

A background image of a businessman in a suit holding a large, transparent, 3D gear. Several other similar gears are floating in the air around him, creating a sense of motion and complexity. The image is overlaid with a semi-transparent white rectangle in the bottom left corner.

СКЗИ

Средства защиты

СРЕДСТВА ЗАЩИТЫ ИНФОРМАЦИИ

Физические средства защиты

Регламентные средства
защиты

Технические средства защиты

Криптографические средства
защиты

Средства анализа
и фильтрации
трафика

Средства
разграничения
доступа

Средства контроля
съемных
машинных
носителей

Средства
доверенной
загрузки

Средства
антивирусной
защиты

:

VPN

PKI

...

The background image shows a black smartphone lying on a black laptop keyboard. A large, brass-colored metal padlock is attached to the phone's charging port. A set of keys, including a car key and a house key, is attached to the padlock's shackle. The scene is lit with soft, natural light, creating subtle reflections on the phone's screen and the keyboard keys.

НПА, определения

НПА

1. Приказ ФАПСИ 152 (Инструкция)
 2. ПКЗ-2005 (Приказ ФСБ № 66)
 3. ПП 313
 4. Открытые требования (ТК26)
- <https://tc26.ru/standarts>

Приказ ФАПСИ от 13 июня 2001 г. N 152
"Об утверждении Инструкции и требований к обработке информации в целях обеспечения безопасности государственной информации"

В соответствии с Федеральным законом от 20 февраля 1993 г. N 34-ФЗ "Об информации, информационных технологиях и о защите информации" (далее - Закон) и постановлением Правительства Российской Федерации от 21 апреля 2001 г. N 268 "О мерах по реализации постановления Правительства Российской Федерации от 19.05.2000 N 207" (далее - Постановление), постановлением Правительства Российской Федерации от 19.05.2000 N 207 (далее - Постановление) и постановлением Правительства Российской Федерации от 19.05.2000 N 207 (далее - Постановление) утвердить прилагаемую Инструкцию и требования к обработке информации в целях обеспечения безопасности государственной информации.

Утвердить прилагаемую Инструкцию и требования к обработке информации в целях обеспечения безопасности государственной информации.

Генеральный директор Агентства И.Маслов

Согласно постановлению Правительства Российской Федерации от 19.05.2000 N 207
Правительство Российской Федерации от 19.05.2000 N 207

Принято в соответствии с постановлением Правительства Российской Федерации от 19.05.2000 N 207

Инструкция
об организации и обеспечении безопасности обработки информации в целях обеспечения безопасности государственной информации

1. Настоящая Инструкция определяет порядок и организацию обработки информации в целях обеспечения безопасности государственной информации.

2. Настоящая Инструкция определяет порядок и организацию обработки информации в целях обеспечения безопасности государственной информации.

3. Настоящая Инструкция определяет порядок и организацию обработки информации в целях обеспечения безопасности государственной информации.

4. Настоящая Инструкция определяет порядок и организацию обработки информации в целях обеспечения безопасности государственной информации.

5. Настоящая Инструкция определяет порядок и организацию обработки информации в целях обеспечения безопасности государственной информации.

6. Настоящая Инструкция определяет порядок и организацию обработки информации в целях обеспечения безопасности государственной информации.

7. Настоящая Инструкция определяет порядок и организацию обработки информации в целях обеспечения безопасности государственной информации.

8. Настоящая Инструкция определяет порядок и организацию обработки информации в целях обеспечения безопасности государственной информации.

9. Настоящая Инструкция определяет порядок и организацию обработки информации в целях обеспечения безопасности государственной информации.

10. Настоящая Инструкция определяет порядок и организацию обработки информации в целях обеспечения безопасности государственной информации.

11. Настоящая Инструкция определяет порядок и организацию обработки информации в целях обеспечения безопасности государственной информации.

12. Настоящая Инструкция определяет порядок и организацию обработки информации в целях обеспечения безопасности государственной информации.

13. Настоящая Инструкция определяет порядок и организацию обработки информации в целях обеспечения безопасности государственной информации.

14. Настоящая Инструкция определяет порядок и организацию обработки информации в целях обеспечения безопасности государственной информации.

15. Настоящая Инструкция определяет порядок и организацию обработки информации в целях обеспечения безопасности государственной информации.

Определения

Криптографический ключ (криптоключ) — совокупность данных, обеспечивающая выбор одного конкретного криптографического преобразования из числа всех возможных в данной криптографической системе (определение из [Приказа ФАПСИ № 152 от 13 июня 2001 г.](#))

Определения

Ключевая информация — специальным образом организованная совокупность криптоключей, предназначенная для осуществления криптографической защиты информации в течение определенного срока .

Понять принципиальное отличие между криптоключем и ключевой информацией можно на следующем примере. При организации HTTPS, генерируются ключевая пара открытый и закрытый ключ, а из открытого ключа и дополнительной информации получается сертификат. Так вот, в данной схеме совокупность сертификата и закрытого ключа образуют ключевую информацию, а каждый из них по отдельности является криптоключом. Тут можно руководствоваться следующим простым правилом – конечные пользователи при работе с СКЗИ используют ключевую информацию, а криптоключи обычно используют СКЗИ внутри себя. В тоже время важно понимать, что ключевая информация может состоять из одного криптоключа.

Определения

Ключевые документы — электронные документы на любых носителях информации, а также документы на бумажных носителях, содержащие ключевую информацию ограниченного доступа для криптографического преобразования информации с использованием алгоритмов криптографического преобразования информации (криптографический ключ) в шифровальных (криптографических) средствах.
(определение из [Постановления Правительства № 313 от 16 апреля 2012 г.](#))

То есть, ключевой документ — это ключевая информация, записанная на носителе. При анализе ключевой информации и ключевых документов следует выделить, что эксплуатируется (то есть используется для криптографических преобразований – шифрование, электронная подпись и т.д.) ключевая информация, а передаются работникам ключевые документы ее содержащие.

Виды СКЗИ

- средства шифрования,
- средства имитозащиты,
- средства электронной подписи,
- средства кодирования,
- средства изготовления ключевых документов, ключевые документы,
- аппаратные шифровальные (криптографические) средства,
- программно-аппаратные шифровальные (криптографические) средства.

Определения (ПКЗ-2005 и ППЗ13)

Шифровальные (криптографические) средства защиты информации конфиденциального характера именуются средствами криптографической защиты информации (далее - СКЗИ). К СКЗИ относятся:

а) средства шифрования - аппаратные, программные и аппаратно-программные средства, системы и комплексы, реализующие алгоритмы криптографического преобразования информации и предназначенные для защиты информации при передаче по каналам связи и (или) для защиты информации от несанкционированного доступа при ее обработке и хранении;

Определения

б) средства имитозащиты - аппаратные, программные и аппаратно-программные средства, системы и комплексы, реализующие алгоритмы криптографического преобразования информации и предназначенные для защиты от навязывания ложной информации;

в) средства электронной подписи - аппаратные, программные и аппаратно-программные средства, обеспечивающие на основе криптографических преобразований реализацию хотя бы одной из следующих функций: создание электронной подписи с использованием закрытого ключа электронной подписи, подтверждение с использованием открытого ключа электронной подписи подлинности электронной подписи, создание закрытых и открытых ключей электронной подписи;

Определения

г) средства кодирования - средства, реализующие алгоритмы криптографического преобразования информации с выполнением части преобразования путем ручных операций или с использованием автоматизированных средств на основе таких операций;

д) средства изготовления ключевых документов (независимо от вида носителя ключевой информации)- аппаратные, программные, программно-аппаратные шифровальные (криптографические) средства, обеспечивающие возможность изготовления ключевых документов для шифровальных (криптографических) средств, не входящие в состав этих шифровальных (криптографических) средств;

е) ключевые документы (независимо от вида носителя ключевой информации).

The background of the slide is a close-up photograph of a black smartphone lying on a black laptop keyboard. A large, brass-colored metal padlock is attached to the phone's charging port. A set of keys, including a circular metal fob and a standard metal key, is also attached to the padlock. The scene is lit with soft, natural light, creating subtle reflections on the phone's screen and the keyboard keys.

Аудит СКЗИ

Как провести аудит СКЗИ

- Опрос сотрудников;
- Анализ документации организации, включая внутренние нормативные и распорядительные документы;
- Визуальный анализ серверных комнат и коммуникационных шкафов;
- Технический анализ содержимого автоматизированных рабочих мест (АРМ), серверов и средств виртуализации.

Перечень СКЗИ

- Модель СКЗИ. (например, СКЗИ ViPNet CSP или Кripto CSP)
- Идентификатор экземпляра СКЗИ. (серийный, лицензионный или регистрационный по [ПКЗ-2005](#), номер СКЗИ)
- Сведения о сертификате ФСБ на СКЗИ (включая номер и даты начала и окончания сроков действия).
- Сведения о месте эксплуатации СКЗИ (имя компьютера на которое установлено программное СКЗИ, или наименование технических средств или помещения где установлены аппаратные СКЗИ).

Данная информация позволит:

1. Управлять уязвимостями в СКЗИ, то есть быстро их обнаруживать и исправлять.
2. Отслеживать сроки действия сертификатов на СКЗИ, а также проверять используется ли сертифицированное СКЗИ в соответствии с правилами, установленными документацией или нет.
3. Планировать затраты на СКЗИ, зная сколько уже находится в эксплуатации и сколько еще есть сводных средств.
4. Формировать регламентную отчетность.

Перечень ключевой информации

По каждому элементу перечня фиксируем следующие данные:

1. Наименование или идентификатор ключевой информации. Например, «Ключ квалифицированной ЭП. Серийный номер сертификата 31:2D:AF», при этом идентификатор следует подбирать таким образом, чтобы по нему можно было найти ключ. Например, удостоверяющие центры, когда посылают уведомления обычно идентифицируют ключи по номерам сертификатов.
2. Центр управления ключевой системой (ЦУКС), выпустивший данную ключевую информацию. Это может быть организация выпустившая ключ, например, удостоверяющий центр.
3. Физическое лицо, на имя которого выпущена ключевая информация. Эту информацию можно извлечь из полей CN сертификатов X.509
4. Формат ключевой информации. Например, СКЗИ ViPNet, КриптоПРО, СКЗИ Верб-OW, X.509 и т.д (или другими словами для использования с какими СКЗИ предназначена данная ключевая информация).
5. Назначение ключевой информации. Например, «Участие в торгах на площадке Сбербанк АСТ», «Квалифицированная электронная подпись для сдачи отчетности» и т.д.
6. Начало и окончание сроков действия ключевой информации.
7. Порядок перевыпуска ключевой информации. То есть знания о том, что нужно делать и как, при перевыпуске ключевой информации. По крайней мере желательно фиксировать контакты должностных лиц ЦУКС, выпустившего ключевую информацию.
8. Перечень информационных систем, сервисов или бизнес-процессов в рамках которых используется ключевая информация. Например, «Система дистанционного банковского обслуживания Интернет Клиент-Банк».

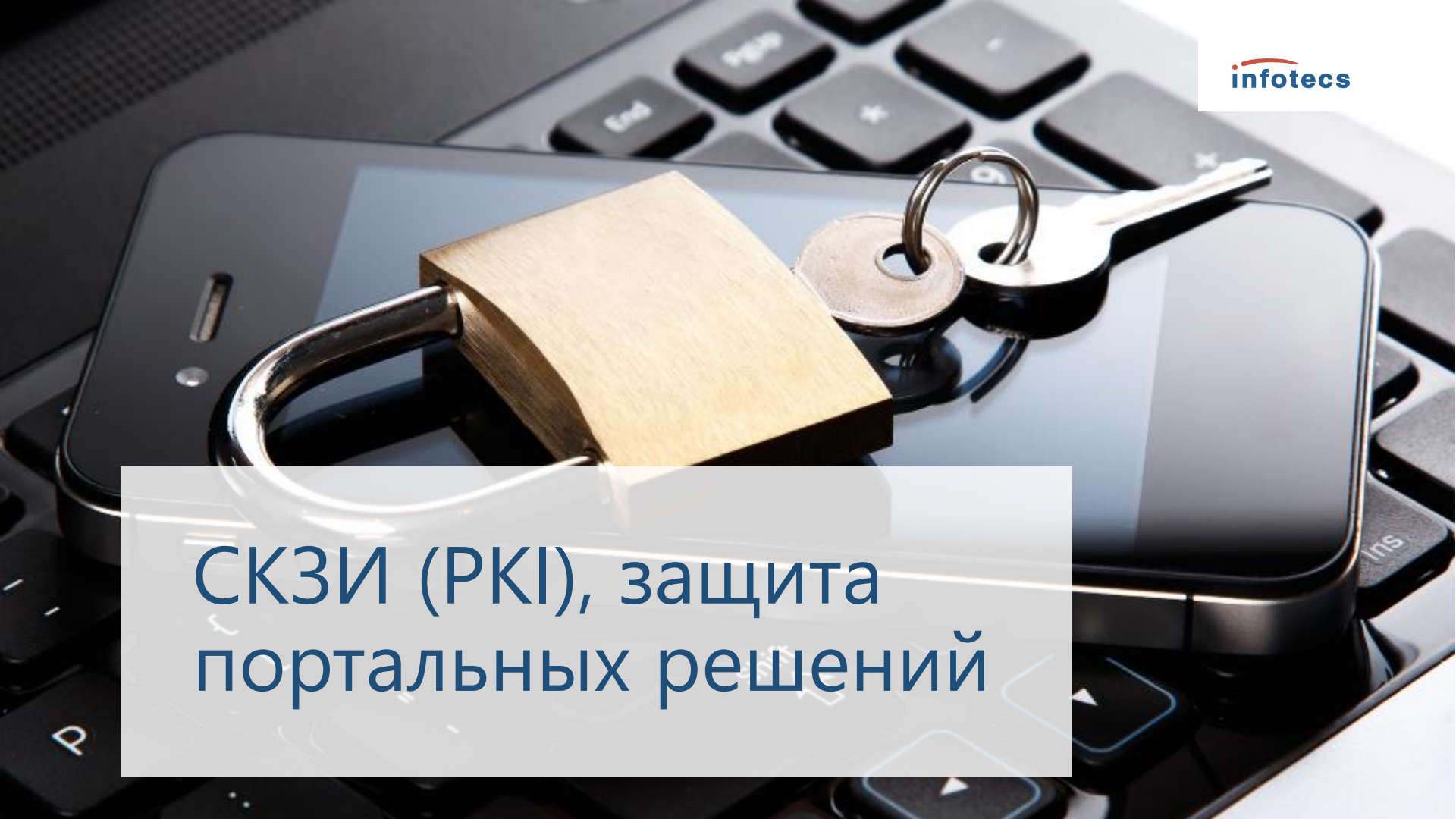
Перечень ключевых документов

По каждому элементу перечня необходимо указать данные:

1. Ключевая информация, содержащаяся в ключевом документе.
2. Носитель ключевой информации, на который записана ключевая информация.
3. Лицо, ответственное за сохранность ключевого документа и конфиденциальность содержащейся в нем ключевой информации.

Данная информация позволит:

- Перевыпускать ключевую информацию в случаях: увольнения работников, обладающих ключевыми документами, а также при компрометации носителей.
- Обеспечивать конфиденциальность ключевой информации, путем инвентаризации носителей ее содержащих.

The background of the slide is a close-up photograph of a black smartphone lying on a black laptop keyboard. A large, brass-colored metal padlock is attached to the phone's charging port. A set of keys, including a car key and a house key, is resting on the phone's screen. The text 'СКЗИ (PKI), защита порталных решений' is overlaid on a semi-transparent white box in the lower-left area of the image.

СКЗИ (PKI), защита порталных решений

Услуги, предоставляемые УЦ

В процессе своей деятельности УЦ предоставляет пользователям УЦ следующие виды услуг:


- внесение в реестр УЦ регистрационной информации о владельцах сертификатов;
- изготовление сертификатов в электронной форме;
- изготовление сертификатов на бумажном носителе;
- формирование ключей ЭП и ключей проверки ЭП по обращениям заявителей с записью их на ключевой носитель;
- ведение реестра сертификатов, изданных в данном УЦ;
- предоставление в электронной форме сертификатов, находящихся в реестре изготовленных сертификатов, по запросам пользователей;
- аннулирование сертификатов по обращениям владельцев сертификатов;
- ведение списков аннулированных сертификатов (далее – CRL) и предоставление доступа к ним пользователям;
- подтверждение подлинности ЭП в документах, представленных в электронной форме, по обращениям пользователей;
- подтверждение подлинности ЭП доверенного лица УЦ в изготовленных им сертификатах по обращениям пользователей;
- распространение средств ЭП по обращениям пользователей.

Пример (Удостоверяющий центр ViPNet)

Обязательные компоненты		
Средства удостоверяющего центра	программный комплекс ViPNet Administrator®	выполняет функции Центра сертификации
	программное обеспечение ViPNet Registration Point	выполняет функции Центра регистрации
	программное обеспечение ViPNet CA Informing	предоставляет функции Сервиса информирования
Вспомогательное программное обеспечение	программное обеспечение ViPNet Publication Service	выполняет функции Сервиса публикации
Средство криптографической защиты информации	программное обеспечение ViPNet CSP 4.2	используется в качестве средства ЭП
Дополнительные компоненты		
	Программный комплекс ViPNet TSP-OCSP Service	выполняет функции службы штампов времени и сервиса проверки статуса сертификатов
	Веб-служба ViPNet CA Web Service	для организации взаимодействия между клиентами веб-службы и программой ViPNet УКЦ
	Программа ViPNet CryptoFile	для защиты файлов любых форматов с помощью шифрования

TLS Gateway

- СКЗИ в исполнениях класса КС1 и КС3
- Сертификат действует до 28.02.2021


**ФЕДЕРАЛЬНАЯ СЛУЖБА БЕЗОПАСНОСТИ
РОССИЙСКОЙ ФЕДЕРАЦИИ**

Система сертификации РОСС RU.0001.030001

СЕРТИФИКАТ СООТВЕТСТВИЯ

Регистрационный номер СФ/124-3339 от "28" февраля 2021 г.
Действителен до "28" февраля 2021 г.


Выдан Открытому акционерному обществу «Информационные технологии и коммуникационные системы» (ОАО «ИнфоТеКС»).


Настоящий сертификат удостоверяет, что изделие VIPNet TLS Gateway (исполнения 1, 2, 3, 5) в комплектации согласно формуляру ФРКБ.00169-01.30.01 ФГО

соответствует Требованиям к средствам криптографической защиты информации, предназначенным для защиты информации, не содержащей сведений, составляющих государственную тайну, класса КС1 (для исполнения 5) класса КС3 (для исполнений 1, 2, 3), и может использоваться для криптографической защиты (создание и управление ключевой информацией, шифрование файлов и данных, содержащихся в областях оперативной памяти, выделение выделенных функций для файлов и данных, содержащихся в областях оперативной памяти, защита TLS-соединений) информации, не содержащей сведений, составляющих государственную тайну.


Сертификат выдан на основании результатов проведенных _____ ОАО «ИнфоТеКС»
сертификационных испытаний образцов продукции №№ 906-000501, 906-000502, 906-000503, 906-000504.

Безопасность информации обеспечивается при использовании изделия в соответствии с требованиями аттестационной документации согласно формуляру ФРКБ.00169-01.30.01 ФГО.

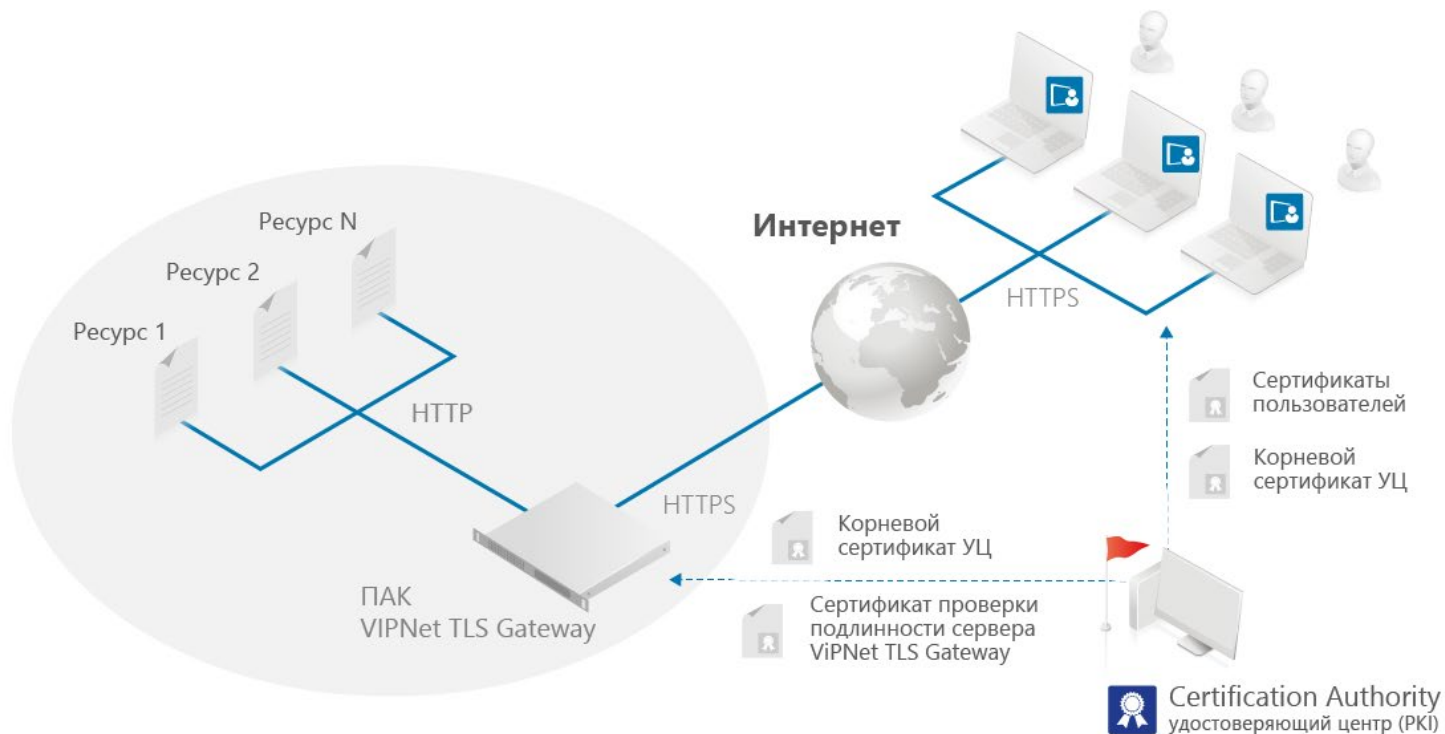
Заместитель руководителя Научно-технической
службы – начальник Центра защиты информации
и специальной связи ФСБ России  **А.М. Изашко**



Настоящий сертификат зарегистрирован в государственном реестре сертификатов ФСБ России.

Заместитель начальника Центра по лицензированию,
сертификации и защите государственной тайны ФСБ России  **А.В. Парфенов**

Пример ViPNet TLS Gateway



Пример ViPNet TLS Gateway

Управление доступом на основе сертификатов

- Ведение черных и белых списков
- Задание правил предоставления доступа
- Обработка запросов на предоставление доступа

Поддержка различных центров доверия

- Автоматическое обновление CRL
- Поддержка TSL-списка (Минкомсвязь)

Удаленное управление

- Ролевая модель
- Управление и пользовательский интерфейс разделены

The background image shows a black smartphone lying on a black laptop keyboard. A large, brass-colored metal padlock is attached to the phone's charging port. A set of keys, including a circular metal fob and a standard metal key, is also attached to the padlock's shackle. The scene is lit from the top right, creating highlights on the metal and the phone's screen.

ОРД

Услуги, предоставляемые УЦ

В процессе своей деятельности УЦ предоставляет пользователям УЦ следующие виды услуг:

- внесение в реестр УЦ регистрационной информации о владельцах сертификатов;
- изготовление сертификатов в электронной форме;
- изготовление сертификатов на бумажном носителе;
- формирование ключей ЭП и ключей проверки ЭП по обращениям заявителей с записью их на ключевой носитель;
- ведение реестра сертификатов, изданных в данном УЦ;
- предоставление в электронной форме сертификатов, находящихся в реестре изготовленных сертификатов, по запросам пользователей;
- аннулирование сертификатов по обращениям владельцев сертификатов;
- ведение списков аннулированных сертификатов (далее – CRL) и предоставление доступа к ним пользователям;
- подтверждение подлинности ЭП в документах, представленных в электронной форме, по обращениям пользователей;
- подтверждение подлинности ЭП доверенного лица УЦ в изготовленных им сертификатах по обращениям пользователей;
- распространение средств ЭП по обращениям пользователей.

The background image shows a black smartphone lying on a black laptop keyboard. A large, brass-colored metal padlock is attached to the phone's charging port. A set of keys, including a circular metal fob and a standard house key, is attached to the padlock's shackle. The scene is lit with soft, directional light, creating highlights on the metal and the phone's surface.

VPN

Определения

VPN – способ использования открытых и частных сетей такой, чтобы пользователи VPN были отделены от других пользователей и могли взаимодействовать между собой, как если бы они находились в единой закрытой (выделенной) сети.

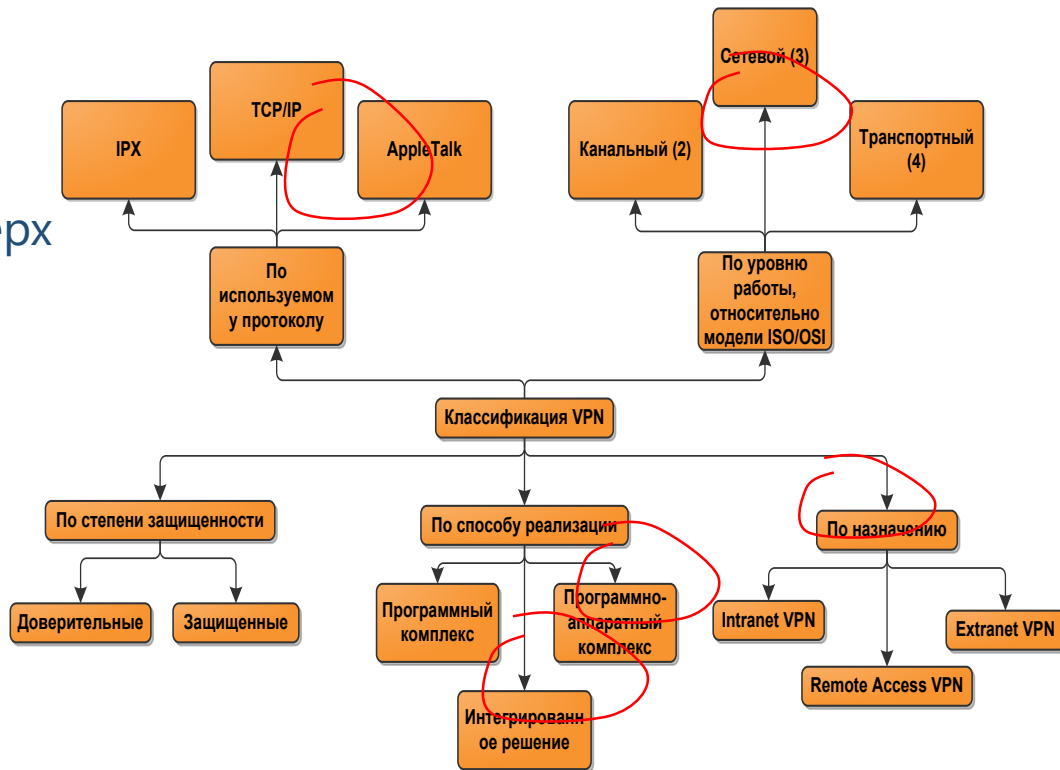
VPN – virtual private network (виртуальная частная сеть) или virtual **protected** network (виртуальная **защищенная** сеть)

Классификация VPN

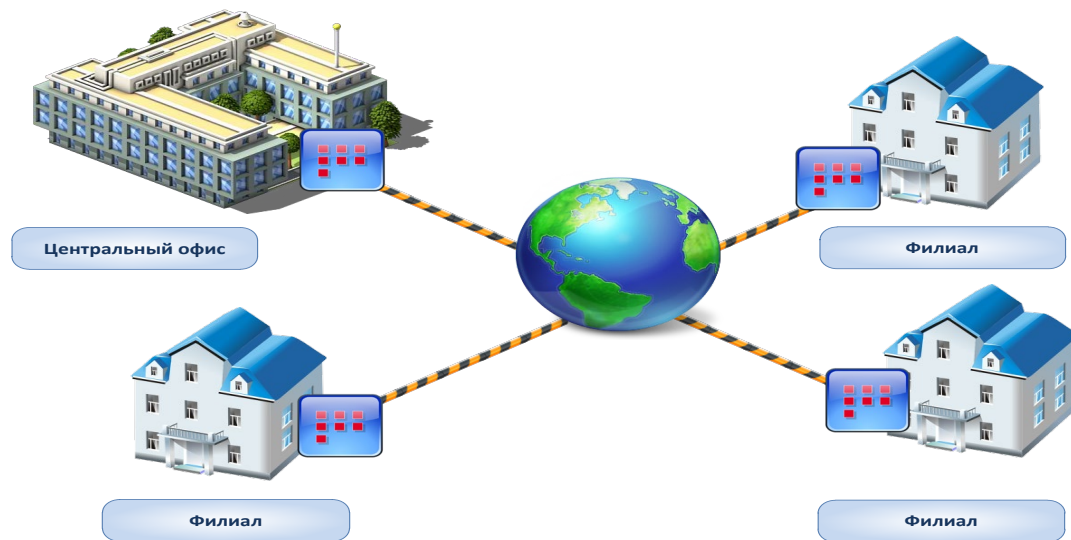
VPN (*Virtual Private Network* — виртуальная частная сеть) — логическая сеть, создаваемая поверх другой сети, например Интернет.

Примеры технологий VPN

- L2TP/IPSec
- PPTP
- OpenVPN
- **ViPNet**
- ...

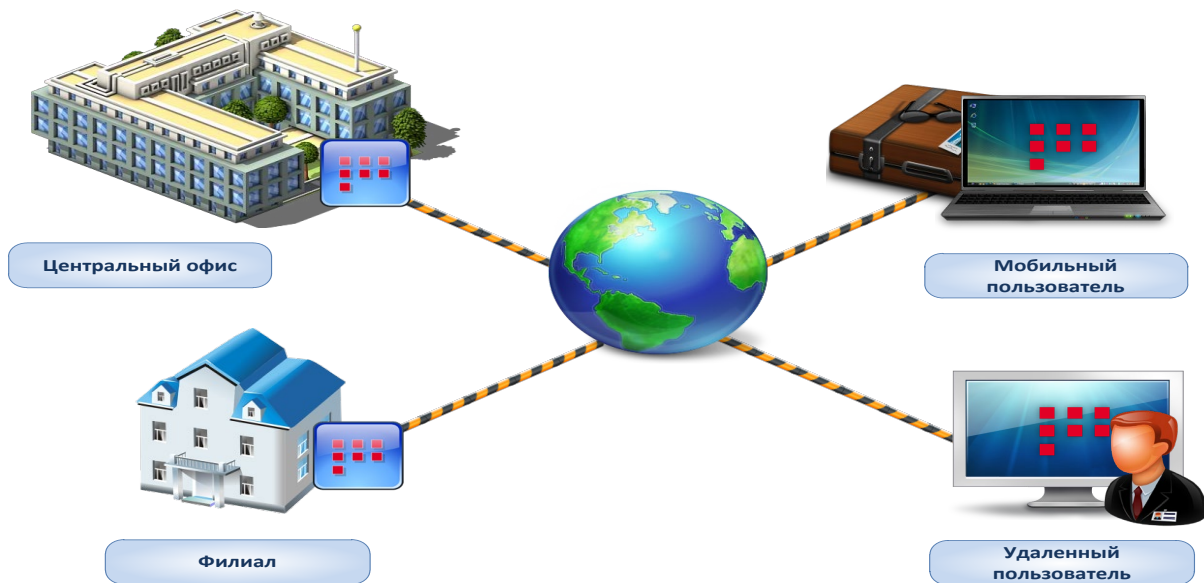


Intranet VPN



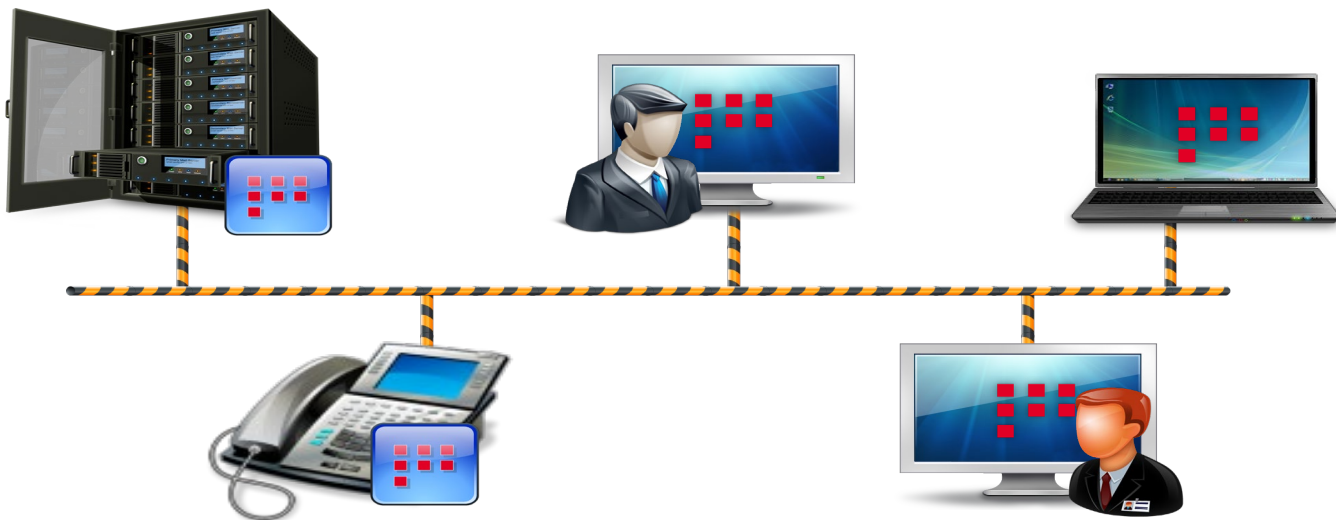
- внутрикорпоративная виртуальная сеть
- объединяет в единую защищенную сеть подразделения одной организации
- строится на базе общедоступных сетей связи

Remote Access VPN



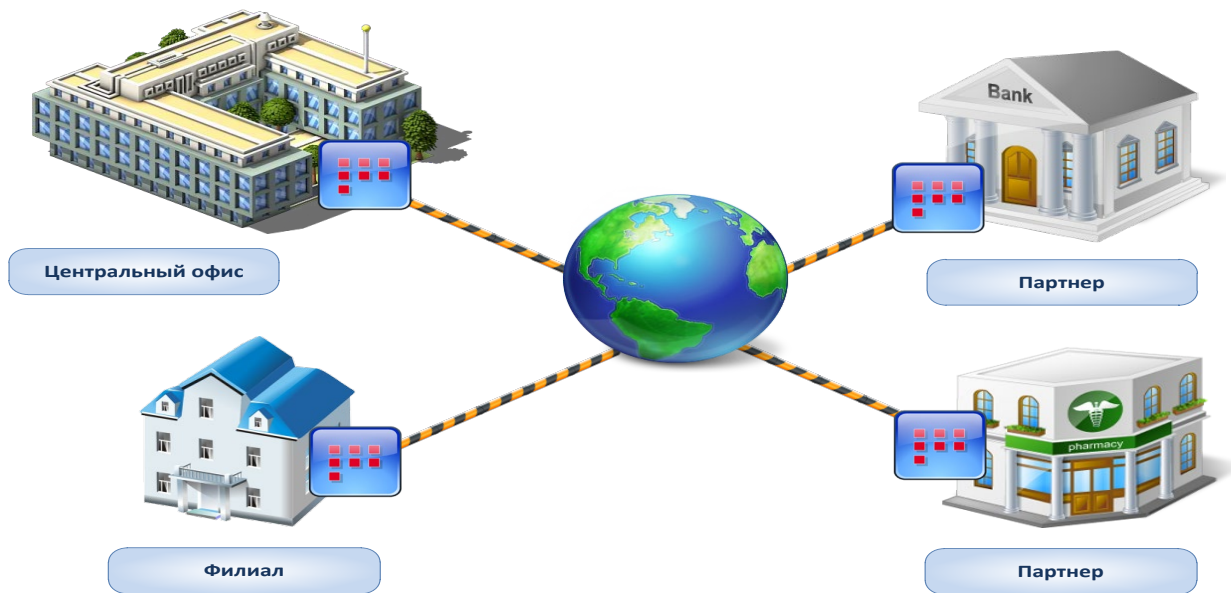
- виртуальная сеть с удаленным доступом
- обеспечивает **защищенное взаимодействие** между сегментом корпоративной сети и внешними пользователями
- строится на базе общедоступных сетей связи

Client-Server VPN



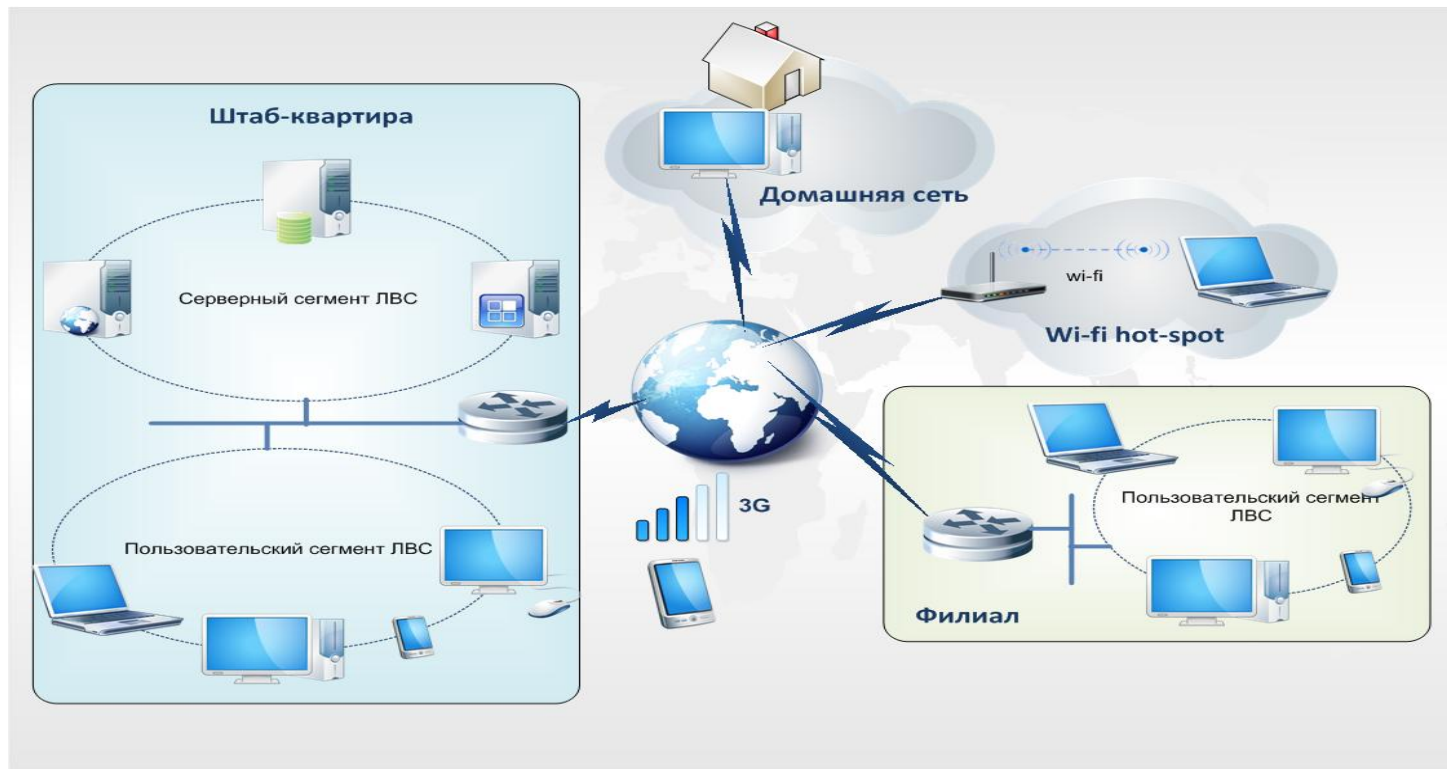
- обеспечивает защиту передаваемых данных между двумя узлами корпоративной сети

Extranet VPN

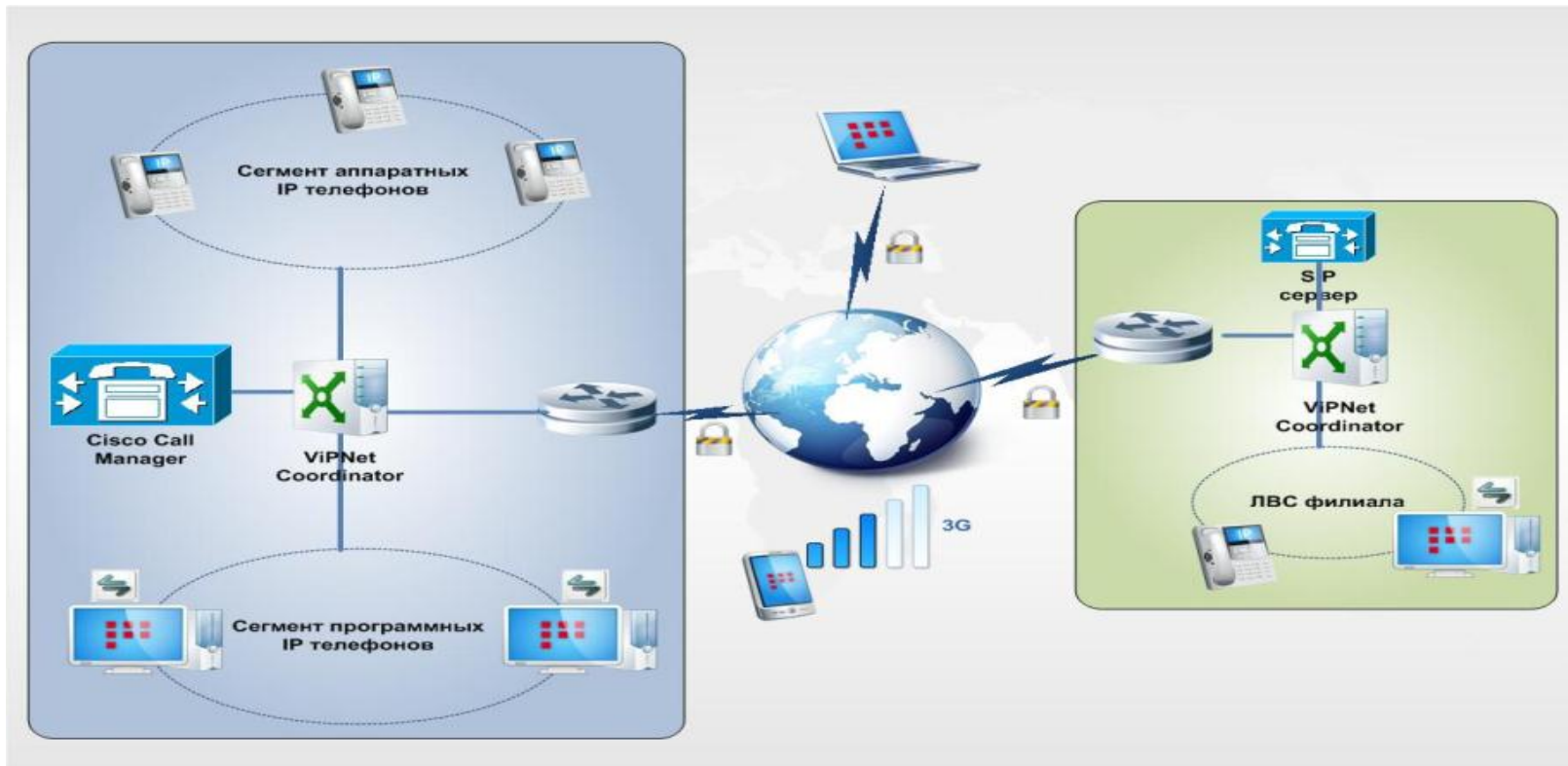


- междооорпоративная виртуальная сеть
- обеспечивает защищенное соединение сети компании с сетями ее деловых партнеров и клиентов
- строится на базе общедоступных сетей связи

Пример 1



Пример 2



Структура VPN

VPN состоит из двух частей:

- «внутренняя» (подконтрольная) сеть, которых может быть несколько,
- и «внешняя» сеть, по которой проходит инкапсулированное соединение (обычно используется Интернет).



Туннелирование IP-трафика

Туннель – защищенное соединение, созданное для передачи конфиденциальной информации через открытую сеть

Туннель создается с помощью технологий инкапсуляции и туннелирования

Туннель обладает свойствами защищенной выделенной линии



Туннелирующий VPN-шлюз – VPN-шлюз за которым находится открытый узел и который с помощью туннелирования защищает трафик открытого узла

Туннелируемый ресурс – незащищенный компьютер, трафик которого защищается при передаче через открытые сети с помощью процедуры туннелирования

Туннелирование IP-трафика



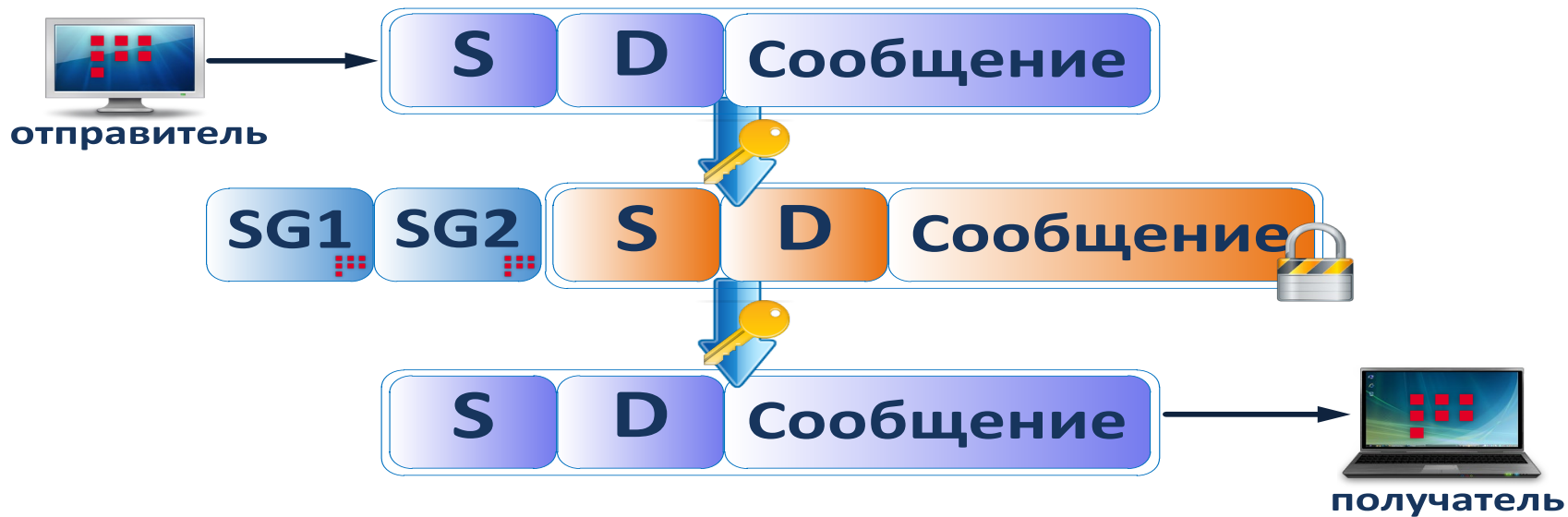
Инкапсуляция IP-трафика

Инкапсуляция:

- способ передачи защищаемой информации через открытую сеть при котором передаваемый IP-пакет вместе со служебными полями упаковывается в новый пакет
- при инкапсуляции любые IP-пакеты с использованием шифрования преобразуются в IP-пакеты единого типа. Это позволяет полностью скрыть структуру информационного обмена



Инкапсуляция IP-трафика



Инкапсуляция IP-трафика

При инкапсуляции пакеты любых IP-протоколов упаковываются в пакеты IP-протоколов двух типов: (IP/241 и IP/UDP)

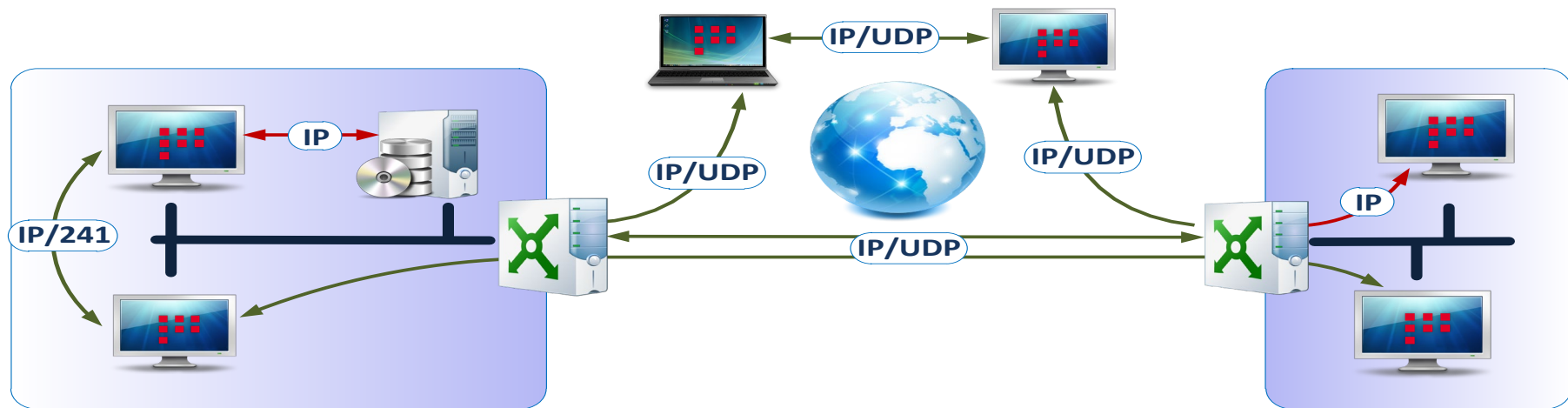
Используется протокол IP/241

- если по пути следования пакета нет преобразования IP-адресов (узлы доступны по реальным IP-адресам)
- если узлы расположены в одном маршрутизируемом сегменте

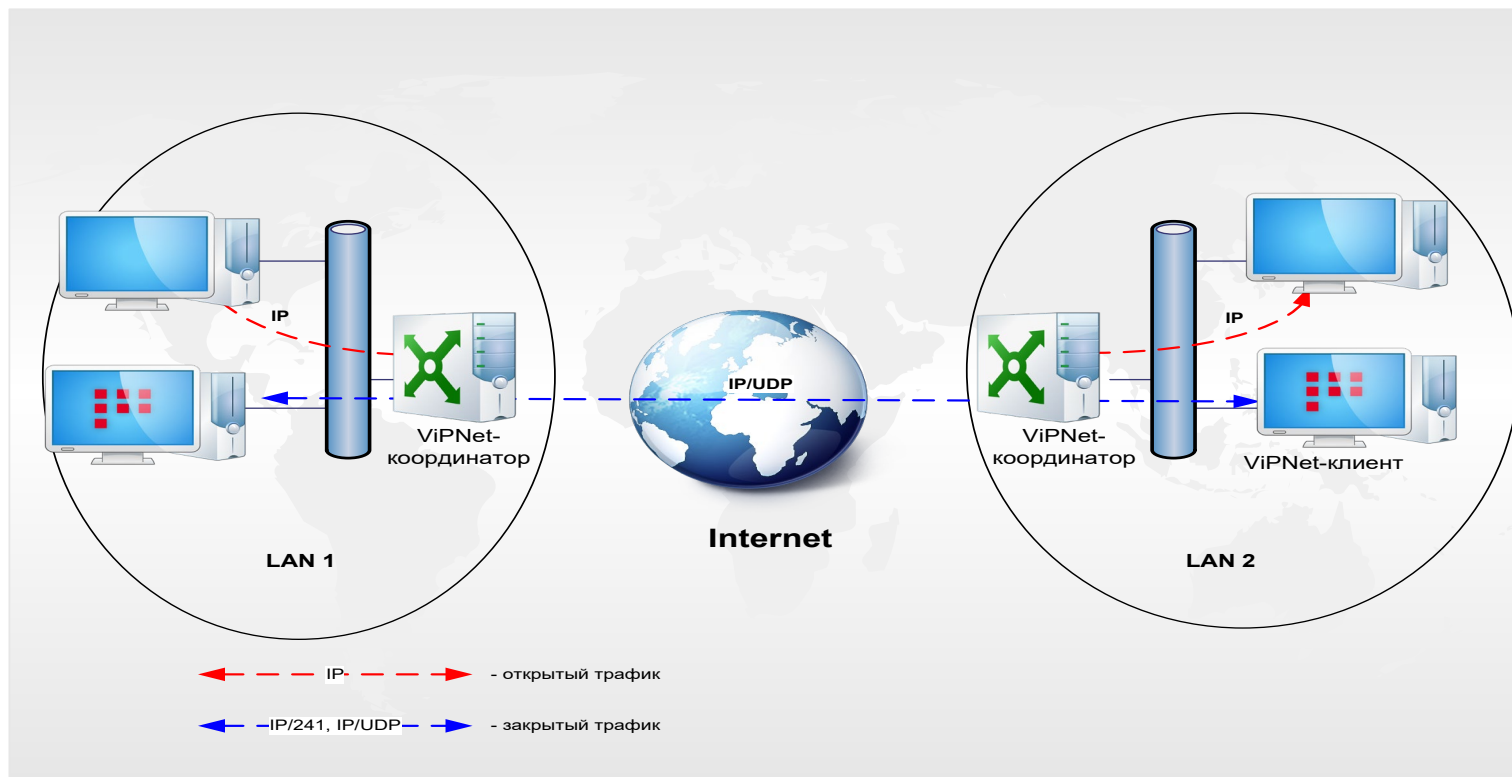
Используется протокол IP/UDP (порт 55777)

- если по пути пакета выполняется преобразование IP-адресов (на пути следования IP-пакета расположено устройство NAT)

Инкапсуляция IP-трафика



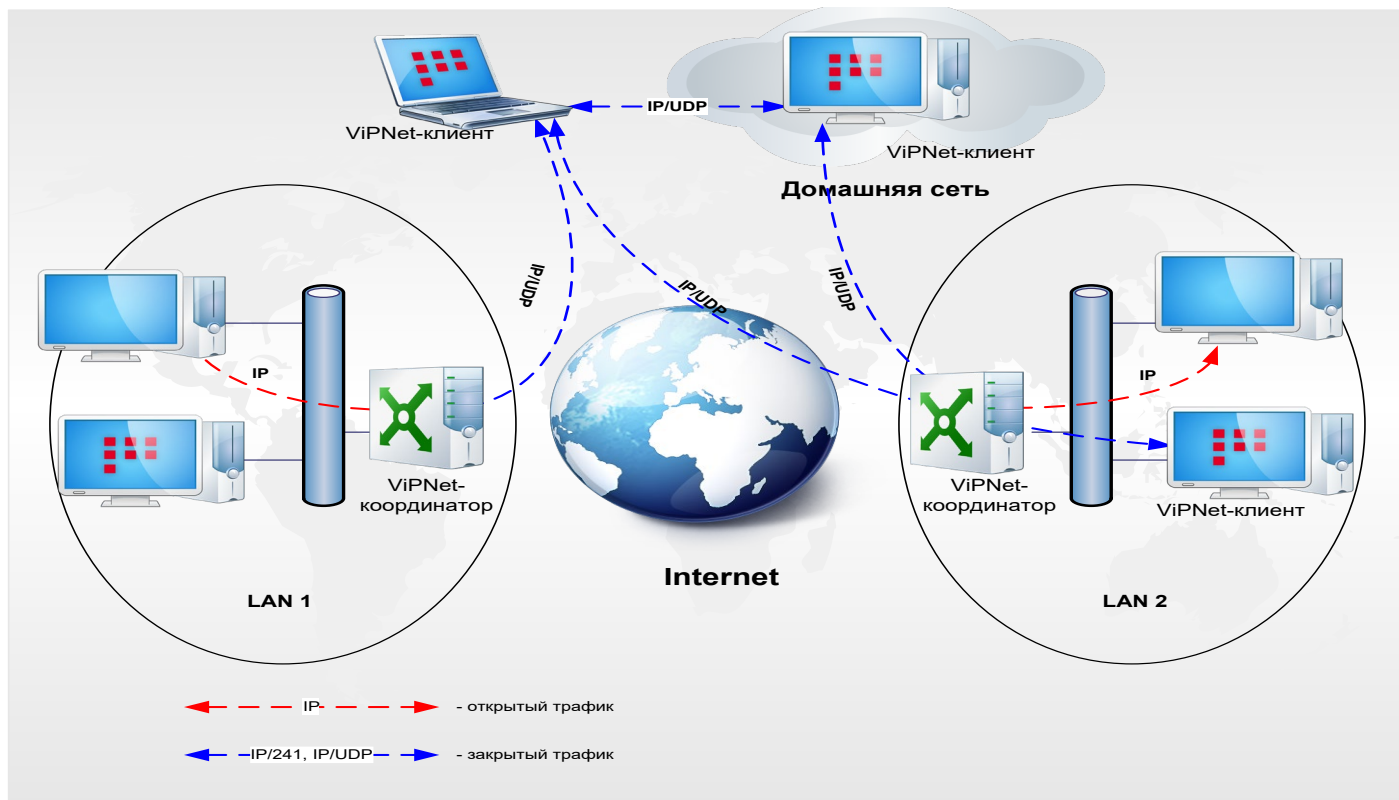
Примеры



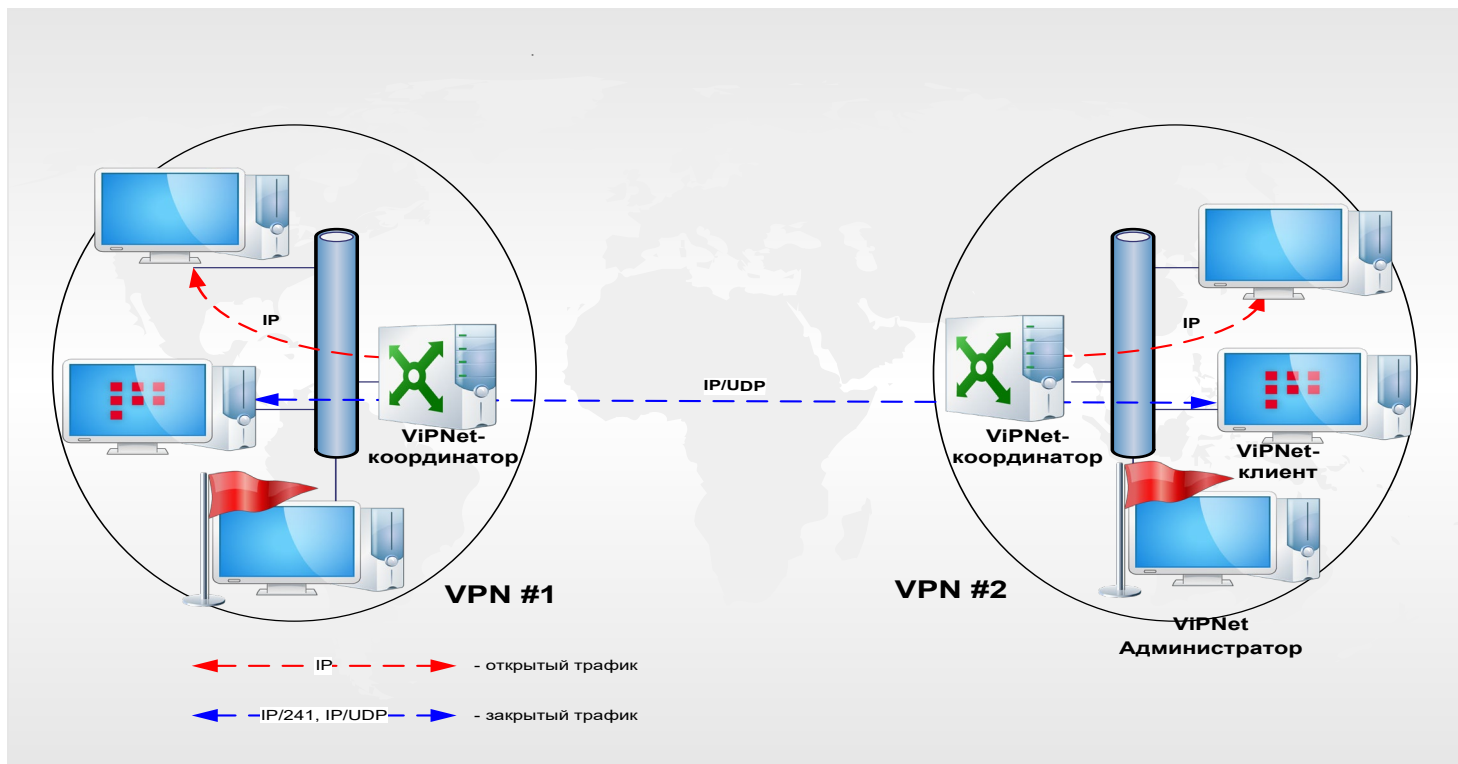
Терминальный доступ



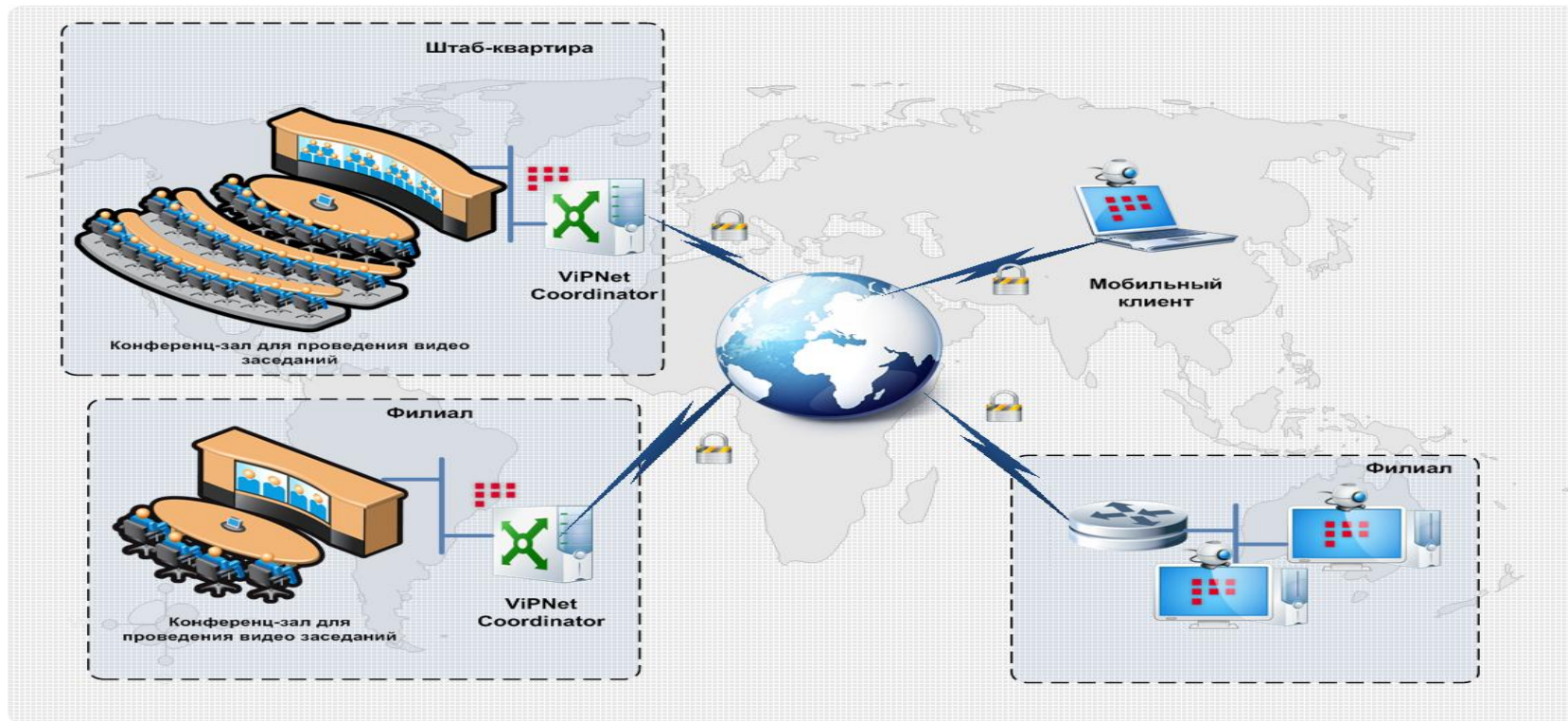
Защищенный удаленный доступ



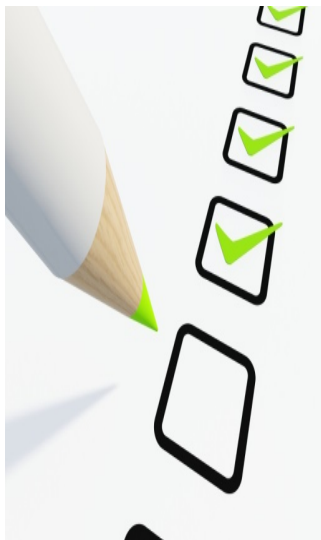
Межсетевое взаимодействие



Защита видеоконференцсвязи



Преимущества VPN



Технологии VPN на основе симметричной криптографии:

- позволяют быстро построить VPN-сеть любой масштабируемости, не обращая внимания на адресную структуру,
- позволяют размещать VPN-модули, как на компьютерах внутри локальных сетей, защищенных NAT-устройствами, так и на VPN-шлюзах на границе локальных сетей для защиты локальной сети в целом или ее фрагментов.

Предоставляется возможность обеспечить безопасность информации при наличии внутренних и внешних нарушителей.

Network Security

Защита
корпоративного
уровня

ViPNet VPN

Обнаружение и
пресечение
вторжений и атак

Intrusion & Threats
Detection and
Prevention

Защита порталных и
WEB based систем

Web Secured Gateways

Защита конечных узлов Endpoint Protection

Доверенная среда
функционирования

Обнаружение и
предотвращение угроз

Безопасность данных

Криптографические системы, сервисы и приложения

Инфраструктура
открытого ключа
PKI

Прикладная
криптография

Криптографические
платформы

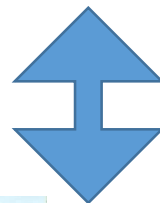
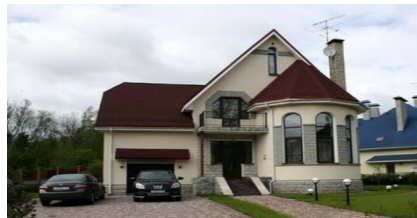
The background of the slide is a close-up photograph of a black smartphone lying on a black laptop keyboard. A large, brass-colored metal padlock is attached to the phone's charging port. A set of keys, including a circular metal fob and a standard metal key, is resting on the phone's screen. The lighting is dramatic, with strong highlights and shadows.

Шифраторы дисков

Шифраторы дисков

Такой шифратор решает следующие задачи:

- конфиденциальная информация хранится на нескольких компьютерах (например, дома и на работе), и вам нужно защитить каждый из них таким образом, чтобы можно было передавать данные между компьютерами;



Шифраторы дисков

- нужно передать конфиденциальную информацию на съемном носителе, и вы не хотите, чтобы данные были потеряны или украдены;

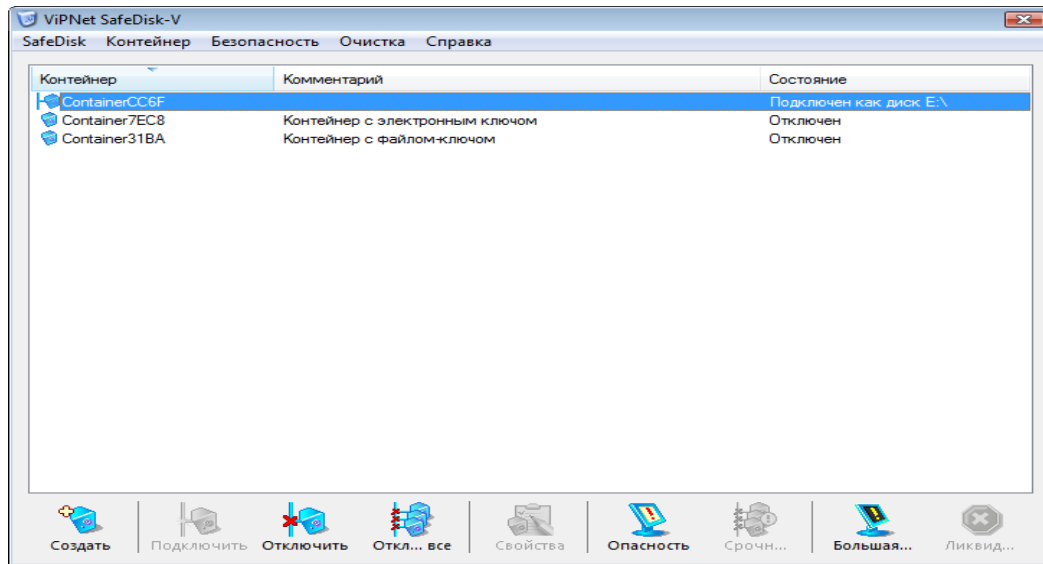


Шифраторы дисков

- вам нужно контролировать доступ к конфиденциальной информации на одном или нескольких компьютерах (например, предоставить доступ к документам некоторым пользователям и скрыть их от других пользователей);
- при приближении посторонних лиц вам необходимо закрыть доступ к информации и скрыть ее наличие;
- при приближении злоумышленников вам необходимо быстро и надежно удалить всю конфиденциальную информацию.

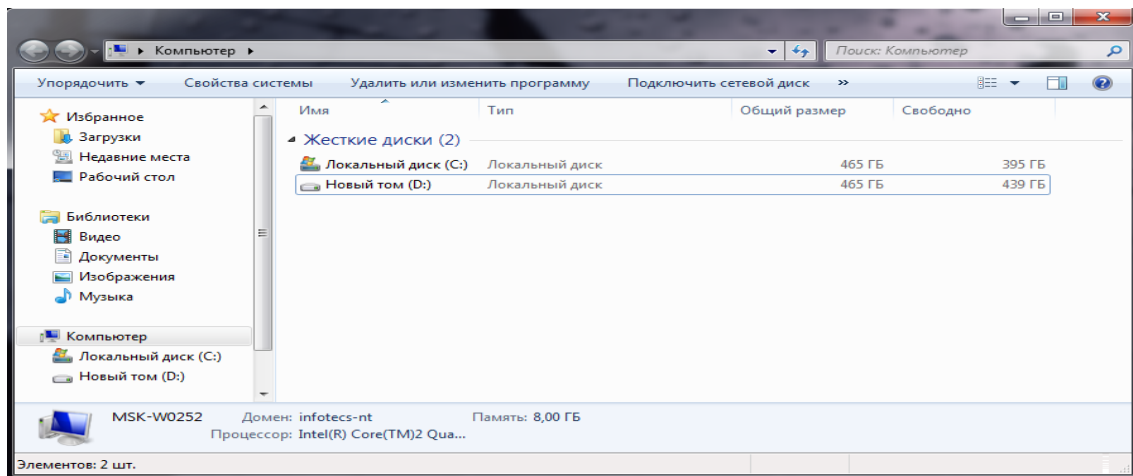
Шифраторы дисков

В таких шифраторах создается контейнер, который представляет собой зашифрованный файл на жестком диске или съемном носителе.



Шифраторы дисков

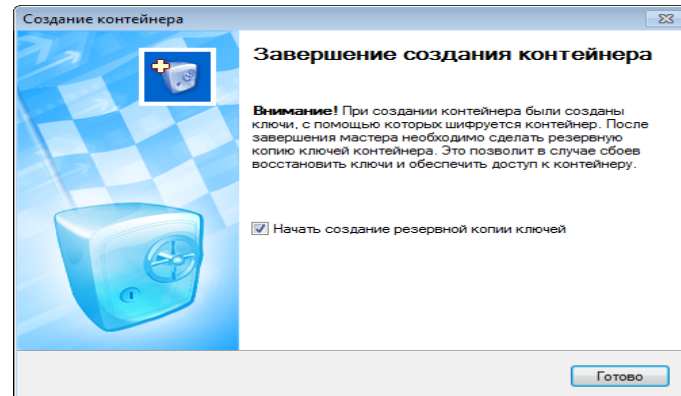
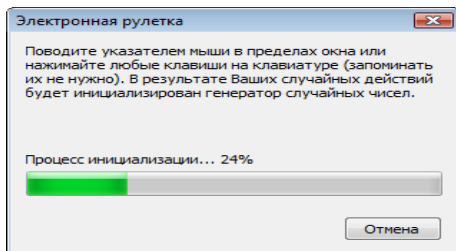
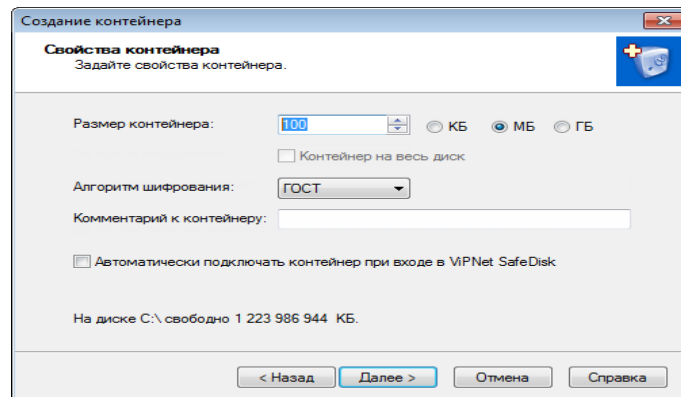
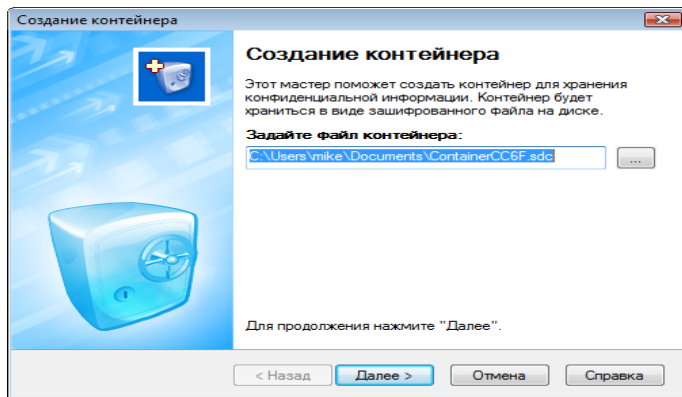
При подключении контейнер отображается в системе как обычный диск, на который можно сохранять конфиденциальную информацию.



Защита информации: порядок действий

- Создать контейнер (контейнеры);
- Создать резервные копии ключей контейнера (контейнеров);
- Регулярно создавать резервные копии конфигурации;
- Регулярно создавать файлы экспорта контейнера;
- Подготовиться к работе в условиях потенциальной опасности;
- Всегда проводить полную очистку для уничтожения следов работы с конфиденциальной информацией;

Создание контейнера




Создание резервной копии ключей контейнера

Создание резервной копии ключей контейнера

Способ хранения резервной копии ключей контейнера
Укажите способ хранения резервной копии ключей.

Способ хранения: Файл

 Резервная копия ключей контейнера будет храниться в файле, который рекомендуется разместить на внешнем носителе.

Задайте имя и расположение файла резервной копии ключей:


< Назад **Далее >** Отмена Справка



Создание резервной копии ключей контейнера

Способ хранения резервной копии ключей контейнера
Укажите способ хранения резервной копии ключей.

Способ хранения: Электронный ключ

 Резервная копия ключей контейнера будет храниться на электронном ключе. Электронным ключом может быть, например, смарт-карта, USB-токен или таблета TouchMemory.

Имя резервной копии ключей:

Устройство: eToken Aladdin(0001d408)

Введите ПИН-код:

☐ Сохранить ПИН-код

< Назад **Далее >** Отмена Справка



Создание резервной копии ключей контейнера

Пароль доступа
Задайте пароль для последующего доступа к резервной копии ключей.

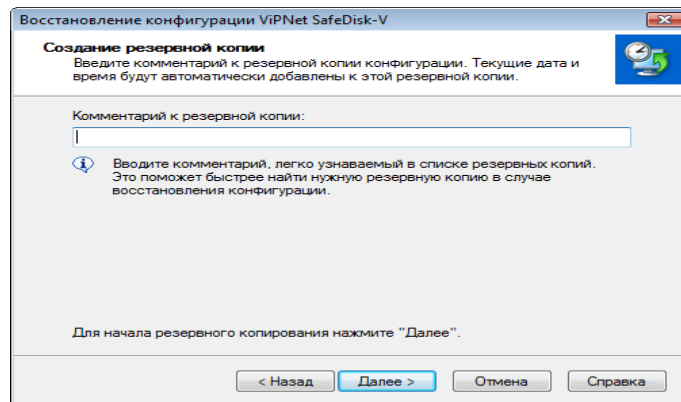
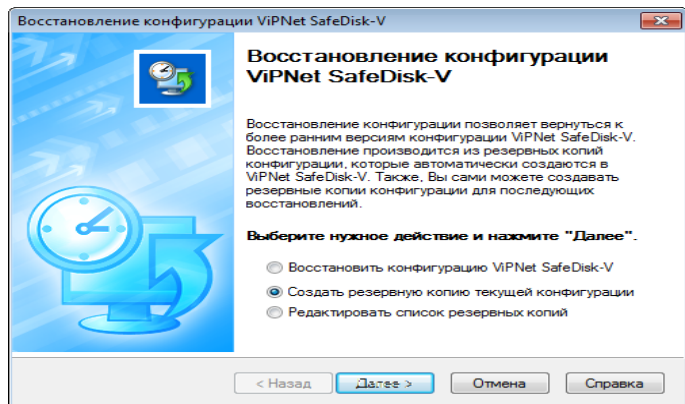
Задайте пароль:

Введите пароль еще раз для подтверждения:

Не рекомендуется использовать пароль для входа в VIPNet SafeDisk. Пароль должен содержать не менее 6 символов.

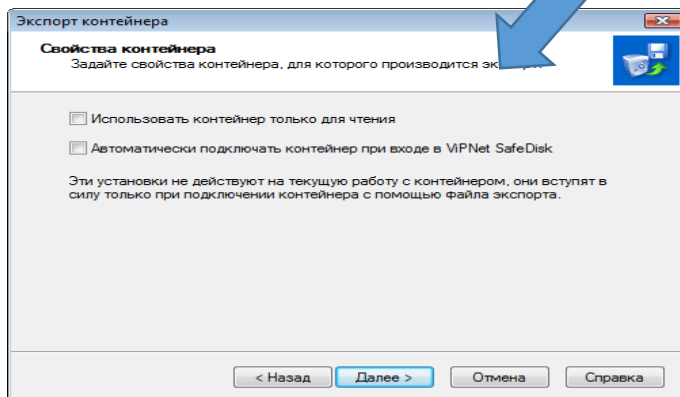
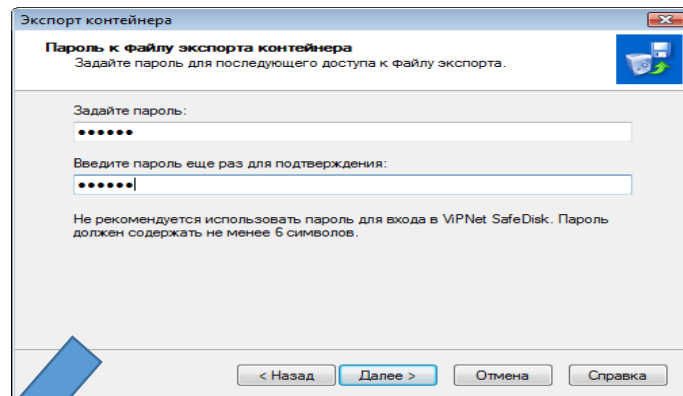
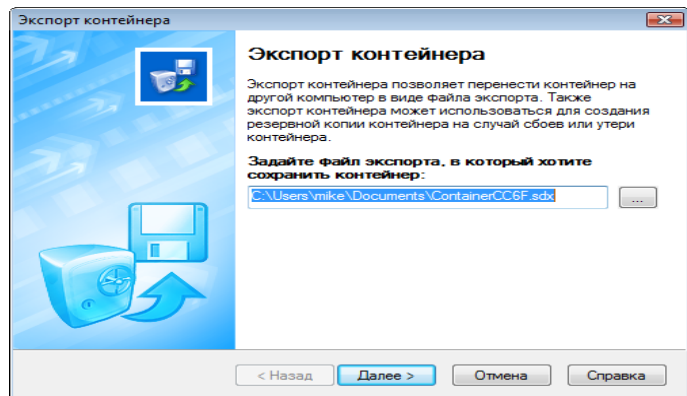
< Назад **Далее >** Отмена Справка

Восстановление доступа ко всем контейнерам с помощью восстановления конфигурации

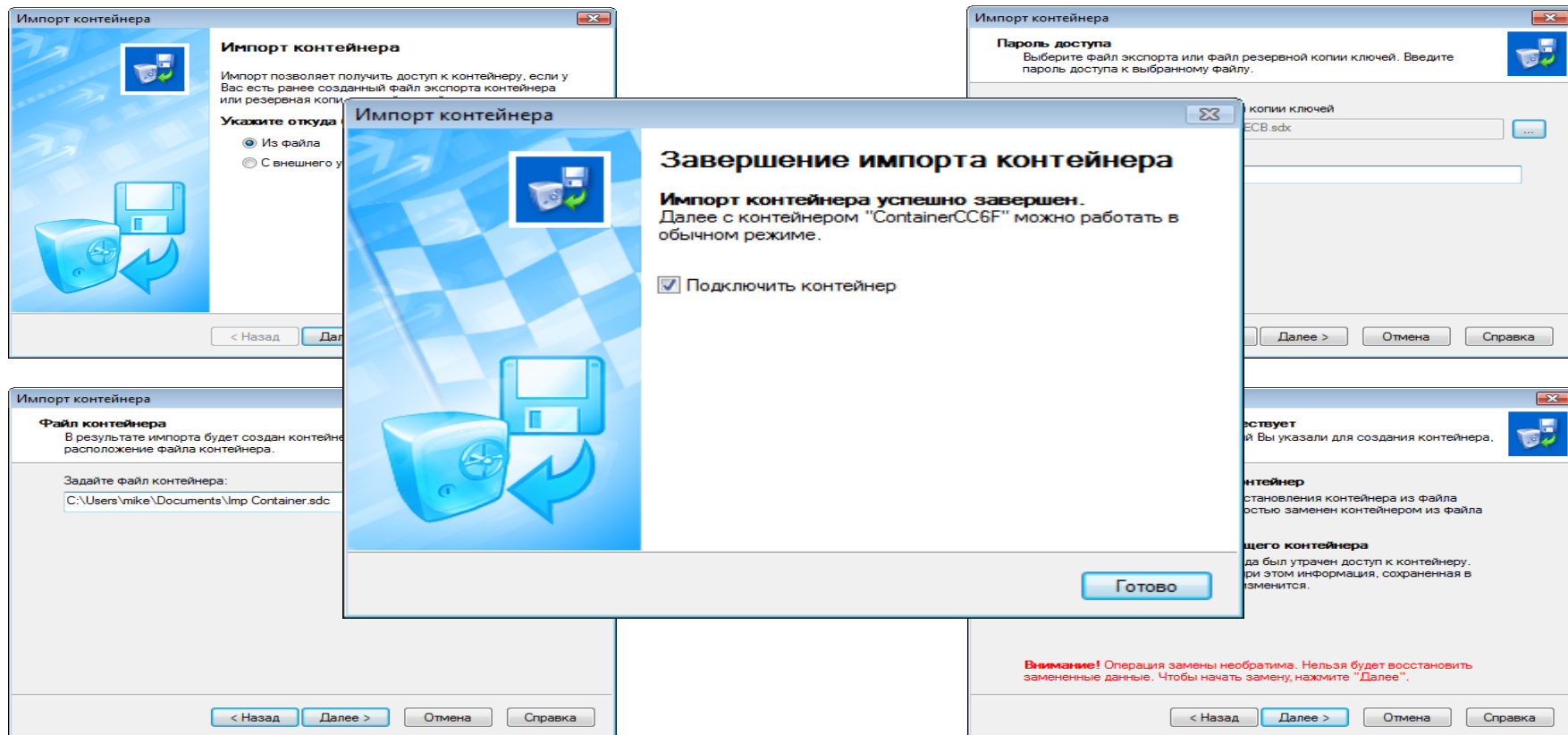


Созданная резервная копия конфигурации будет сохранена в подпапке \Restore папки установки программы.

Экспорт контейнера



Импорт контейнера

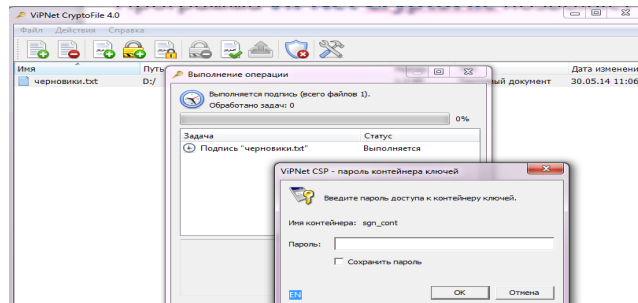
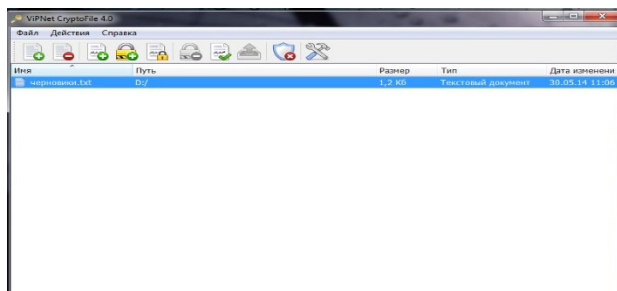


Программа для подписи и шифрования файлов (CryptoFile) -

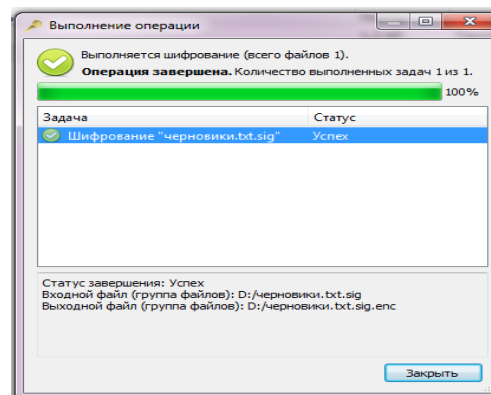
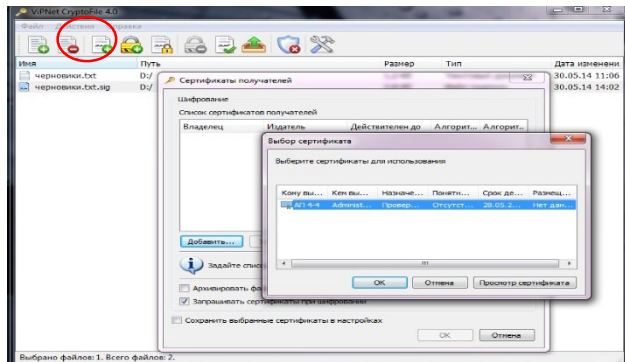
предназначена для **обеспечения безопасности различных файлов, передаваемых по открытым каналам связи или с помощью съемных носителей**

CryptoFile

Защищает файлы с помощью электронной подписи

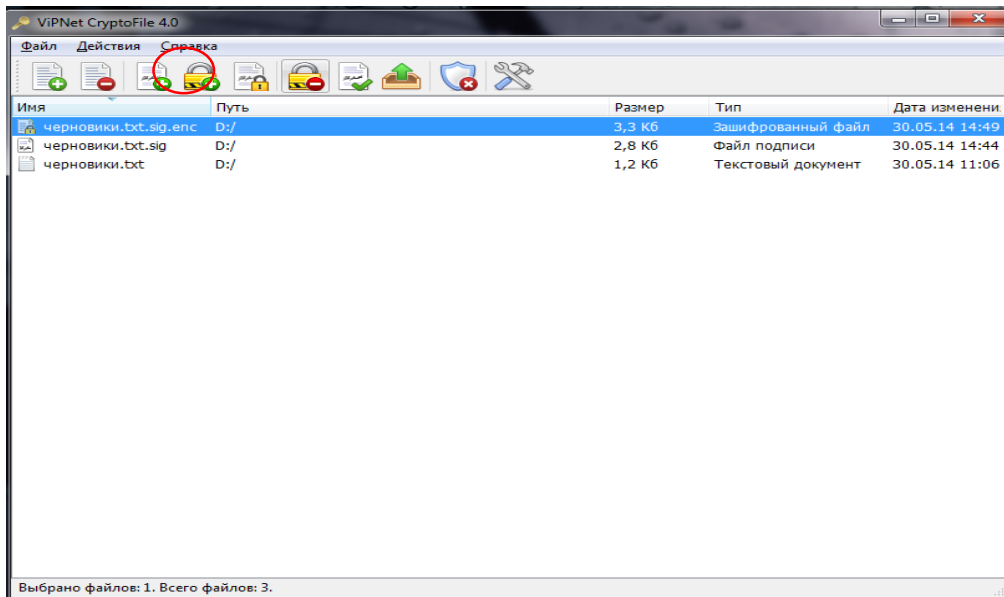


и шифрования:



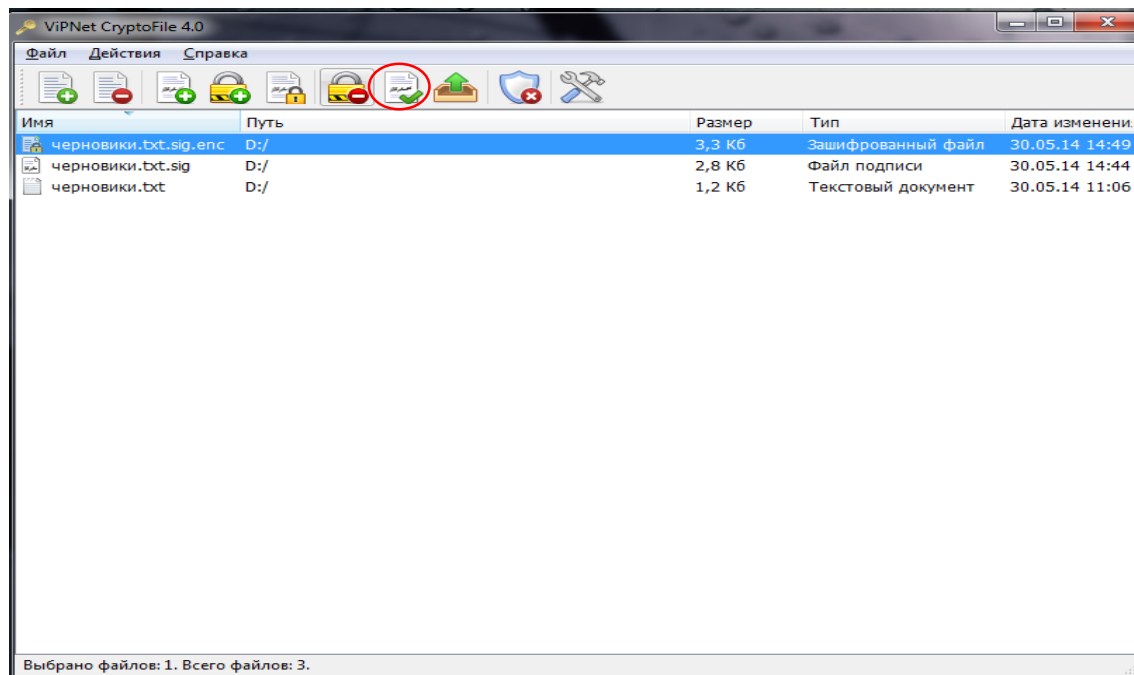
CryptoFile

Позволяет расшифровывать полученные файлы - зашифрованные в программах, поддерживающих асимметричные алгоритмы шифрования и стандартное расширение ***.enc** для зашифрованных файлов.



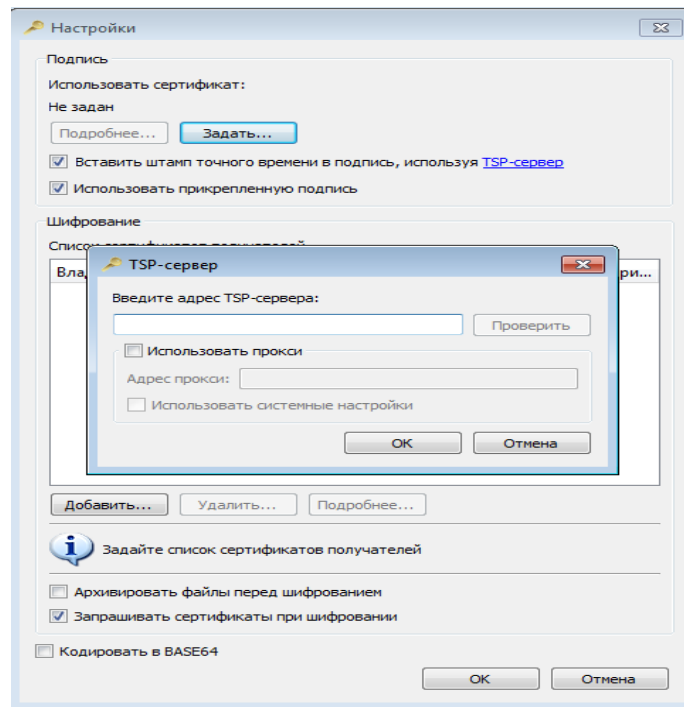
CryptoFile

Проверяет электронную подпись файлов



Добавление штампа точного времени при заверении файлов электронной подписью

При заверении файла электронной подписью вы можете добавить к подписи штамп точного времени. Штамп точного времени подтверждает точное время подписания файла и при возникновении спорных ситуаций позволяет доказать факт существования файла на момент его подписания.



Архивирование файлов перед шифрованием

Позволяет объединить несколько файлов в один архив формата ZIP и далее поместить этот архив в один контейнер при шифровании. Данная функция позволяет ускорить работу при отправлении большого количества зашифрованных файлов одному получателю.



Использовать прикрепленную или открепленную подпись

При использовании прикрепленной подписи электронная подпись и исходный файл совместно помещаются в контейнер.

Прикрепленная подпись обеспечивает простоту обмена, копирования и шифрования подписанных файлов. При этом ознакомиться с содержимым файла смогут только пользователи, на компьютерах которых установлены специальные средства работы с контейнерами

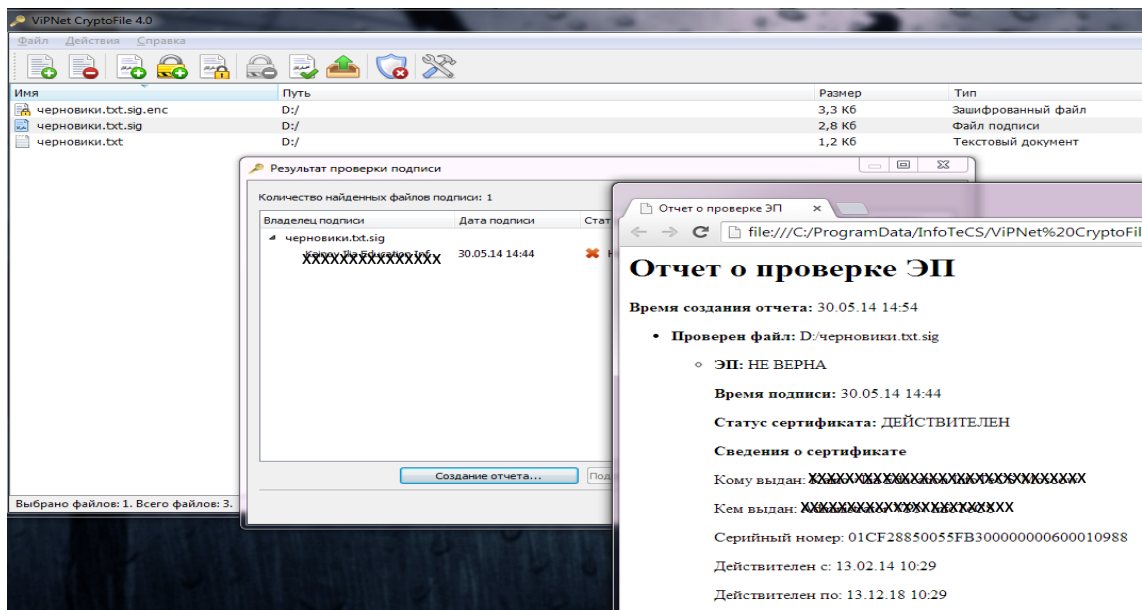
Использовать прикрепленную или открепленную подпись

В случае использования открепленной подписи электронная подпись помещается в контейнер, при этом исходный файл в данный контейнер не помещается, а передается другим пользователям отдельно.

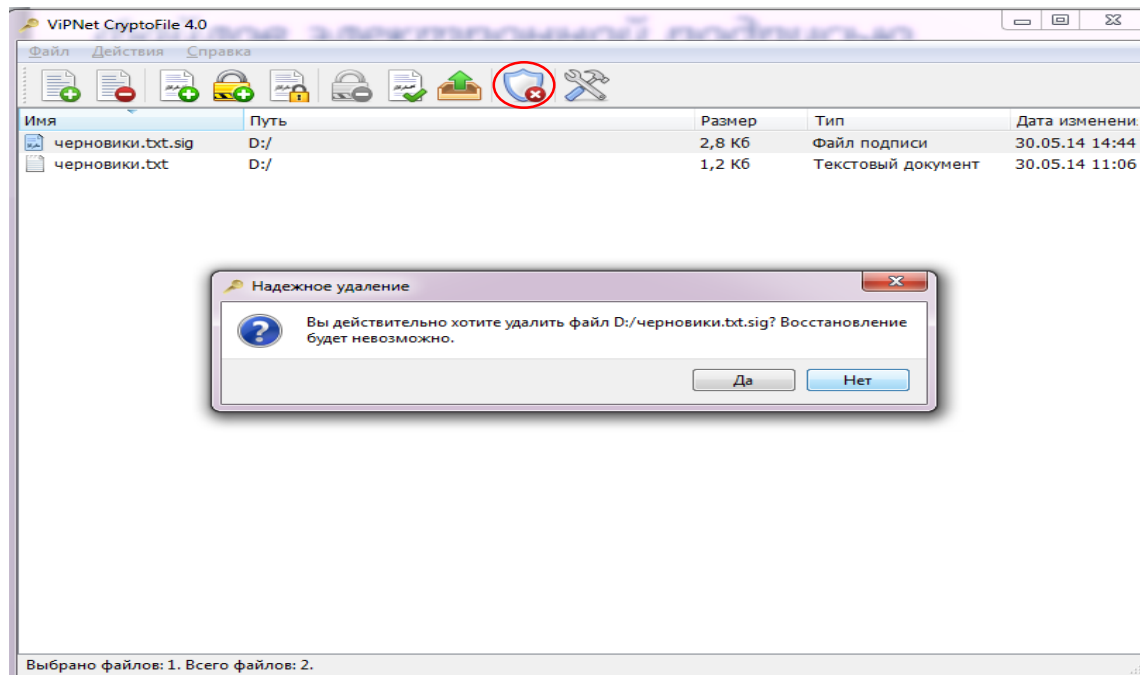
Открепленная подпись позволяет ознакомиться с содержимым исходного файла пользователям, на компьютерах которых не установлены средства работы с контейнерами.

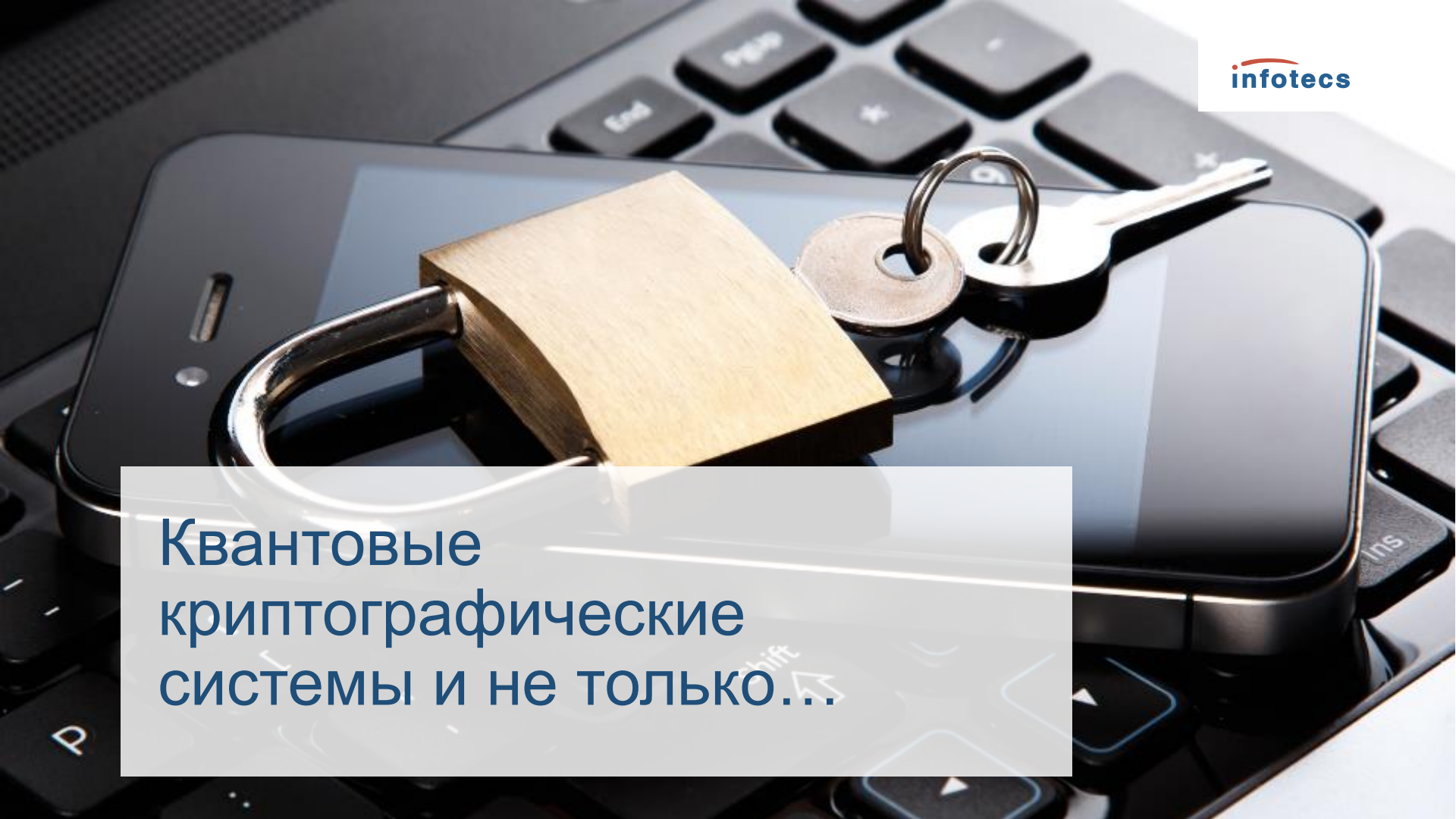
Однако в этом случае затрудняется передача, шифрование и другие операции с файлом подписи, так как операции необходимо производить с двумя файлами: исходным файлом и контейнером.

Создание отчетов о результатах проверки электронной подписи файла




Надежное удаление файлов



The background of the slide is a close-up photograph of a black smartphone lying on a black laptop keyboard. A large, brass-colored metal padlock is attached to the phone's charging port. A set of keys, including a circular metal fob and a standard metal key, is resting on the phone's screen. The lighting is dramatic, with strong highlights and shadows.

Квантовые
криптографические
системы и не только...

The background of the slide is a photograph of a landscape at sunset. In the foreground, several wind turbines are silhouetted against the bright orange and yellow sky. In the background, a series of high-voltage power lines stretch across the horizon. The sun is low on the horizon, creating a strong glow and casting long shadows.

Спасибо за
внимание!