Криптосистема ViPNet

УОНЦ ДПО ПТК «Учебный центр «ИнфоТеКС»

Ключевая система ViPNet

Ключевая система ViPNet

Виды шифрования в ViPNet

- **Шифрование на сетевом уровне:**
  - ✔ шифрование IP-трафика
  - ✔ шифрование сообщений программы ViPNet Деловая почта
  - ✔ шифрование прикладных и служебных конвертов
- **Шифрование на прикладном уровне:**
  - ✔ создание и проверка электронной подписи
  - ✔ шифрование в прикладных программах с помощью криптопровайдера ViPNet CSP

Ключевая система ViPNet

Типы ключей в ViPNet

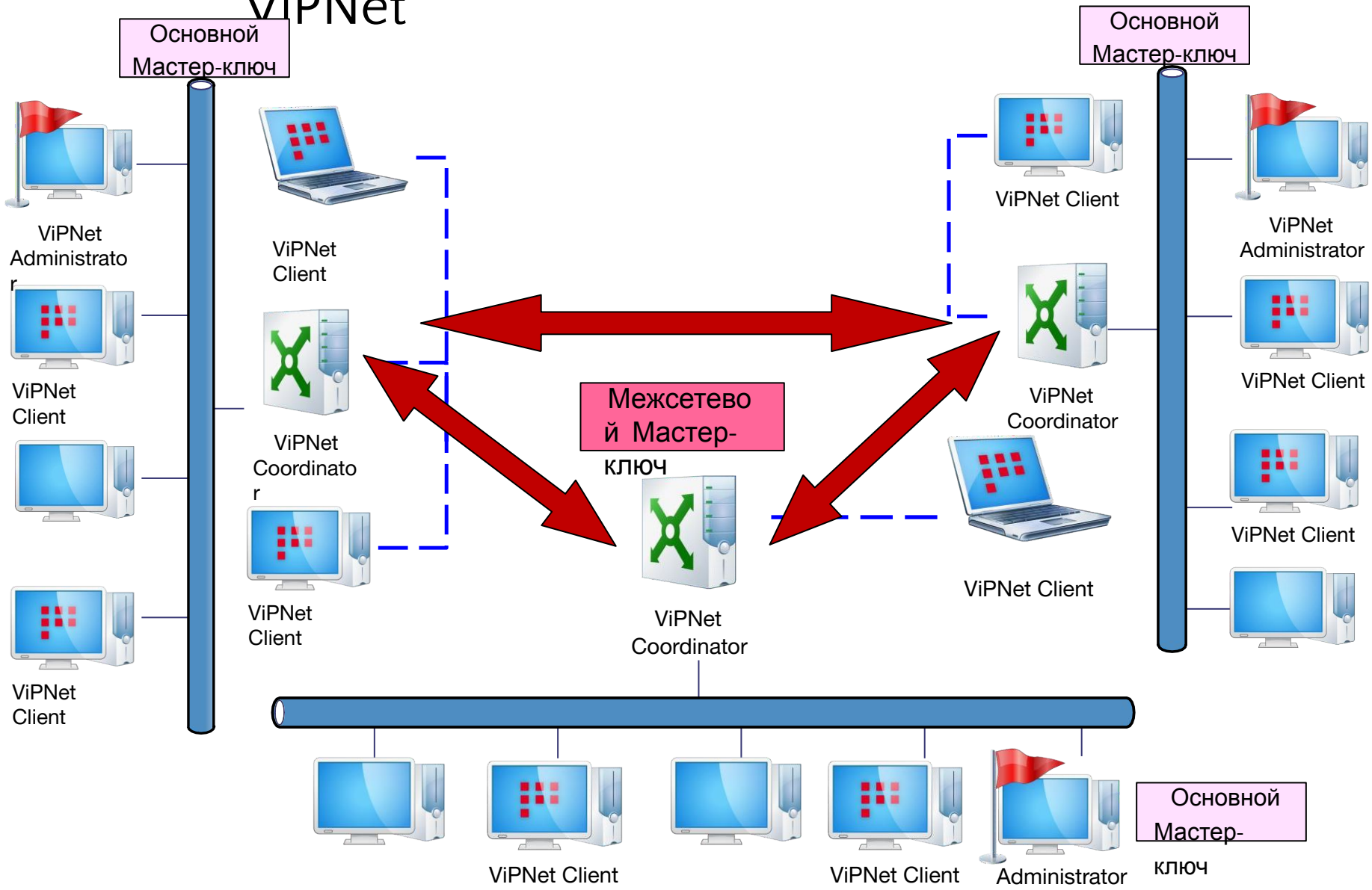
Мастер-ключи

Симметричные ключи шифрования

Асимметричные ключи шифрования

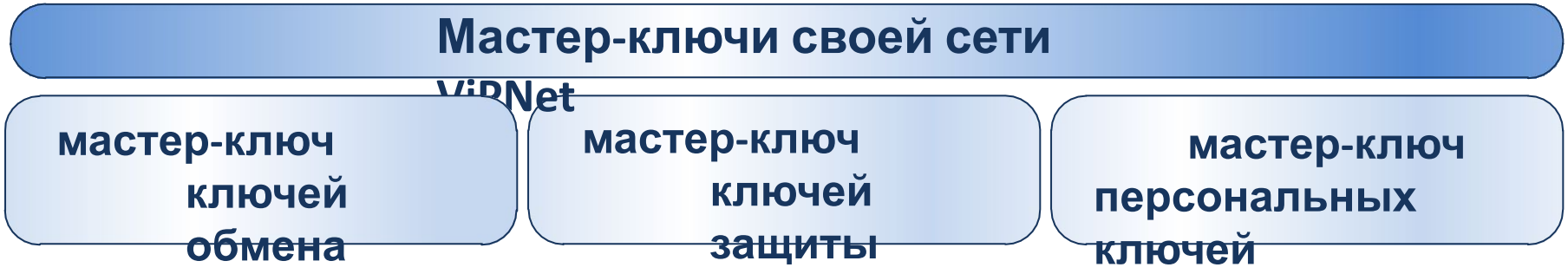
Асимметричные ключи ЭП

Типы мастер-ключей в ViPNet



Межсетевые мастер-ключи ViPNet

Основные мастер-ключи (мастер-ключи своей сети) ViPNet



- *формируются с помощью датчика случайных чисел*
- *хранятся в программе ViPNet Удостоверяющий и ключевой центр*
- *используются для формирования симметричных ключей*

Ключевая система ViPNet

Виды симметричных ключей

Ключи обмена

- *формируются на основе мастер-ключа ключей обмена*
- *используются для шифрования трафика между узлами ViPNet*
- *шифрование выполняется на случайных ключах, сделанных на основе ключей обмена, уникальных для каждого IP-пакета*
- *при хранении на сетевых узлах шифруются на специальных ключах защиты*

Ключевая система ViPNet

Применение ключей обмена

Ключевая система ViPNet

Виды симметричных ключей

Ключи защиты ключей обмена

- *формируются на основе мастер-ключа ключей защиты*
- *на этих ключах зашифрованы ключи обмена*
- *при хранении на сетевых узлах шифруются на персональных ключах*

Ключевая система ViPNet

Виды симметричных ключей

Персональные ключи

- *формируются на основе мастер-ключа персональных ключей*
- *используются для разграничения доступа нескольких пользователей сетевого узла к разной ключевой информации*
- *на этих ключах зашифрованы ключи защиты и другая ключевая информация, принадлежащая отдельному пользователю*
- *могут храниться как на внешнем устройстве, так и на сетевом узле*
- *при хранении шифруются на парольном ключе пользователя*

Ключевая система ViPNet

Виды симметричных ключей

Парольный ключ

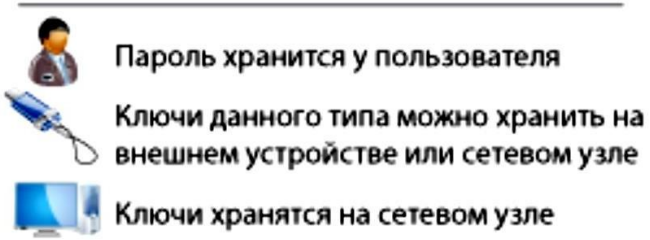
- *формируется путем вычисления значения хэш-функции пароля пользователя*
- *на парольном ключе зашифрованы персональные ключи пользователя*
- *может быть создан как централизованно в программе ViPNet УКЦ, так и пользователем на сетевом узле*

Ключевая система ViPNet

Защита ключевой

Для защиты ключей обмена применяется три уровня шифрования:

- *ключи обмена зашифрованы на ключах защиты*
- *ключи защиты зашифрованы на персональных ключах*
- *персональные ключи зашифрованы на парольных ключах*



Ключевая система ViPNet

Ключевая информация

Ключи

пользователя

Ключи узла

Дистрибутив ключей

Ключевая система ViPNet

Ключи пользователя ViPNet

Набор файлов, который создается в программе ViPNet Удостоверяющий и ключевой центр для каждого пользователя сети ViPNet. Содержит информацию, идентифицирующую пользователя и позволяющую ему работать с программным обеспечением ViPNet

Ключевая система ViPNet

Состав ключей пользователя ViPNet

Ключевая система ViPNet

Ключи пользователя ViPNet

- **Необходима смена ключей пользователя в случае:**
  - ✔ компрометация ключей пользователя
  - ✔ смена мастера персональных ключей
  - ✔ выдача ключей подписи пользователю
  - ✔ издание нового сертификата пользователя при истечении срока действия имеющегося у него закрытого ключа и соответствующего сертификата открытого ключа подписи

- **по умолчанию хранятся в каталоге ..\key_disk**

Ключевая система ViPNet

Ключи узла ViPNet

Набор файлов, который создается в программе ViPNet УКЦ для каждого узла сети ViPNet. Предназначены для шифрования передаваемого трафика и информации ViPNet-приложений, которой обмениваются сетевые узлы

Ключевая система ViPNet

Состав ключей узла ViPNet

- ключи обмена
- ключи защиты ключей обмена
- справочники сертификатов администраторов своей сети
- справочники сертификатов администраторов доверенных сетей
- списки отозванных сертификатов своей сети
- списки отозванных сертификатов доверенных сетей
- изданные кросс-сертификаты
- служебная информация

Ключевая система ViPNet

Ключи узла ViPNet

- **Необходима смена ключей узла в случае:**
  - ✔ добавление или удаление связи с другим сетевым узлом вашей сети ViPNet или доверенной сети
  - ✔ смена мастер-ключа обмена или мастер-ключа защиты
  - ✔ сменамежсетевого мастер-ключа, в случае, если текущий сетевой узел имеет связь с узлами доверенной сети
  - ✔ компрометация текущего сетевого узла
  - ✔ компрометация сетевого узла или пользователя, с которым установлена связь

- **по умолчанию хранятся в каталоге ..\d_station**

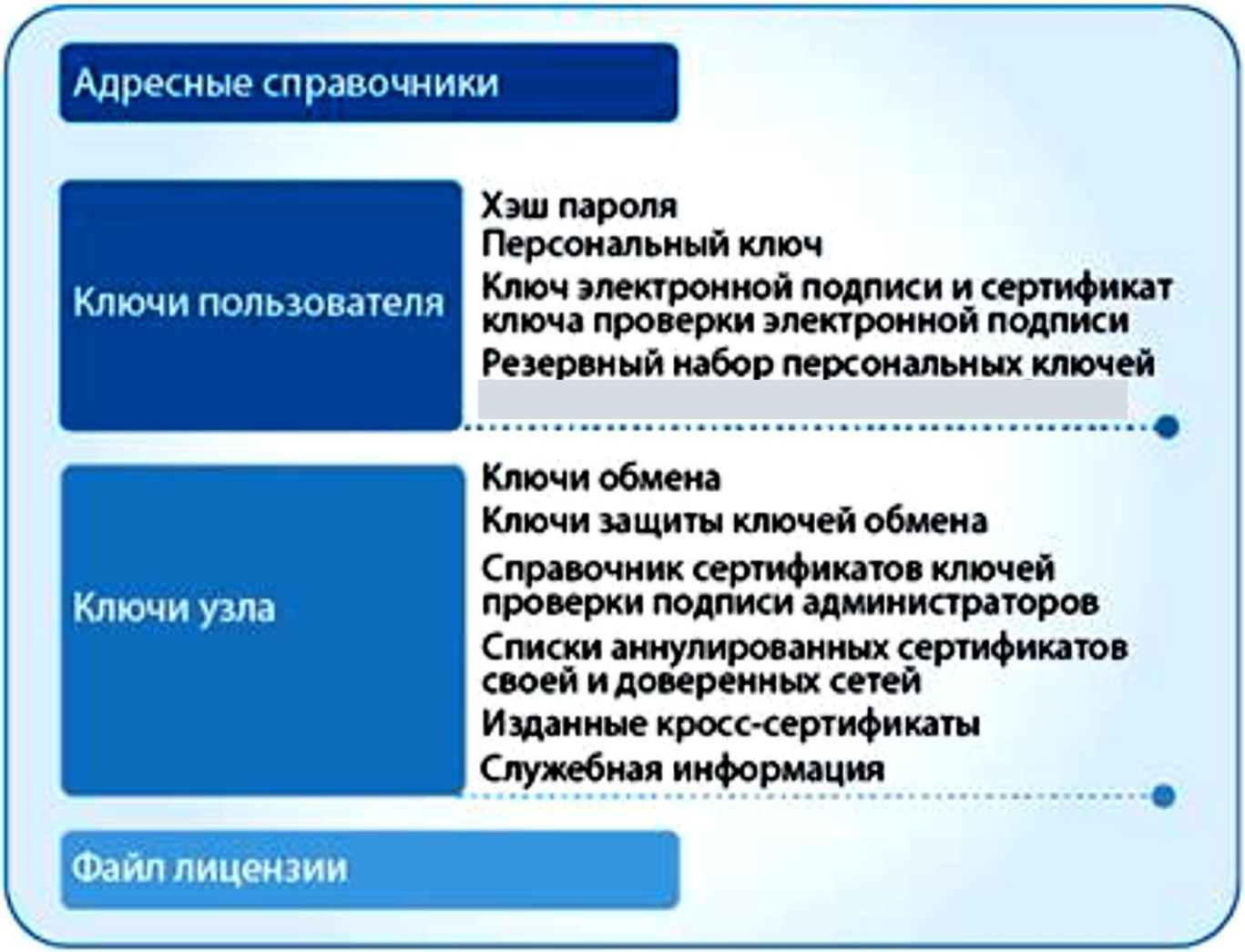
Ключевая система ViPNet

Дистрибутив ключей

Файл с расширением .dst, который создается в программе ViPNet УКЦ для каждого пользователя ViPNet и содержит все необходимое для развертывания рабочего места пользователя ViPNet на сетевом узле

Ключевая система ViPNet

Состав дистрибутива ключей



Ключевая система ViPNet

Дистрибутив ключей

- **Необходимо создание дистрибутива ключей в случае:**
  - ✔ добавления пользователя в сеть ViPNet
  - ✔ проблемы при функционировании узла пользователя в сети ViPNet, например, если произошла поломка компьютера и информация, хранившаяся на нем, была повреждена, и восстановить ее невозможно (в том числе справочники и ключи)
  - ✔ текущее состояние узла пользователя не позволяет выполнять отправку и прием зашифрованных писем, шифрование трафика, при этом удаленное обновление справочников и ключей по каким-либо причинам не может быть произведено

Компрометация ключей

Компрометация ключей

Компрометация ключей

Компрометацией ключей — *утрата доверия к тому, что используемые ключи не стали известны злоумышленникам и обеспечивают безопасность информации, то есть ее*

- ✔ *конфиденциальность*
- ✔ *целостность*
- ✔ *неотрекаемость (подтверждение авторства)*

Компрометация ключей

Явная компрометация

Явная компрометация — *события, когда факт компрометации стал доподлинно известен*

- ✔ *доступ к файлу дистрибутива ключей посторонних лиц*
- ✔ *утеря ключевых носителей*
- ✔ *утеря ключевых носителей с их последующим обнаружением*
- ✔ *увольнение сотрудников, имевших доступ к ключевой информации*
- ✔ *нарушение правил хранения и уничтожения (после окончания срока действия) закрытых ключей*

Компрометация ключей

Неявная компрометация

Неявная компрометация — *события, когда факт компрометации не является доподлинно установленным, однако вероятность того, что злоумышленники могли получить несанкционированный доступ к ключевой информации достаточна велика*

- ✔ *возникновение подозрений на утечку информации или ее искажение в системе конфиденциальной связи*
- ✔ *нарушение печати на сейфе с ключевыми носителями*
- ✔ *случаи, когда нельзя достоверно установить, что произошло с ключевыми носителями (в том числе случаи, когда ключевой носитель вышел из строя и не опровергнута возможность того, что это произошло в результате действий злоумышленника)*

Компрометация ключей

Компрометация в сетях ViPNet

Компрометация закрытого ключа

- **Выполняется при:**
  - ✔ утрате контейнера закрытого ключа
  - ✔ утрате дистрибутива ключей
  - ✔ увольнении сотрудника

Компрометация администратора сети

- **Выполняется при:**
  - ✔ утрате пароля или любой ключевой информации администратора сети ViPNet
  - ✔ возможности того, что посторонние лица могли получить доступ к компьютеру с установленным ViPNet УКЦ
  - ✔ увольнении администратора УКЦ

Компрометация ключей

Компрометация в сетях ViPNet

Компрометация пользователя

- **Выполняется при:**
  - ✔ утрате дистрибутива ключей, если дистрибутив не содержал резервного набора персональных ключей
  - ✔ увольнении сотрудника

Компрометация сетевого

- **Выполняется при:**
  - ✔ компрометации всех пользователей сетевого узла

Компрометация пользователя при утрате доверия к РНПК

- **Выполняется при:**
  - ✔ утрате носителя с РНПК
  - ✔ утрате дистрибутива, содержащего РНПК

Компрометация ключей

Резервный набор персональных ключей:

- *это набор из нескольких персональных ключей, который создается в программе ViPNet УКЦ для каждого пользователя сети ViPNet*
- ***используется при компрометации*** *или смене мастер-ключа персональных ключей и позволяет удаленно обновить ключи пользователя и ключи узла*
- *резервный набор ключей входит в состав первого дистрибутива ключей пользователя (dst-файла)*
- *файл с резервным набором ключей имеет вид AAAA.pk (где AAAA — идентификатор пользователя в сети ViPNet)*
- *по умолчанию резервный набор состоит из 20 персональных ключей*

Компрометация ключей

Резервный набор персональных ключей

- ***РНПК создается автоматически в случае:***
  - ✔ формирования самого первого дистрибутива ключей пользователя
  - ✔ формирования ключей пользователя при добавлении пользователя на узел, на котором уже имеются другие пользователи
  - ✔ смене мастер-ключа персональных ключей
  - ✔ формировании ключей после компрометации пользователя, если в текущем резервном наборе пользователя были скомпрометированы все ключи

- ***РНПК создается вручную в случае:***
  - ✔ повторного создания дистрибутива ключей для пользователя, при этом его содержание не изменяется, остается таким же, как и в предыдущих наборах, созданных автоматически

Компрометация ключей

Резервный набор персональных ключей

- ***при передаче РНПК пользователю рекомендуется:***
  - ✔ сохранять резервный набор на отдельном устройстве хранения данных
  - ✔ устройство с резервным набором передавать пользователю лично в руки либо по защищенному альтернативному каналу связи
  - ✔ после получения хранить резервный набор персональных ключей в безопасном месте, отдельно от других ключей (например, в сейфе)

Компрометация ключей

Действия при компрометации ключей

- ***при компрометации ключей пользователю следует:***
  - ✔ уведомить администратора сети ViPNet о факте и обстоятельствах компрометации
  - ✔ приостановить работу скомпрометированного узла до получения обновления при компрометации

- ***при компрометации ключей администратору сети ViPNet следует:***
  - ✔ провести процедуру компрометации ключей
  - ✔ высылать пользователю новые ключи, защищенные с помощью очередного варианта персонального ключа
  - ✔ провести служебное расследование