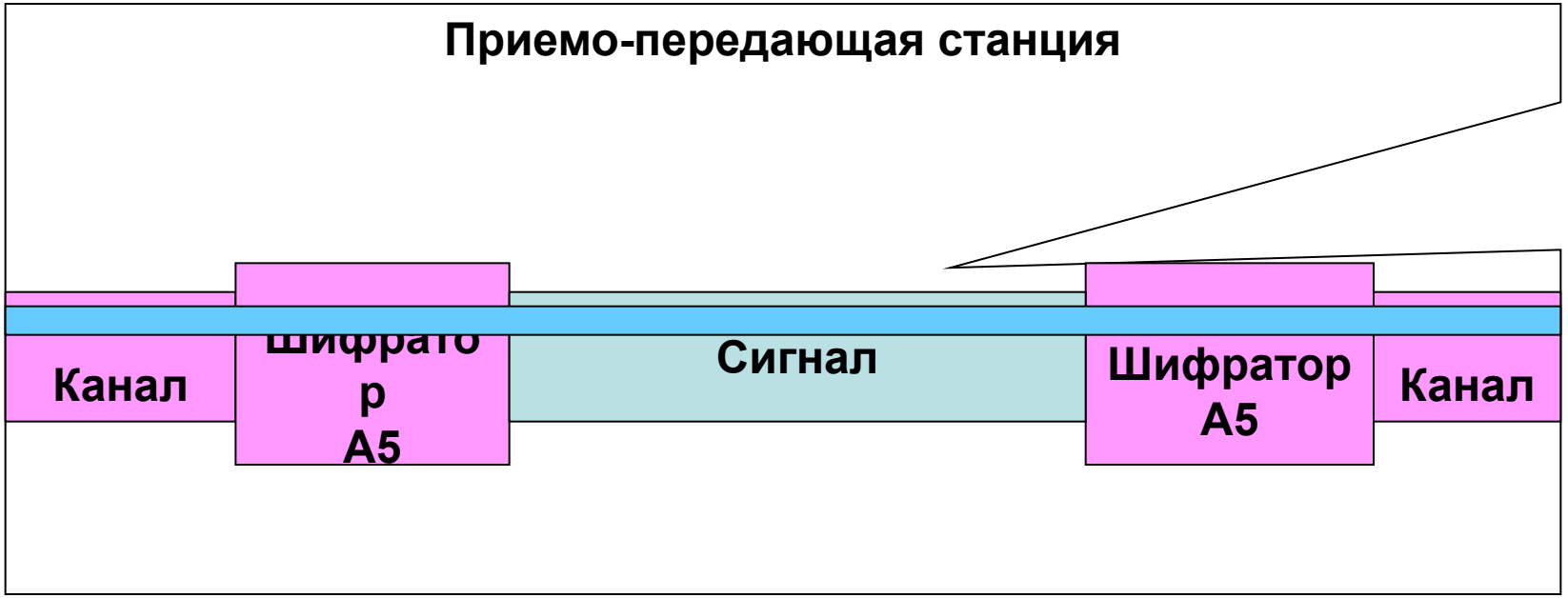
Встроенное шифрование GSM





Аппаратная защита GSM

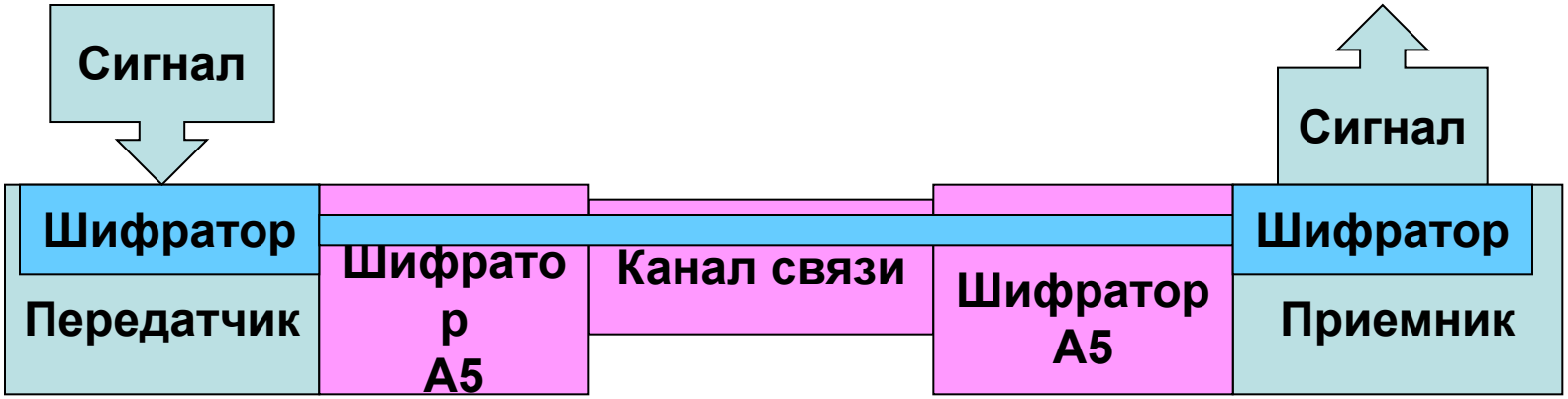


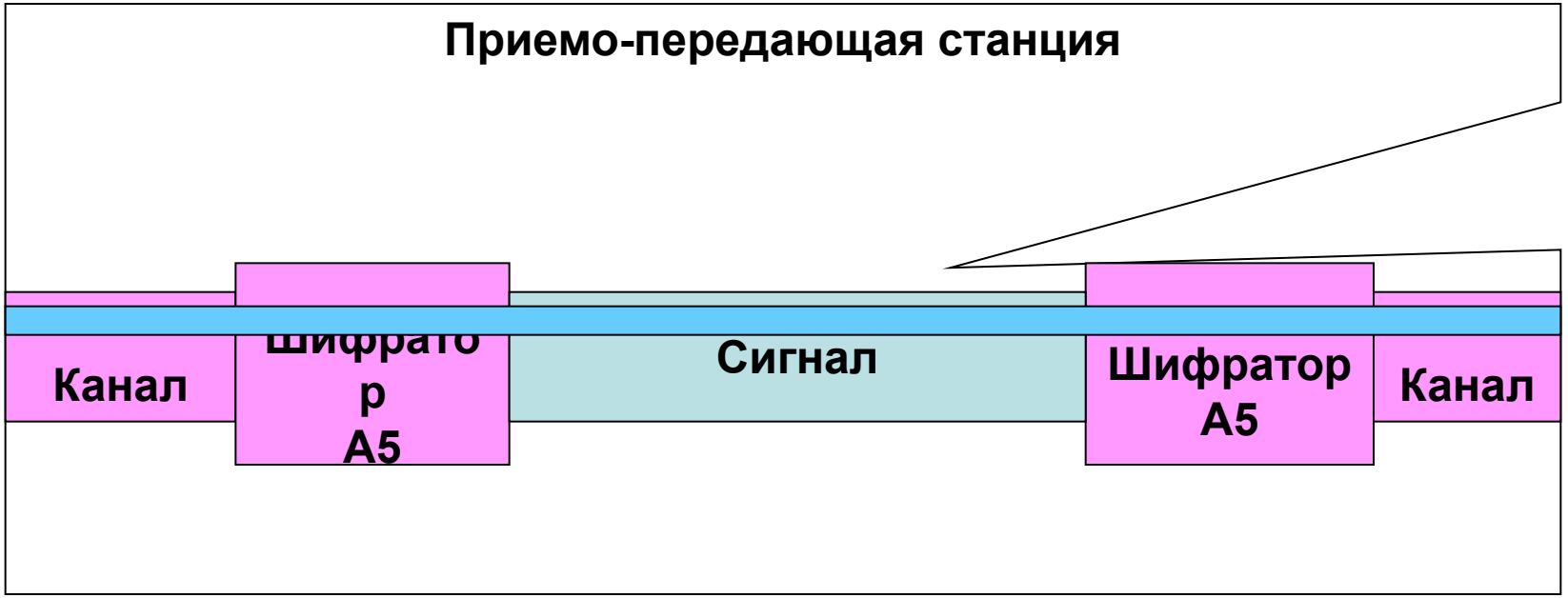


Мобильное устройство

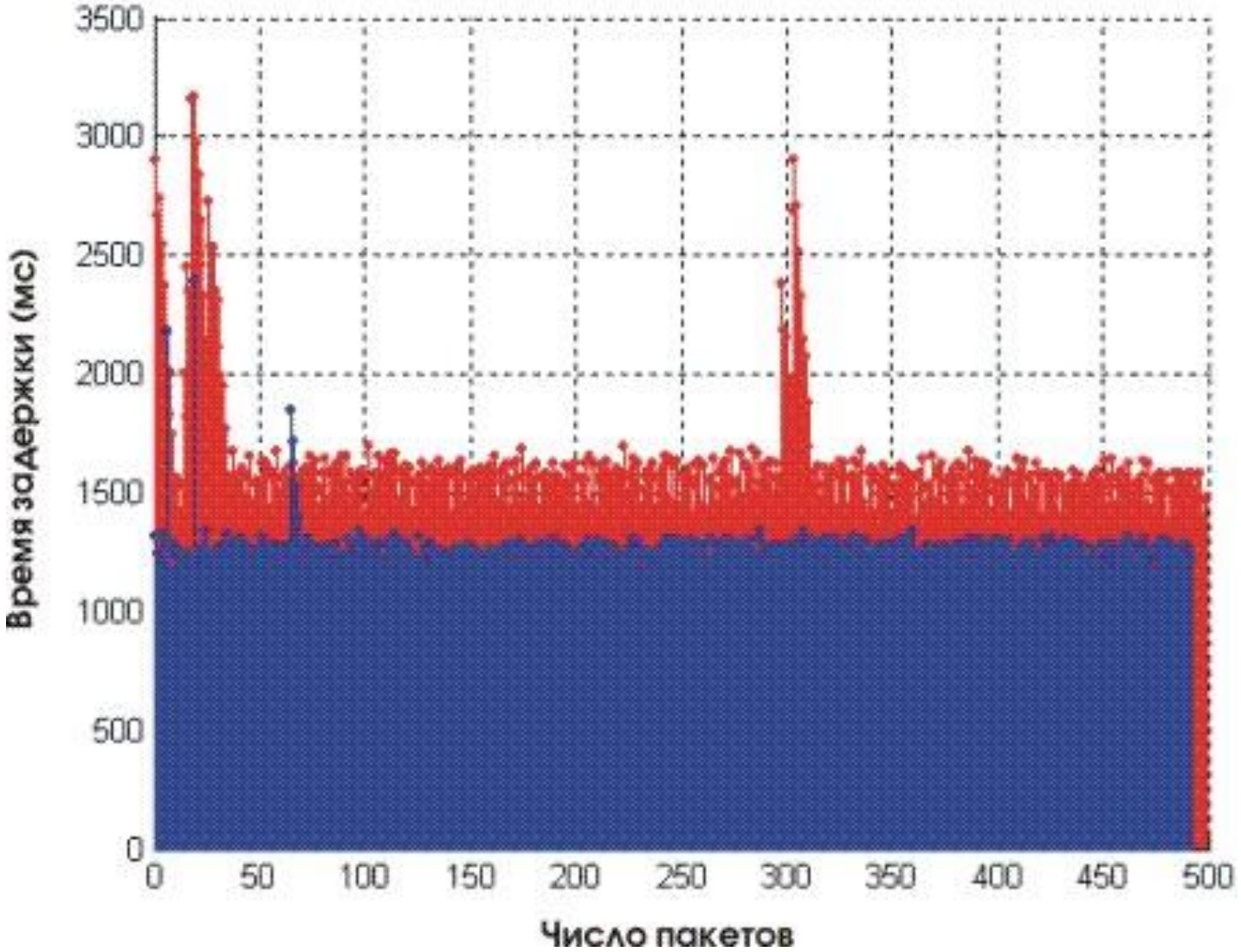
Программная реализация шифратора возможна только на iPhone и Pocket PC

Программная защита GSM

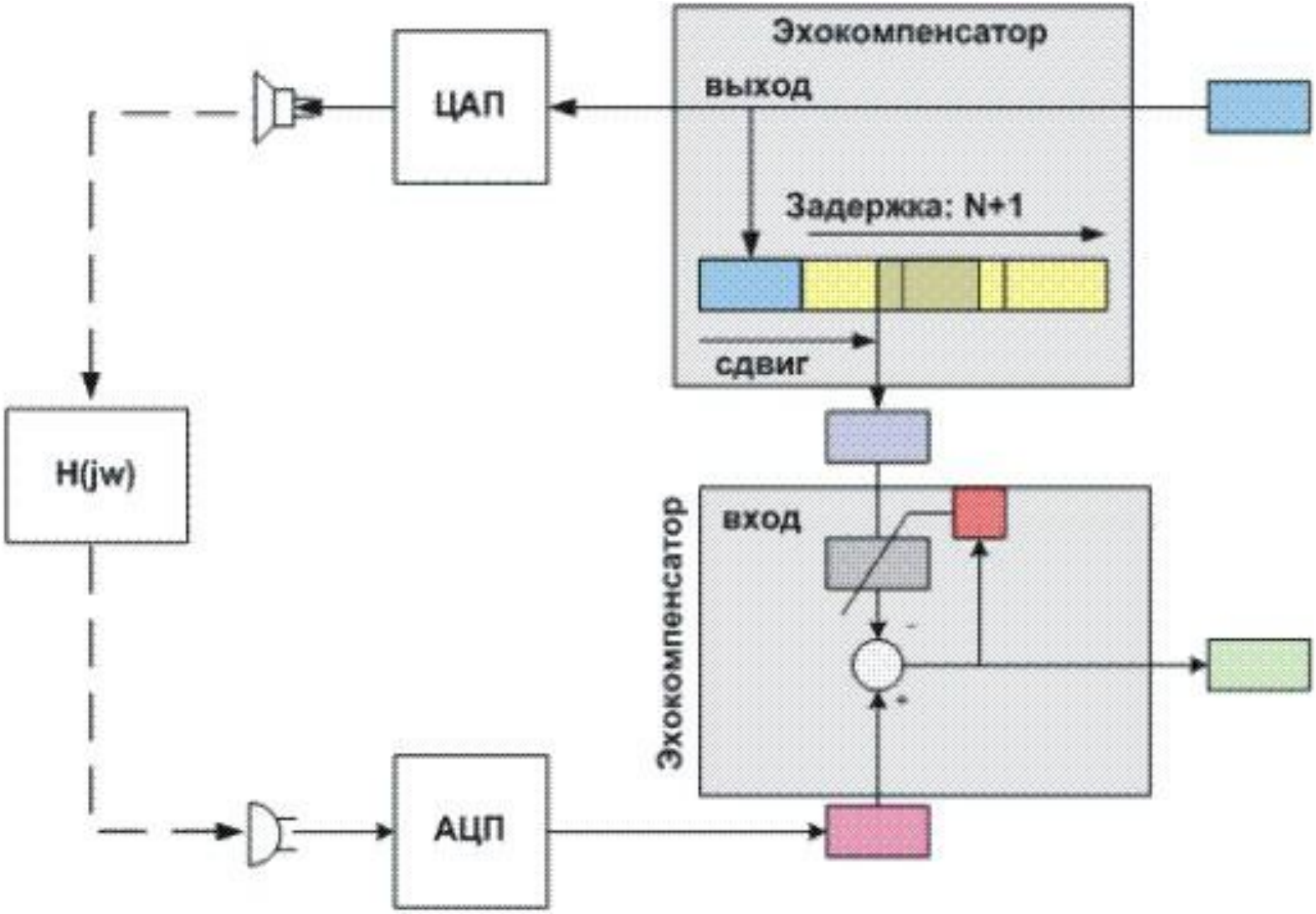




Задержки в канале связи



Эхокомпенсация



КОАП РФ

Статья 13.12. Нарушение правил защиты информации

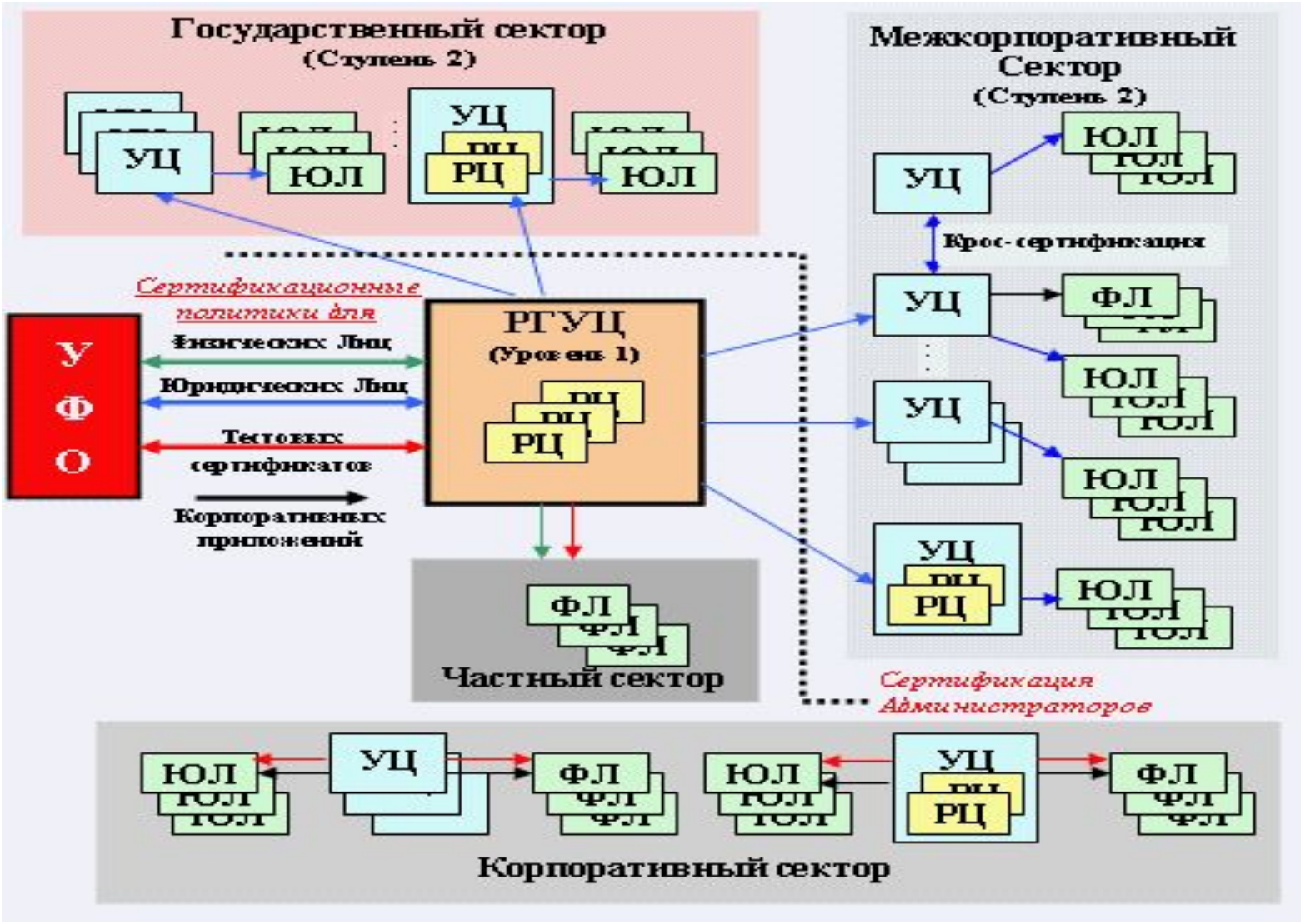
2. Использование несертифицированных информационных систем, баз и банков данных, а также несертифицированных средств защиты информации, если они подлежат обязательной сертификации (за исключением средств защиты информации, составляющей государственную тайну), - влечет наложение административного штрафа на граждан в размере от пятисот до одной тысячи рублей с конфискацией несертифицированных средств защиты информации или без таковой; на должностных лиц - от одной тысячи до двух тысяч рублей;
на юридических лиц - от десяти тысяч до двадцати тысяч рублей с конфискацией несертифицированных средств защиты информации или без таковой.
(в ред. Федерального закона от 22.06.2007 N 116-ФЗ)

КОАП РФ

Статья 13.13. Незаконная деятельность в области защиты информации

1. **Занятие видами деятельности в области защиты информации (за исключением информации, составляющей государственную тайну) без получения в установленном порядке специального разрешения (лицензии), если такое разрешение (такая лицензия) в соответствии с федеральным законом обязательно (обязательна), - влечет наложение административного штрафа на граждан в размере от пятисот до одной тысячи рублей с конфискацией средств защиты информации или без таковой; на должностных лиц - от двух тысяч до трех тысяч рублей с конфискацией средств защиты информации или без таковой; на юридических лиц - от десяти тысяч до двадцати тысяч рублей с конфискацией средств защиты информации или без таковой. (в ред. Федерального закона от 22.06.2007 N 116-ФЗ)**

Инфраструктура УЦ



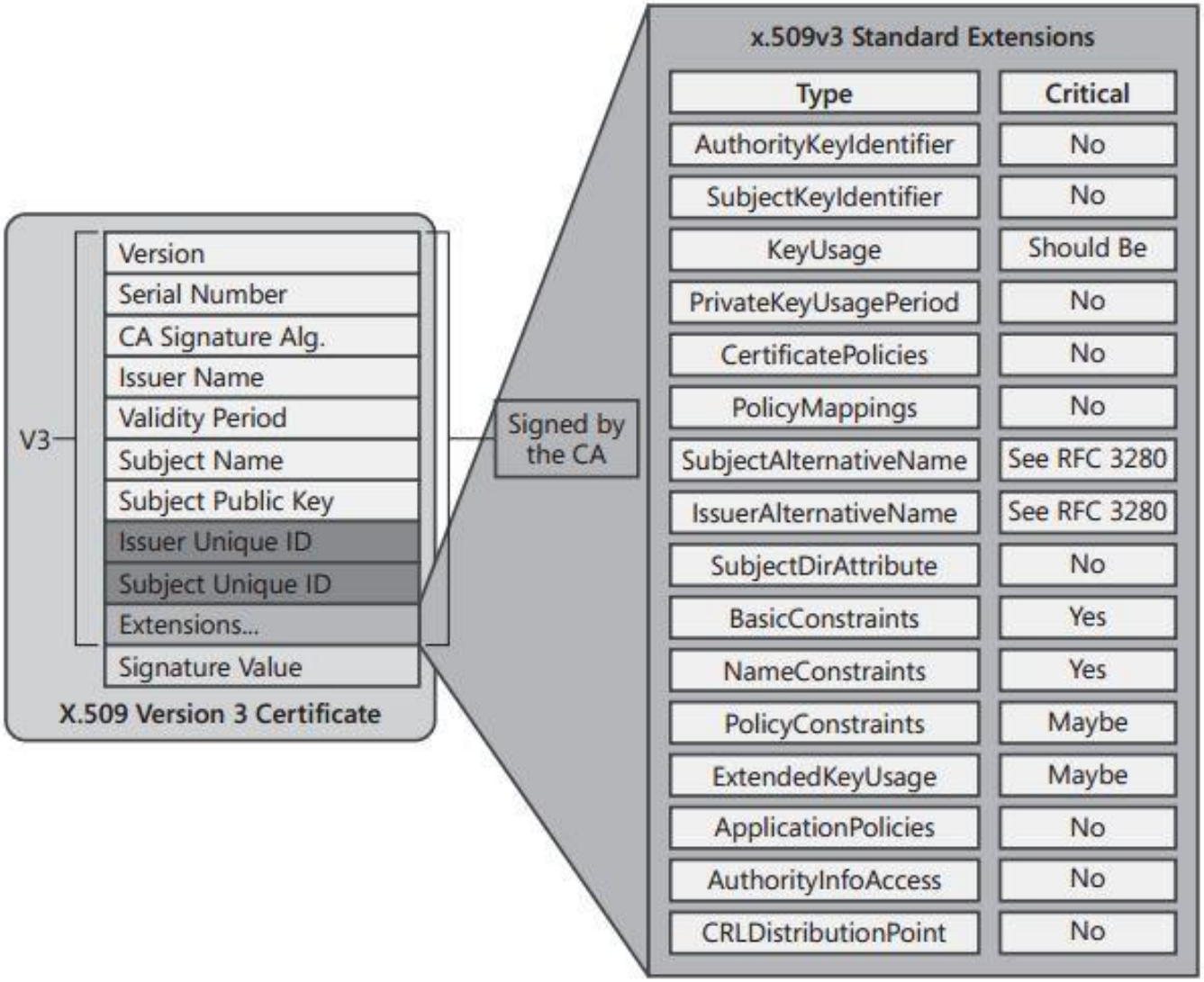
Состав УЦ

- Certification Authority (CA)
  - Политики выдачи сертификатов
  - Хранилище сертификатов
- Registration Authority (RA)
- Список отозванных сертификатов (CRL)
  - Протокол проверки легитимности сертификата
- Структура доверия Центров сертификации
  - Иерархия Центров сертификации
  - Кросс-сертификация

Сертификат x.509 v3

- Типовая архитектура PKI и структура сертификатов (X.509 v.3, CRL v.2) определена в международных стандартах ITU-T X.509 (ISO/IEC/ITU 9594-8) и RFC 2459
- Сертификат X.509 v3 состоит из трех частей
  - «Тело» сертификата – формат, версия и серийный номер сертификата, атрибуты владельца (subject) и издателя (issuer) сертификата, значение открытого ключа, расширения сертификата
  - Алгоритм ЭЦП, на котором произведена подпись удостоверяющего центра (certificate authority, CA)
  - ЭЦП удостоверяющего центра (значение)

Сертификат x.509 v3



Наименование организации-Удостоверяющего Центра

Бланк сертификата открытого ключа

Сведения о сертификате:

Этот сертификат:

Подтверждает удаленному компьютеру идентификацию вашего компьютера

Обеспечивает идентификацию пользователя на центре регистрации

Кому выдан:

Иванов Иван Иванович

Кем выдан:

Test Root CA on SP2

Действителен с 10 ноября 2002 г. 12:52:00 UTC по 17 ноября 2002 г. 13:01:05 UTC

Версия: 3 (0x2)

Серийный номер: 1133 C166 0000 0000 00AF

Алгоритм подписи:

Название: ГОСТ Р 34.11/34.10-94

Идентификатор: 1.2.643.2.2.4

Параметры: 0500

Издатель сертификата: CN = Test Root CA on SP2, OU = Soft Dev, O = Crypto Pro, L = Moscow, S = Moscow, C = RU

Срок действия:

Действителен с: 10 ноября 2002 г. 12:52:00 UTC

Действителен по: 17 ноября 2002 г. 13:01:05 UTC

Владелец сертификата: CN = Иванов Иван Иванович, O = ООО 'Пупкин и сыновья', L = Москва, C = RU, E = alexl@cp.ru

Открытый ключ:

Алгоритм открытого ключа:

Название: ГОСТ Р 34.10-94

Идентификатор: 1.2.643.2.2.20

Параметры: 3012 0607 2A85 0302 0220 0206 072A 8503 0202 1E01

Значение: 0481 808F 18D0 F69C D097 D36C 62E1 8787 C357 0248 7BF0 A917 C757 2F52 A296 6C77 3E4D 3F3C 9860 23A3 F8F7 2CEB B786 1DC0 FBFC DCBA 8234 6133 C72C 4B38 1D5B 455F 2C60 5962 9926 7065 88BF C3C4 2AFE 20BA 2038 3CA4 02CD 980D 9BF5 3DD4 BA4B F208 B726 8D29 EE0E 1D61 BC8A BFF8 B202 9D5D 0CF3 4AAD 56D3 C43F 06B9 33DE C083 53B9 AA1B 92

Расширения сертификата X.509

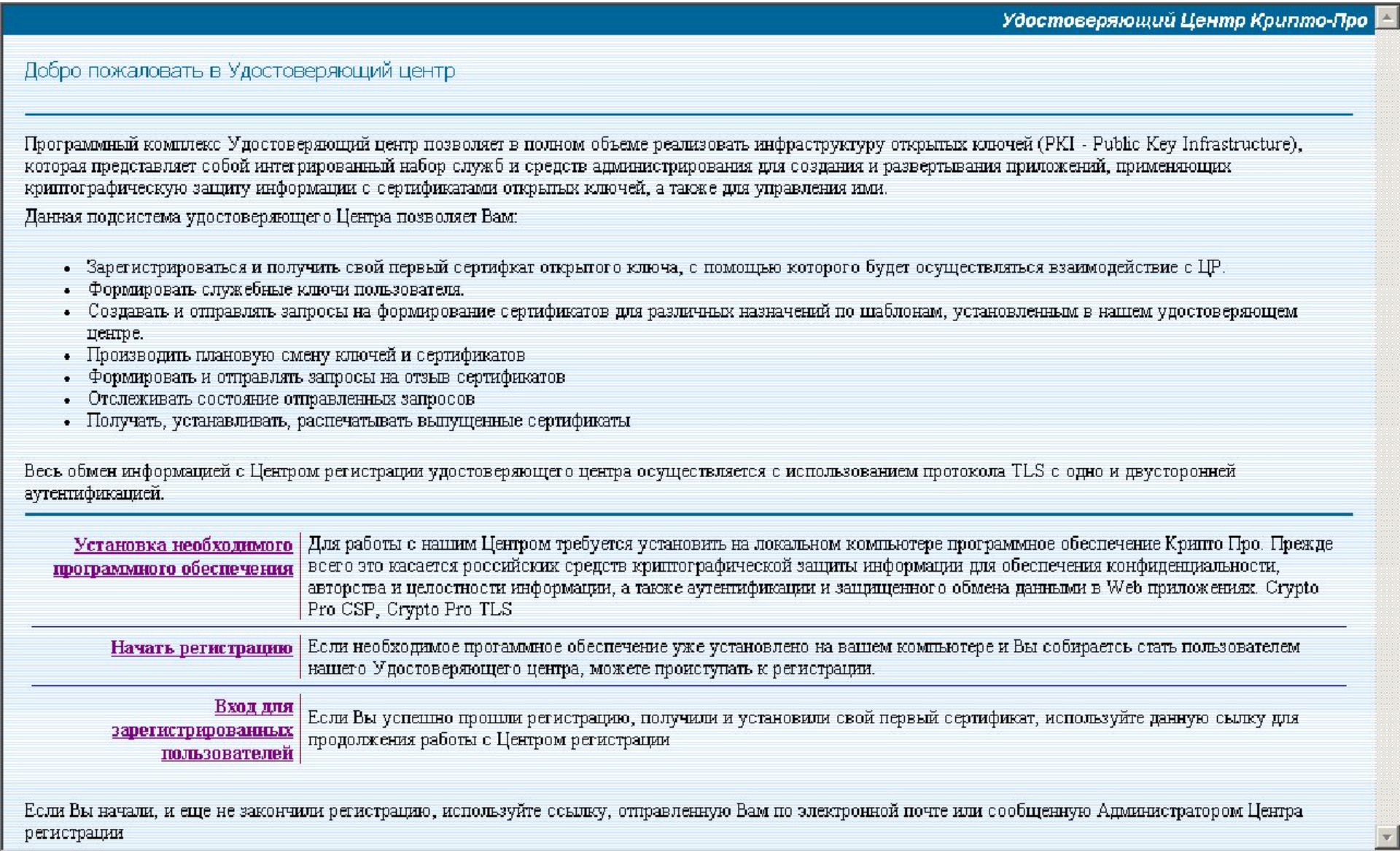
1. Расширение 2.5.29.15 (критическое)
   Название: Использование ключа
   Значение: Цифровая подпись , Неотрекаемость , Шифрование ключей , Шифрование данных(F0)
2. Расширение 2.5.29.37
   Название: Улучшенный ключ
   Значение: Временный доступ к Центру Регистрации(1.2.643.2.2.34.2) Пользователь Центра Регистрации(1.2.643.2.2.34.6) Проверка подлинности клиента(1.3.6.1.5.5.7.3.2)
3. Расширение 2.5.29.14
   Название: Идентификатор ключа субъекта
   Значение: 899F 97DB 23FE 32D3 A804 0D5C D615 D5F8 95D1 FE43
4. Расширение 2.5.29.35
   Название: Идентификатор ключа центра сертификатов
   Значение: Идентификатор ключа=903B 0B6E 7FD9 1DC8 4B3B 28C3 57C6 5CAC 975D 3905 Поставщик сертификата: Адрес каталога: CN=Test Root CA on SP2 OU=Soft Dev O=Crypto Pro L=Moscow S=Moscow C=RU Серийный номер сертификата=155A 765E B4AE CE86 4EAD 1CEC 7B07 DA79

Подпись Удостоверяющего центра:

Алгоритм подписи:

Название: ГОСТ Р 34.11/34.10-94

Интерфейс центра регистрации



Удостоверяющий Центр Крипто-Про

Добро пожаловать в Удостоверяющий центр

Программный комплекс Удостоверяющий центр позволяет в полном объеме реализовать инфраструктуру открытых ключей (PKI - Public Key Infrastructure), которая представляет собой интегрированный набор служб и средств администрирования для создания и развертывания приложений, применяющих криптографическую защиту информации с сертификатами открытых ключей, а также для управления ими.

Данная подсистема удостоверяющего Центра позволяет Вам:

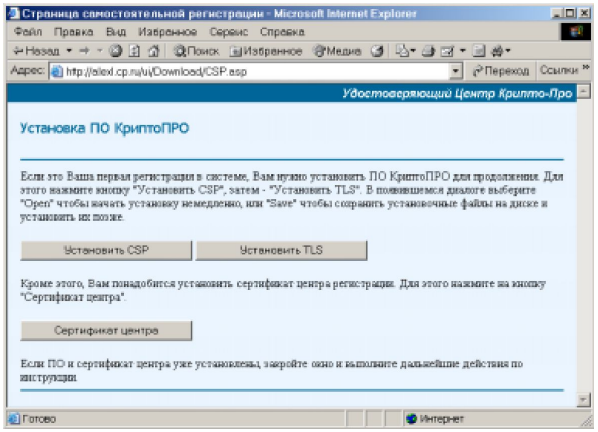
- Зарегистрироваться и получить свой первый сертифкат открытого ключа, с помощью которого будет осуществляться взаимодействие с ЦР.
- Формировать служебные ключи пользователя.
- Создавать и отправлять запросы на формирование сертификатов для различных назначений по шаблонам, установленным в нашем удостоверяющем центре.
- Производить плановую смену ключей и сертификатов
- Формировать и отправлять запросы на отзыв сертификатов
- Отслеживать состояние отправленных запросов
- Получать, устанавливать, распечатывать выпущенные сертификаты

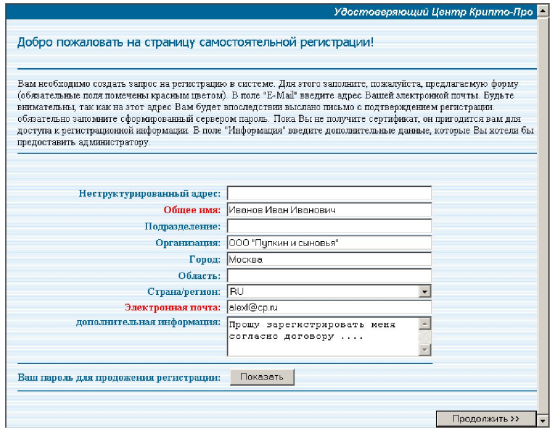
Весь обмен информацией с Центром регистрации удостоверяющего центра осуществляется с использованием протокола TLS с одно и двусторонней аутентификацией.

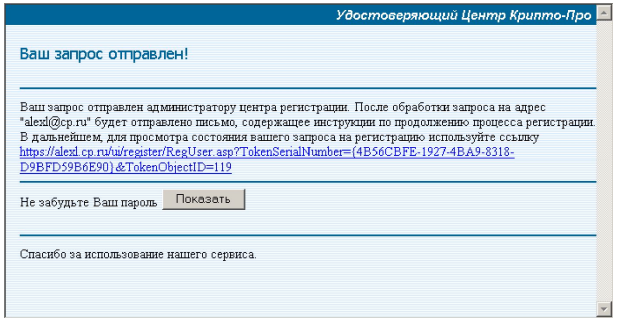
Установка необходимого программного обеспечения	Для работы с нашим Центром требуется установить на локальном компьютере программное обеспечение Крипто Про. Прежде всего это касается российских средств криптографической защиты информации для обеспечения конфиденциальности, авторства и целостности информации, а также аутентификации и защищенного обмена данными в Web приложениях. Crypto Pro CSP, Crypto Pro TLS
Начать регистрацию	Если необходимое прогаммное обеспечение уже установлено на вашем компьютере и Вы собираетесь стать пользователем нашего Удостоверяющего центра, можете проиступать к регистрации.
Вход для зарегистрированных пользователей	Если Вы успешно прошли регистрацию, получили и установили свой первый сертификат, используйте данную ссылку для продолжения работы с Центром регистрации

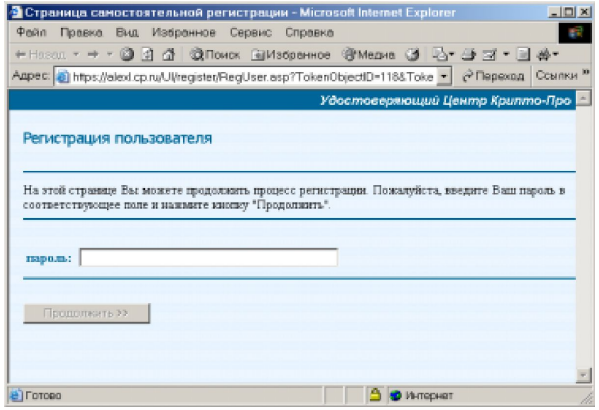
Если Вы начали, и еще не закончили регистрацию, используйте ссылку, отправленную Вам по электронной почте или сообщенную Администратором Центра регистрации

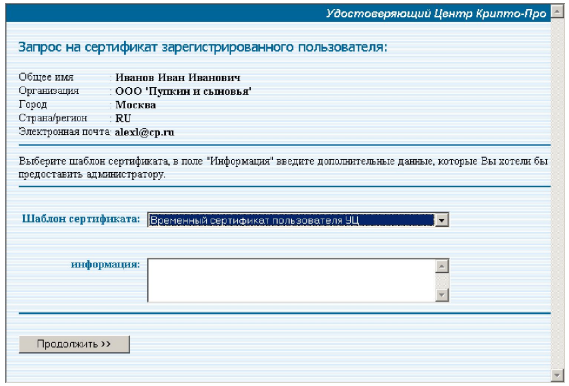
Интерфейс центра регистрации

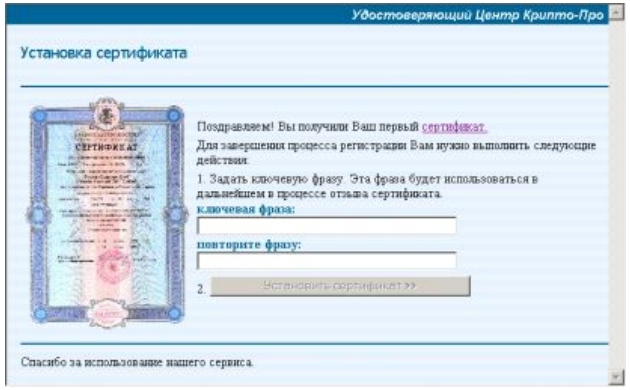




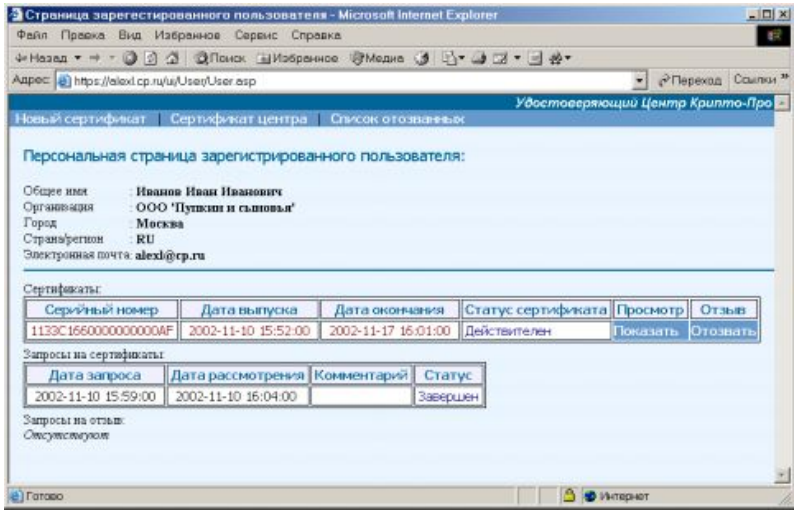


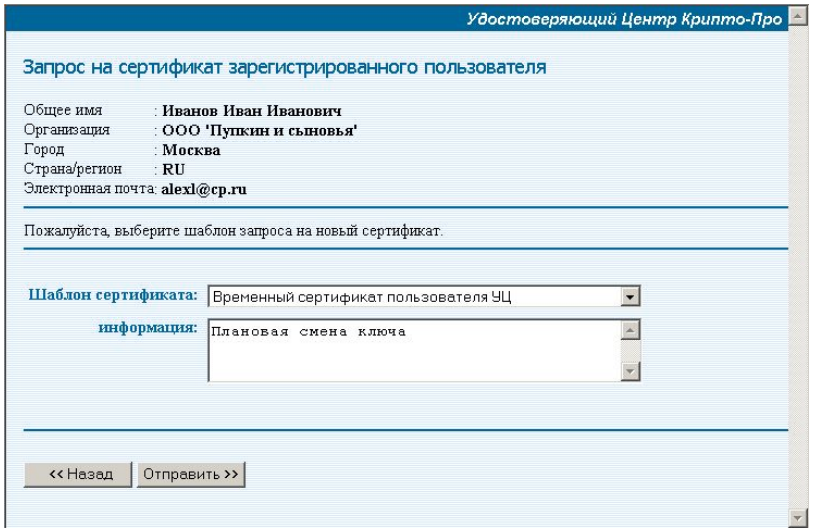


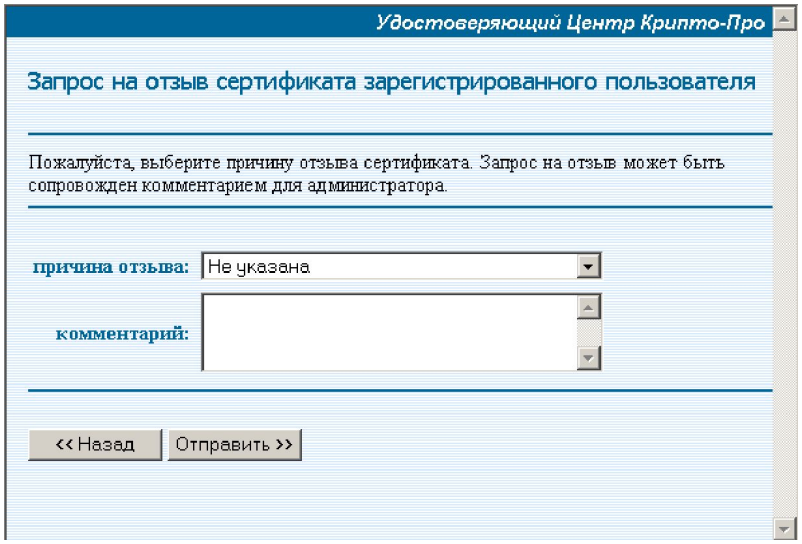


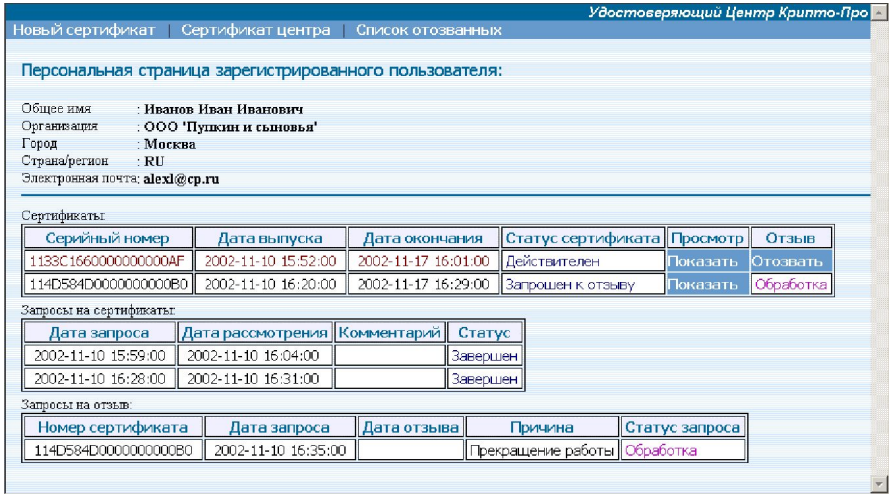


Интерфейс центра регистрации









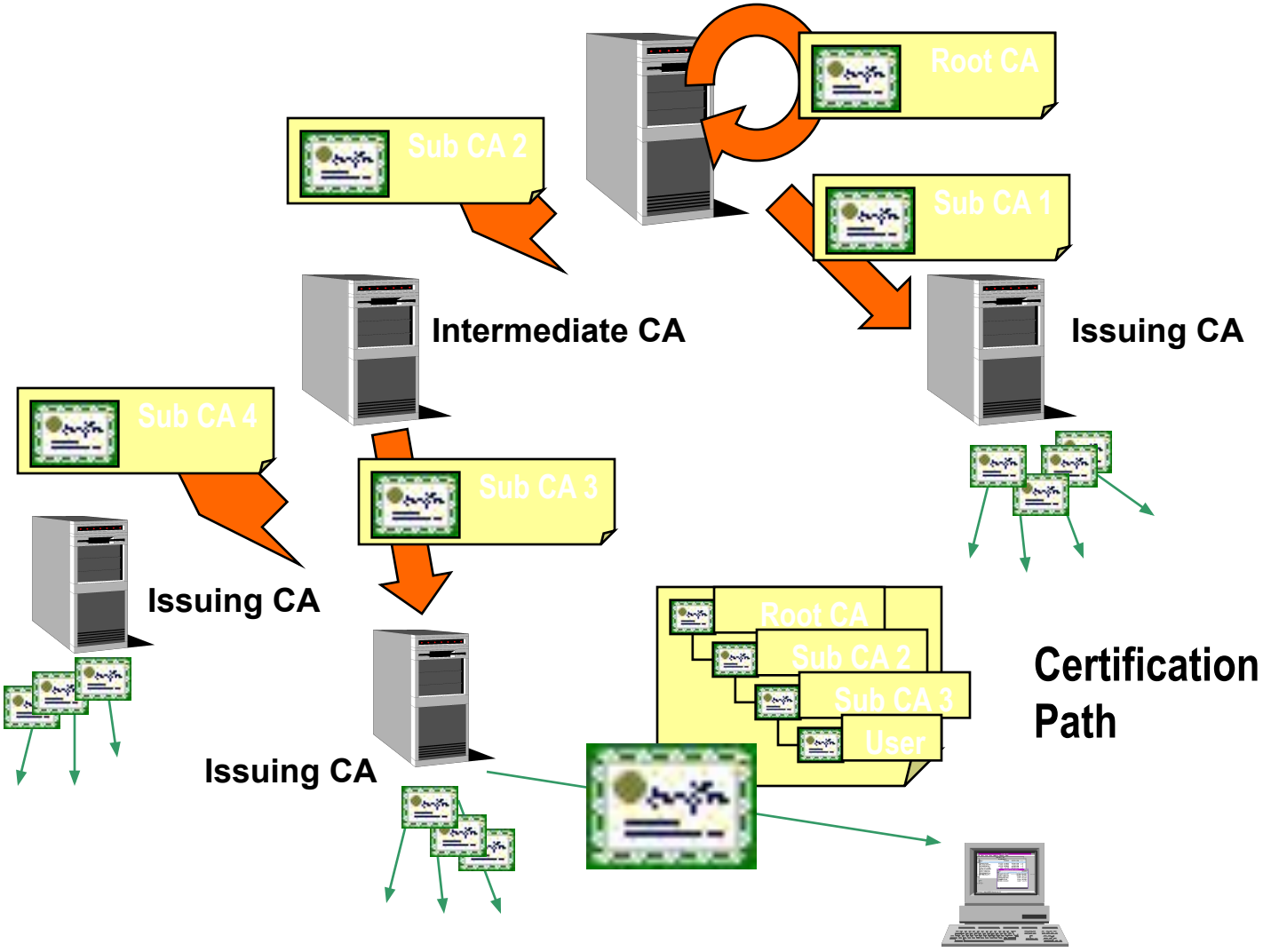
Список отозванных сертификатов

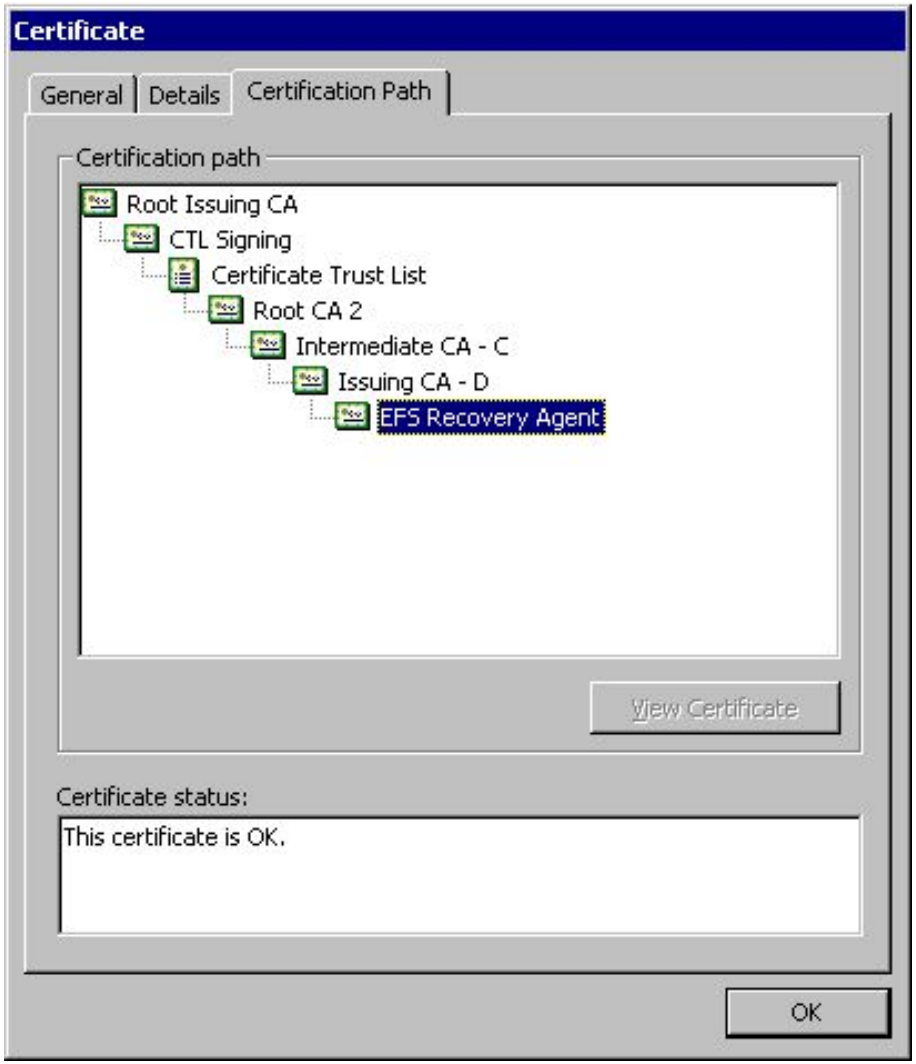
- Certificate Revocation List
  - Список отозванных сертификатов
  - Подписан Центром сертификации
  - Должен публиковаться и регулярно обновляться каждым CA
    - Active Directory
    - Web
    - Файловая система
- Сертификат содержит список узлов публикации CRL

Иерархия УЦ

- Роли CA
  - Root CA
    - Корневой центр сертификации
    - Сертифицирует нижестоящие CA
  - Subordinate CA
    - Intermediate CA
      - Сертифицирует CA следующего уровня
    - Issuing CA
      - Выдает сертификаты пользователям
- Certification Path
  - Указывается в сертификате

Иерархия УЦ


Root CA
Sub CA 2
Sub CA 1
Intermediate CA
Issuing CA
Sub CA 4
Sub CA 3
Issuing CA
Issuing CA
Root CA
Sub CA 2
Sub CA 3
User
Certification Path



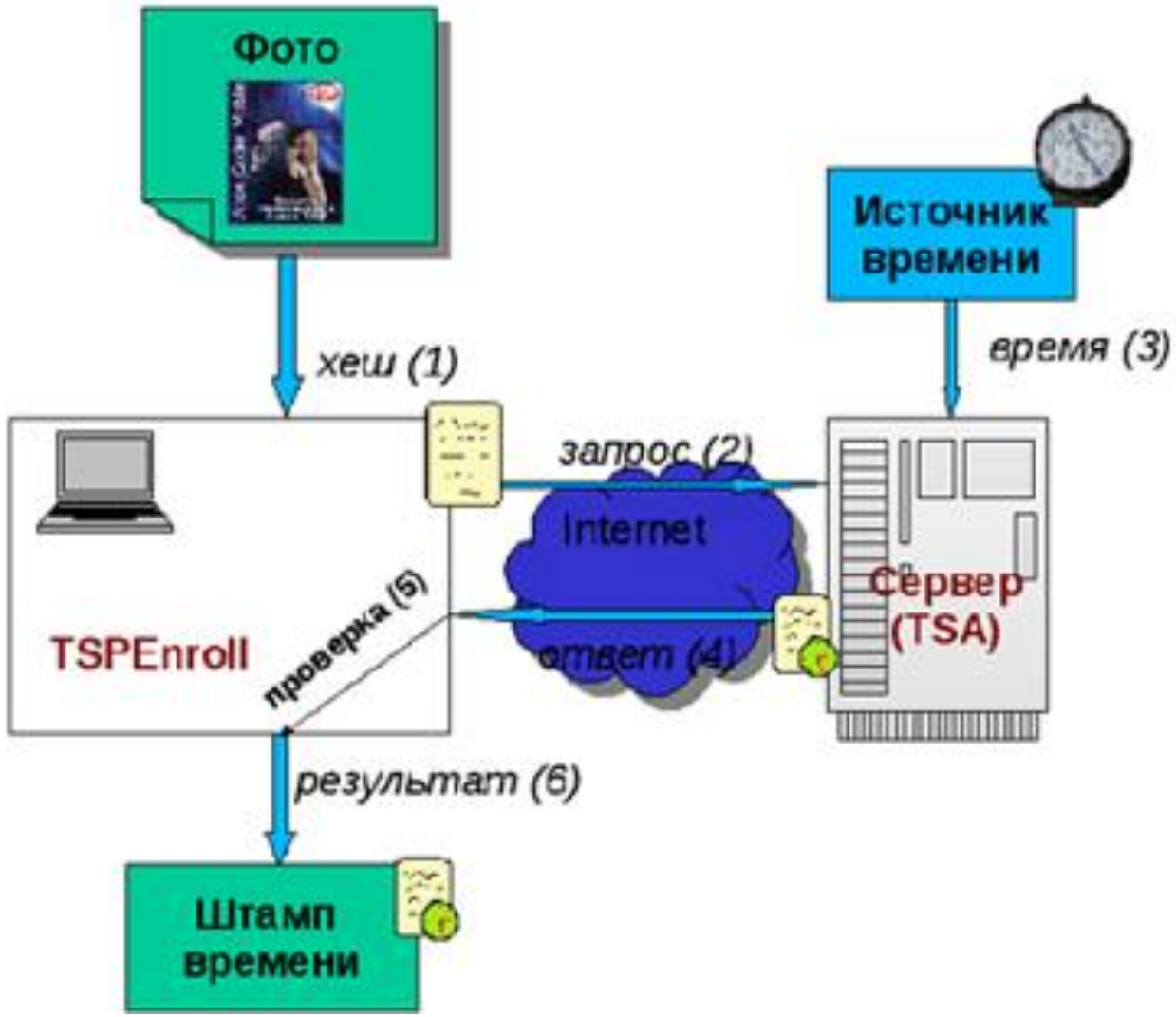
- Список доверия
  - Аналог механизма кросс-сертификации
    - Список доверяемых корневых центров
  - Ограничения по режимам сертификата
  - Назначается в групповой политике

ПАК «КриптоПро УЦ» 1.5 КС2 - Стандартная конфигурация		
174	Лицензия на право использования ПАК "Удостоверяющий центр "КриптоПро УЦ" версии 1.5 класс КС2 до 100 польз. с/к При приобретении лицензии на право использования ПАК «Удостоверяющий центр «КриптоПро УЦ» версии 1.5 КС2 Лицензиату предоставляется ПАК «Удостоверяющий центр «КриптоПро УЦ» версии 1.5 в базовой комплектации, включающей в себя: 1. Дистрибутив ПАК "Удостоверяющий Центр "КриптоПро УЦ" версии 1.5 на CD (включает комплект эксплуатационной документации) - 1 экз. 2. Формуляр ПАК "Удостоверяющий Центр "КриптоПро УЦ" версии 1.5 - 1 экз. 3. Лицензия на "Центр сертификации" - 1 экз. 4. Лицензия на "Центр регистрации" - 1 экз. 5. Лицензия на "АРМ администратора ЦР" - 1 экз. 6. Лицензия на "АРМ разбора конфликтных ситуаций" - 1 экз. 7. Копия сертификата соответствия ПАК "Удостоверяющий Центр "КриптоПро УЦ" версии 1.5 КС2 - 1 экз. 8. Дистрибутив СКЗИ "КриптоПро CSP" версии 3.6 на CD (включает комплект эксплуатационной документации) - 1 экз. 9. Формуляр СКЗИ "КриптоПро CSP" версии 3.6 - 1 экз. 10. Лицензия на СКЗИ "КриптоПро CSP" версии 3.6 на одно рабочее место - 1 экз. 11. Лицензия на СКЗИ "КриптоПро CSP" версии 3.6 на один сервер (включая право использования КриптоПро TLS) – 2 экз. 12. Копия сертификата соответствия СКЗИ "КриптоПро CSP" версии 3.6 - 1 экз.	90 000

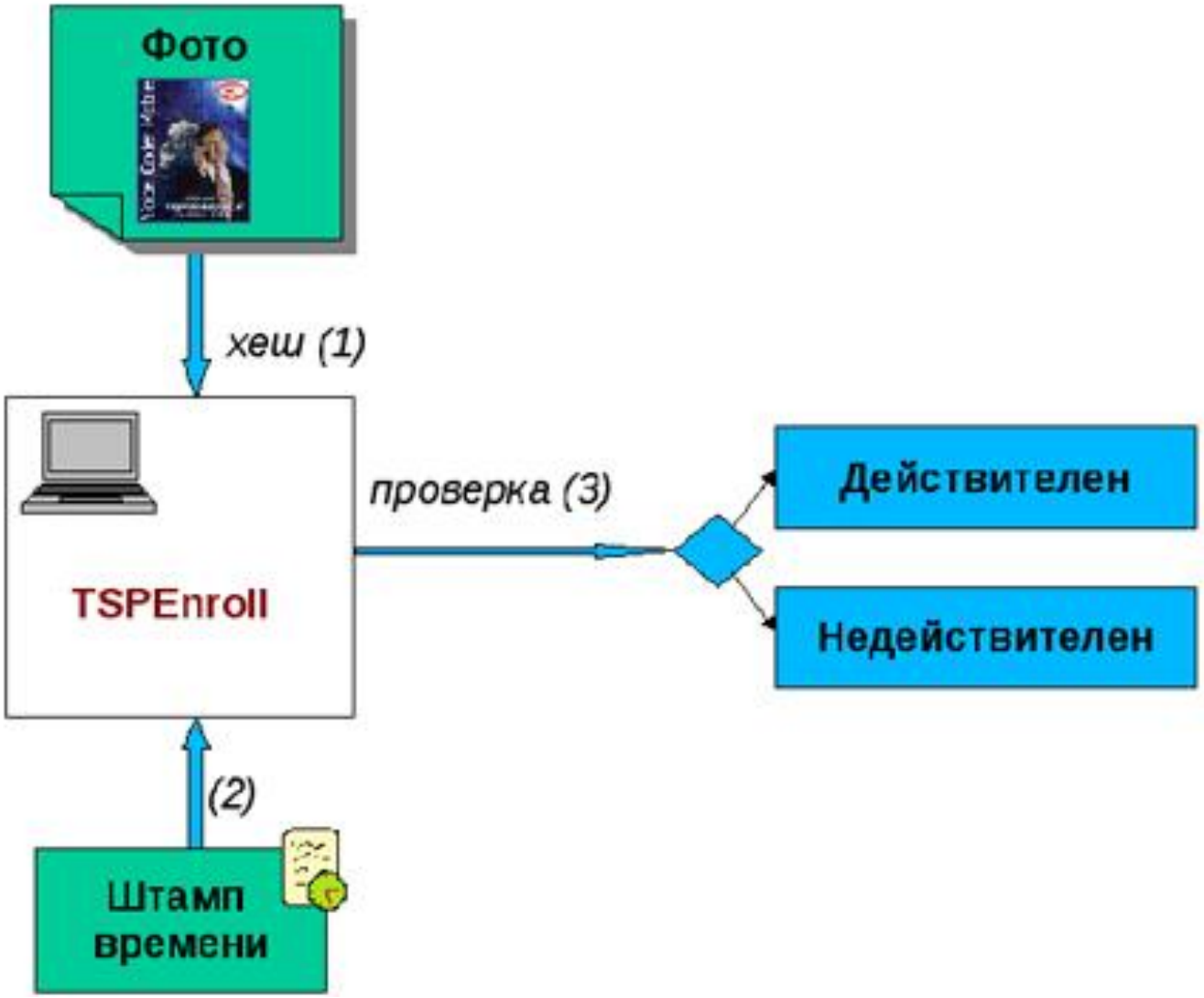
Состав АРМ клиента

- Криптопровайдер (CSP)
- **Утилита генерации ключей**
- Ключевой носитель + Драйвера
- Компонент формирования ЭЦП
- Клиентское приложение (Редактор, браузер и т.п.)
- Библиотеки среды разработки для ОС

Формирование штампа времени



Проверка штампа времени



Основные способы хранения ключевой информации

- На логическом диске ПК
- В памяти человека
- Использование портативных хранилищ
- Использование идентификаторов безопасности
- Безопасный пользовательский интерфейс
- Биометрические параметры
- Системы однократной регистрации
- Разделение секрета

Идентификаторы безопасности

- Touch-memory (таблетка)
- USB-token
- Смарт-карта

Touch-memory

Контактная память (от англ. touch memory иногда встречается англ. contact memory или англ. iButton) — класс электронных устройств, имеющих двухпроходный протокол обмена информацией с ними (1-Wire), и помещённых в стандартный металлический корпус (обычно имеющий вид «таблетки»).

Смарт-карта

Смарт-карты (англ. Smart card) представляют собой пластиковые карты со встроенной микросхемой (ICC, integrated circuit(s) card — карта с интегрированными электронными схемами).

В большинстве случаев смарт-карты содержат микропроцессор и операционную систему, контролирующую устройство и доступ к объектам в его памяти. Кроме того, смарт-карты, как правило, обладают возможностью проводить криптографические вычисления.

USB-token

USB-token - это аналог смарт-карты, но для работы с ним не требуется дополнительное оборудование (считыватель), данные надежно хранятся в энергонезависимой памяти токена, прочный корпус E-token более устойчив к внешним воздействиям.

Комплекс средств аутентификации

Аппаратный компонент		**Программный компонент**
Устройство + считыватель		Драйвера устройств +
Двухфакторная аутентификация		**Поддерживающая инфраструктура**
Наличие устройства	Знание PIN-кода	Центр сертификации ЭЦП

Криптографические функциональные составляющие идентификатора

- Симметричный алгоритм шифрования
- Генератор псевдослучайной последовательности
- Функция хэширования
- Алгоритм асимметричной цифровой подписи
- Алгоритм асимметричного шифрования

Виды идентификаторов по назначению

- E-token (замена парольной защиты, симметричное шифрование, ПСП, хэш)
- Token-DS (+ алгоритм ЭЦП)
- Token-flash (+ хранилище неключевых данных)
- Token-RFID (+ радиочастотная метка)