СЛУЖБА КРОВИ
государственная программа развития добровольного донорства

ФМБА России
Федеральное медико-биологическое агентство

Информационная безопасность в ЕИБД

Общие принципы и предстоящие изменения с введением в действие электронной подписи в ЕИБД

Технический эксперт

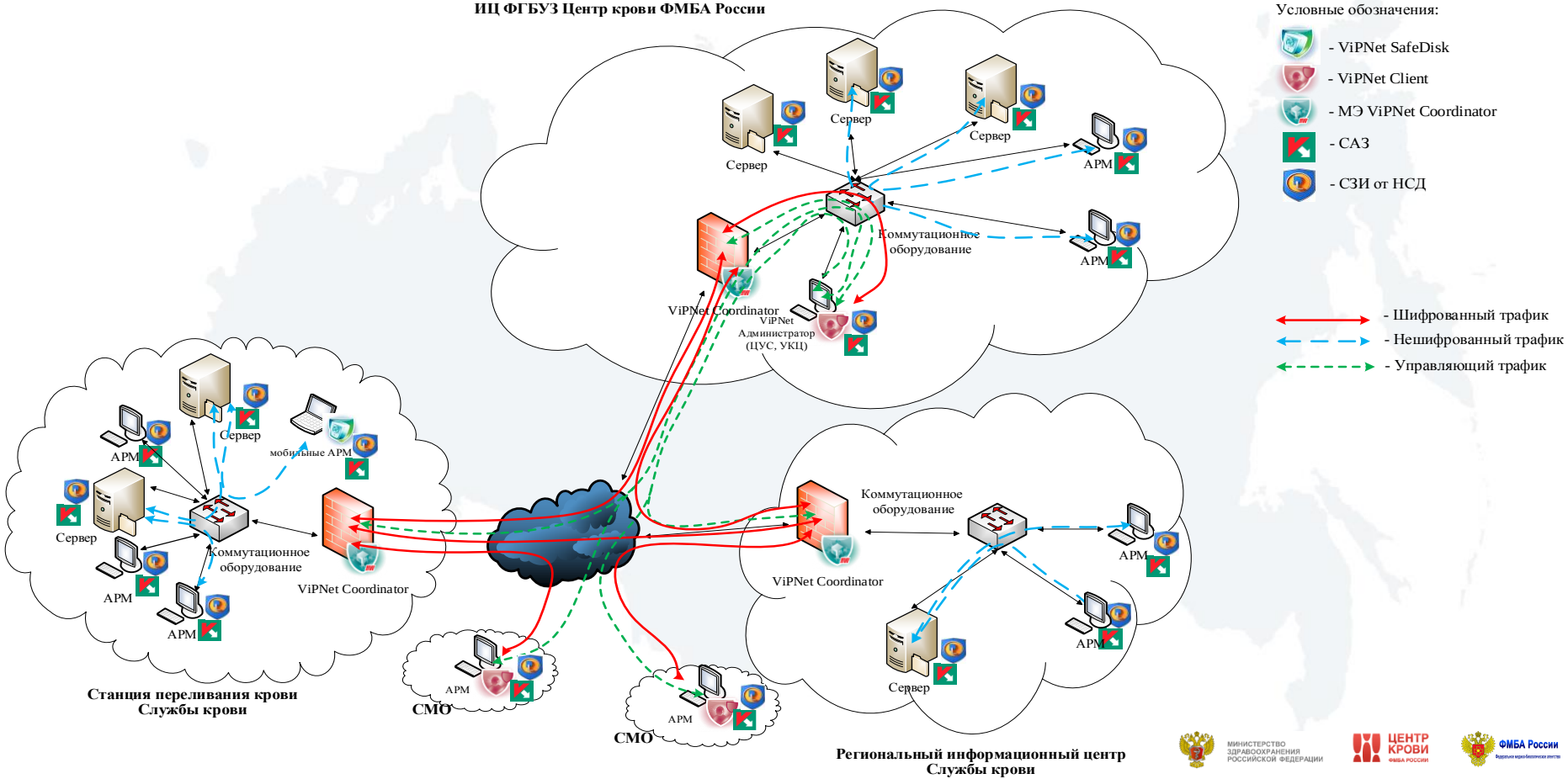
Шимоторов Сергей Александрович

Система защиты ЕИБД

Основные назначения системы защиты ЕИБД

- предотвращение неправомерного доступа, копирования, предоставления и(или) распространения информации и персональных данных
- исключение неправомерного уничтожения и(или) модифицирования информации и персональных данных
- исключение неправомерного блокирования информации и персональных данных
- обеспечение соответствия требованиям действующего законодательства Российской Федерации в сфере защиты информации

Система защиты ЕИБД



Аттестация по требованиям безопасности информации

Аттестат соответствия от 30.05.2018
Приказ ФСТЭК № 17 – К1 || Приказ ФСТЭК № 21 - УЗ2

ФИЦ ЦК ФМБА

Аттестат соответствия 2012 – 2017 г.
Приказ ФСТЭК № 17 – К2 || Приказ ФСТЭК № 21 – УЗ2

РИЦ | РИЦ | . . . . | РИЦ

Аттестат соответствия 2012 – 2017 г.
Приказ ФСТЭК № 17 – К2 || Приказ ФСТЭК № 21 – УЗ2

СПК | СПК | . . . . | СПК

Централизованные работы по аттестации объектов Службы крови



Требования к подключению новых объектов ЕИБД

Подключение учреждений, осуществляющих заготовку крови и её компонентов (СПК/ОПК), требования Приказа № 63 ФМБА России от 17.04.2015



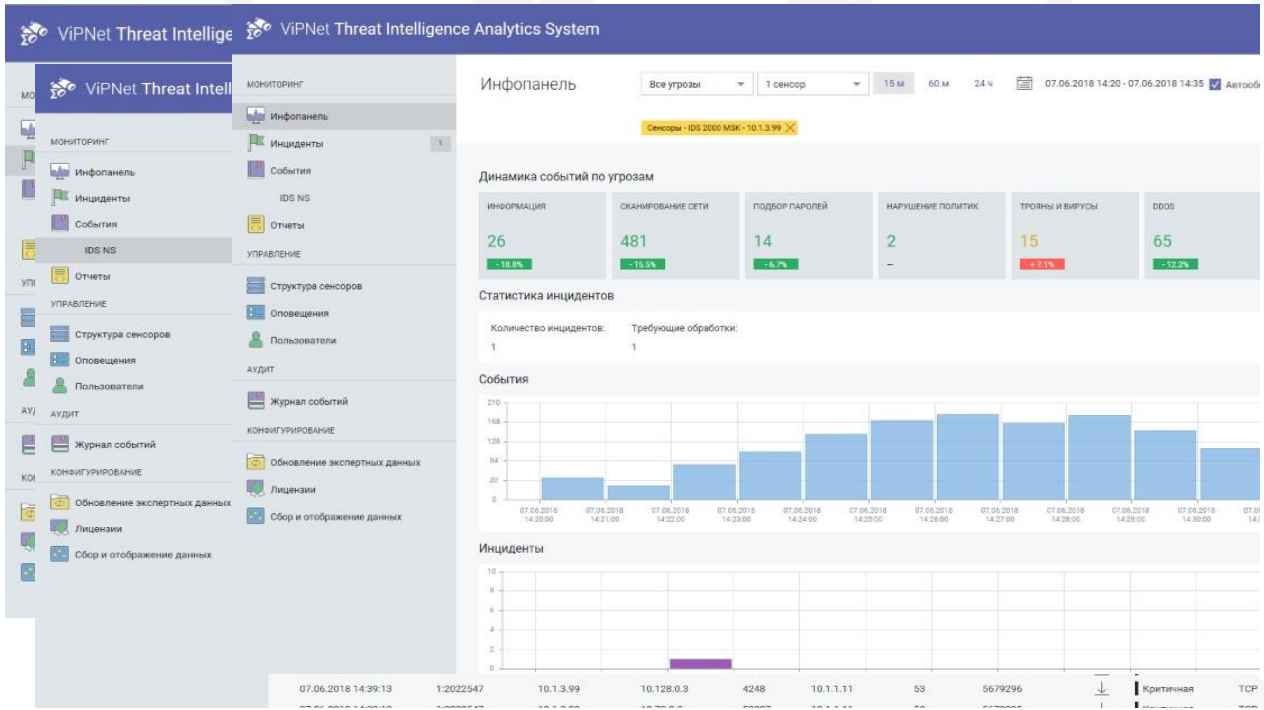
- Подключение осуществляется за счет **собственных** средств
- Требует организации защищенного VPN соединения с ЕИБД посредством подключения к сети **VipNet № 2029**
- Требует предоставления пакета документации по защите персональных данных и государственных информационных систем (Приказы 17 и 21 ФСТЭК России), а также актуального Аттестата соответствия
- Требует **успешного** прохождения процедур верификации ИТ-инфраструктуры и БД АИСТ (соответствие правилам кодирования и диапазонам), а также проверки качества данных в БД АИСТ (получение согласия со стороны РИЦ и Оператора системы принять новые данные)

Статус подключения СПК/ОПК



Анализ угроз информационной безопасности

ViPNet TIAS (Threat Intelligence Analytics System) — программно-аппаратный комплекс предназначенный для автоматического выявления инцидентов на основе анализа событий информационной безопасности.



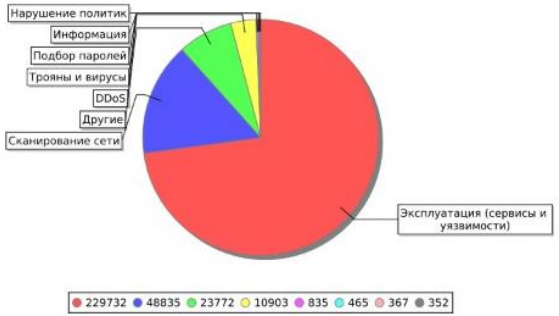
Статистика по событиям

Распределение событий по категориям угроз

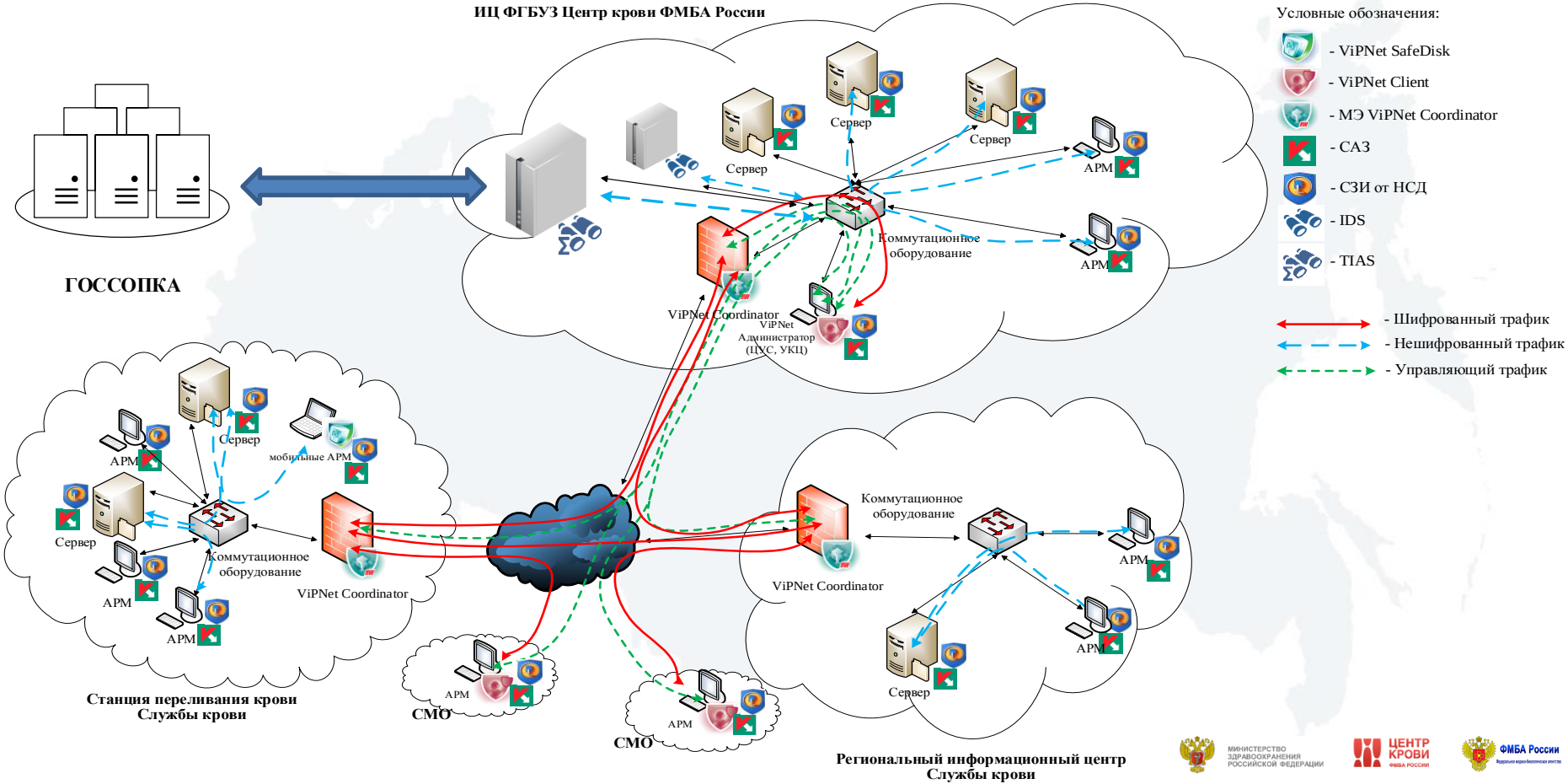
События с 23.04.18 0:00 по 24.04.18 23:59

Организации : СК ФМБА

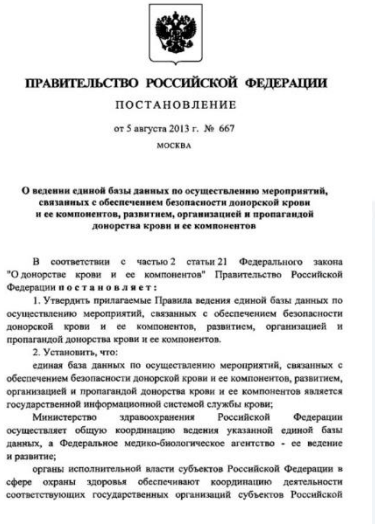
Наименование	Количество
Эксплуатация (сервисы и уязвимости)	229732
Сканирование сети	48835
Другие	23772
DDoS	10903
Трояны и вирусы	835
Подбор паролей	465
Информация	367
Нарушение политик	352



Анализ угроз ИБ и интеграция с ГосСОПКА



Предпосылки использования средств ЭП в ЕИБД



ПРАВИТЕЛЬСТВО РОССИЙСКОЙ ФЕДЕРАЦИИ

ПОСТАНОВЛЕНИЕ

от 5 августа 2013 г. № 667

МОСКВА

О ведении единой базы данных по осуществлению мероприятий, связанных с обеспечением безопасности донорской крови и ее компонентов, развитием, организацией и пропагандой донорства крови и ее компонентов

В соответствии с частью 2 статьи 21 Федерального закона "О донорстве крови и ее компонентов" Правительство Российской Федерации п о с т а н о в л я е т :

1. Утвердить прилагаемые Правила ведения единой базы данных по осуществлению мероприятий, связанных с обеспечением безопасности донорской крови и ее компонентов, развитием, организацией и пропагандой донорства крови и ее компонентов.

2. Установить, что:

единая база данных по осуществлению мероприятий, связанных с обеспечением безопасности донорской крови и ее компонентов, развитием, организацией и пропагандой донорства крови и ее компонентов является государственной информационной системой службы крови;

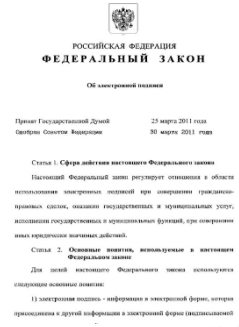
Министерство здравоохранения Российской Федерации осуществляет общую координацию ведения указанной единой базы данных, а Федеральное медико-биологическое агентство - ее ведение и развитие;

органы исполнительной власти субъектов Российской Федерации в сфере охраны здоровья обеспечивают координацию деятельности соответствующих государственных организаций субъектов Российской

Постановление Правительства РФ от 05.08.2013 N 667 "О ведении единой базы данных по осуществлению мероприятий, связанных с обеспечением безопасности донорской крови и ее компонентов, развитием, организацией и пропагандой донорства крови и ее компонентов»

9. Информация, необходимая для ведения базы данных донорства крови и ее компонентов, представляется в виде электронного документа, подписанного **электронной подписью**, или документа на бумажном носителе, форма которого утверждается Министерством здравоохранения Российской Федерации.

Применение средств электронной подписи в ЕИБД



РОССИЙСКАЯ ФЕДЕРАЦИЯ

ФЕДЕРАЛЬНЫЙ ЗАКОН

Об электронной подписи

Принят Государственной Думой 25 марта 2011 года

Одобрен Советом Федерации 30 марта 2011 года

Статья 1. Сфера действия настоящего Федерального закона

Настоящий Федеральный закон регулирует отношения в области использования электронных подписей при совершении гражданско-правовых сделок, оказании государственных и муниципальных услуг, исполнении государственных и муниципальных функций, при совершении иных юридически значимых действий.

Статья 2. Основные понятия, используемые в настоящем Федеральном законе

Для целей настоящего Федерального закона используются следующие основные понятия:

1) электронная подпись - информация в электронной форме, которая присоединена к другой информации в электронной форме (подписываемой

Электронная подпись - информация в электронной форме, которая присоединена к другой информации в электронной форме (подписываемой информации) или иным образом связана с такой информацией и которая используется для определения лица, подписывающего информацию

Средства электронной подписи - шифровальные (криптографические) средства, используемые для подтверждения и шифрования сведений передаваемых в информационной системе

Криптографический провайдер

Криптографический провайдер обеспечивает сертифицированную ФСБ реализацию криптографических алгоритмов ГОСТ

Электронный идентификатор

Электронный идентификатор представляет собой защищенное хранилище ключа электронной подписи

Криптографический клиент

Криптографический клиент обеспечивает выполнение операций подписи и шифрования

Удостоверяющий центр ЦК

Удостоверяющий центр предназначен для создания и управления сертификатами ключа проверки электронной подписи



Формирование запроса на сертификат

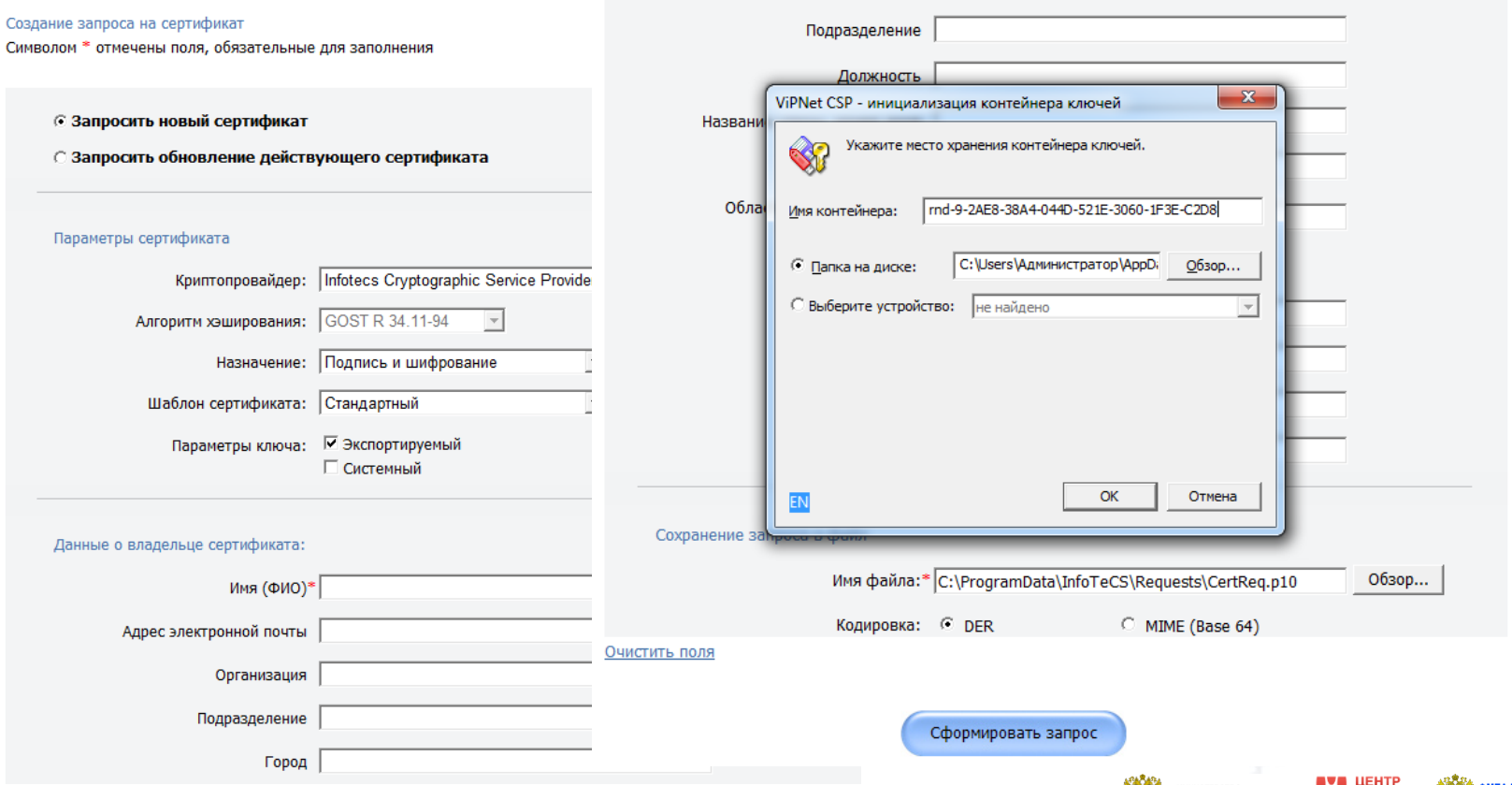
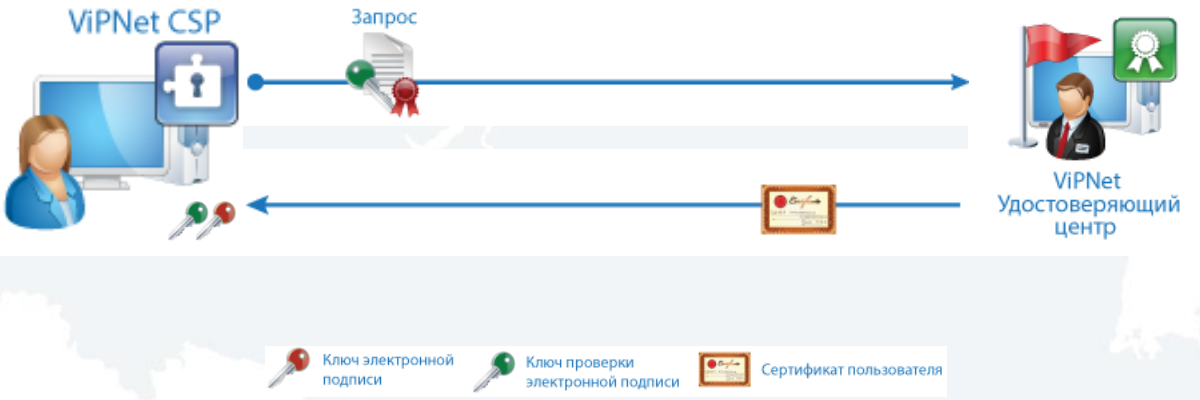


Схема получения сертификата

Получение сертификата по запросу из ViPNet CSP



Использование электронной подписи

Алгоритм получения сертификата ключа проверки электронной подписи (СКП ЭП) состоит из следующих этапов:

- Заявитель с использованием средств электронной подписи осуществляет генерацию ключа электронной подписи (КЭП) и запрос на сертификат ключа проверки электронной подписи (СКП ЭП) на своем рабочем месте
- Заявитель формирует, заверяет и направляет почтовым отправлением необходимый набор заявительных документов, перечисленных в Регламенте Удостоверяющего центра (УЦ)
- Заявитель отправляет запрос на сертификат по электронной почте в УЦ
- УЦ осуществляет проверку заявительных документов, корректность запроса на сертификат, издает сертификат, публикует сертификат на информационном ресурсе удостоверяющего центра

Состав документов необходимый для получения сертификата

Документы, позволяющие УЦ идентифицировать субъект/организацию, включают в себя:

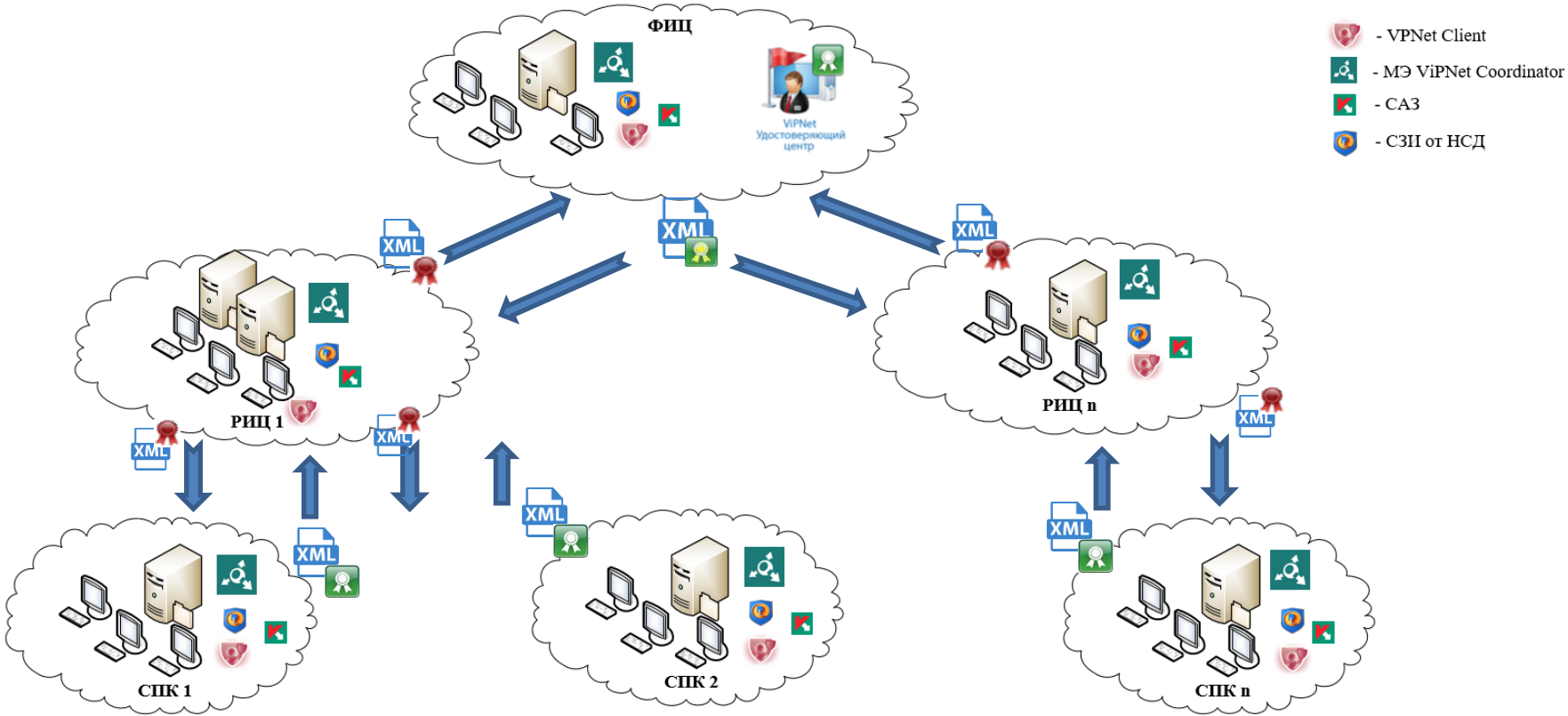
Документы, идентифицирующие субъект – физическое лицо:

- Заявление
- Копия паспорта

Документы, идентифицирующие организацию:

- Копия свидетельства ОГРН
- Копия свидетельства ИНН
- Копия документа подтверждающего полномочия руководителя ОПК/СПК
- Копия документа подтверждающего полномочия сотрудника по внесению информации в ЕИБД

Реализованный функционал электронной подписи



СЛУЖБА КРОВИ
государственная программа развития добровольного донорства

ФМБА России
Федеральное медико-биологическое агентство

Спасибо за внимание!