ИНФОТЕКС
ТРАСТ

Решение по защите биометрических данных для ЕБС на примере сервисов Инфотекс Интернет Траст

ИНФОТЕКС
ТРАСТ

РЕГИСТРАЦИЯ БИОМЕТРИЧЕСКИХ ОБРАЗЦОВ В ЕБС

Защита биометрических ПДн при работе с ЕБС

№152-ФЗ
№149-ФЗ

Федеральный закон
от 31.12.2017 №482-ФЗ

Постановление правительства №1119
Классификация ИСПДн

Минкомсвязь
ст. 14.1 №149-ФЗ и ПП №335

— регулирование в сфере идентификации граждан РФ на основе БПДн
— определение требований к информационным технологиям (ИТ) и техническим средствам (ТС)

ЦБ РФ
ст. 14.1 №149-ФЗ

— контроль за выполнением банками организационно-технических мер по обеспечению безопасности ПДн
— определение перечня угроз безопасности при работе ЕБС

№378
приказ ФСБ
Определение требований к СКЗИ

№21
приказ ФСТЭК
Определение угроз ИБ и мер по защите

Приказ №321
Минкомсвязи
Порядок работы с ЕБС

Указание ЦБ
№4859-У
Определение перечня угроз

Методические рекомендации по нейтрализации банками угроз безопасности <...>
№4-МР от 14.02.2019

Применение надзорных мер

ЦЕНТРАЛЬНЫЙ БАНК
РОССИЙСКОЙ ФЕДЕРАЦИИ
(Банк России)

ПЕРВЫЙ ЗАМЕСТИТЕЛЬ ПРЕДСЕДАТЕЛЯ

107016, Москва, ул. Неглинная, 12
www.cbr.ru
тел. (495) 771-91-00

от 28.06.2018 № ИН-03-13/40

на № _____ от _____

Информационное письмо об особенностях
применения мер к банкам
при совершении ими действий,
предусмотренных пунктом 5^6 статьи 7
Федерального закона от 7 августа 2001 года
№ 115-ФЗ «О противодействии легализации
(отмыванию) доходов, полученных преступным
путем, и финансированию терроризма»

В соответствии с информационным письмом Банка России от 28.06.2018 № ИН-03-13/40, банки обязаны регистрировать клиентов — физических лиц в ЕБС во внутренних структурных подразделениях (ВСП) в каждом субъекте присутствия:

- не менее чем в 20% ВСП (не менее 1 ВСП в регионе) — по состоянию на 31 декабря 2018 года ⁘
- не менее чем в 60% ВСП — по состоянию на 30 июня 2019 года
- во всех ВСП —на 31 декабря 2019 года

⁘ банк обеспечивает принятие организационно-технических мер защиты информации от угроз безопасности, актуальных при обработке, включая сбор и хранение, биометрических персональных данных, их проверку и иные меры из числа установленных Банком России кроме случаев, предусмотренных абзацем 12 настоящего информационного письма

Применение надзорных мер

Рекомендуется обеспечивать функционирование объектов информационной инфраструктуры для выполнения действий по контролю целостности и подтверждения подлинности электронных сообщений путем их подписания УКЭП банка средствами электронной подписи класса не ниже КВ2 **любым из следующих способов**:

- с использованием собственного решения
- с использованием типового решения
- с использованием решения поставщика услуг (облачного решения) при наличии такого решения на рынке информационных технологий

* подпункт 2.3.8 Методических рекомендаций по нейтрализации банками угроз безопасности при сборе и хранении биометрических данных от 14.02.2019 №4-МР

Способы построения корректного взаимодействия с ЕБС при использовании СЭП класса КВ2

Использование типового решения, согласованного с ФСБ России

Построение собственного решения с учетом:

– требований законодательства
– особенностей инфраструктуры банка
– разработанной в банке модели угроз
– необходимости реализации верификации
– возможности выделения бизнес-процесса сбора БО в отдельный контур

Использование облачного решения, согласованного с ФСБ России

+ криптографическая аутентификация банка
+ подписание сообщений сотрудниками

В случае функционирования объектов информационной инфраструктуры с использованием «собственного» решения

Рекомендуется обеспечивать:

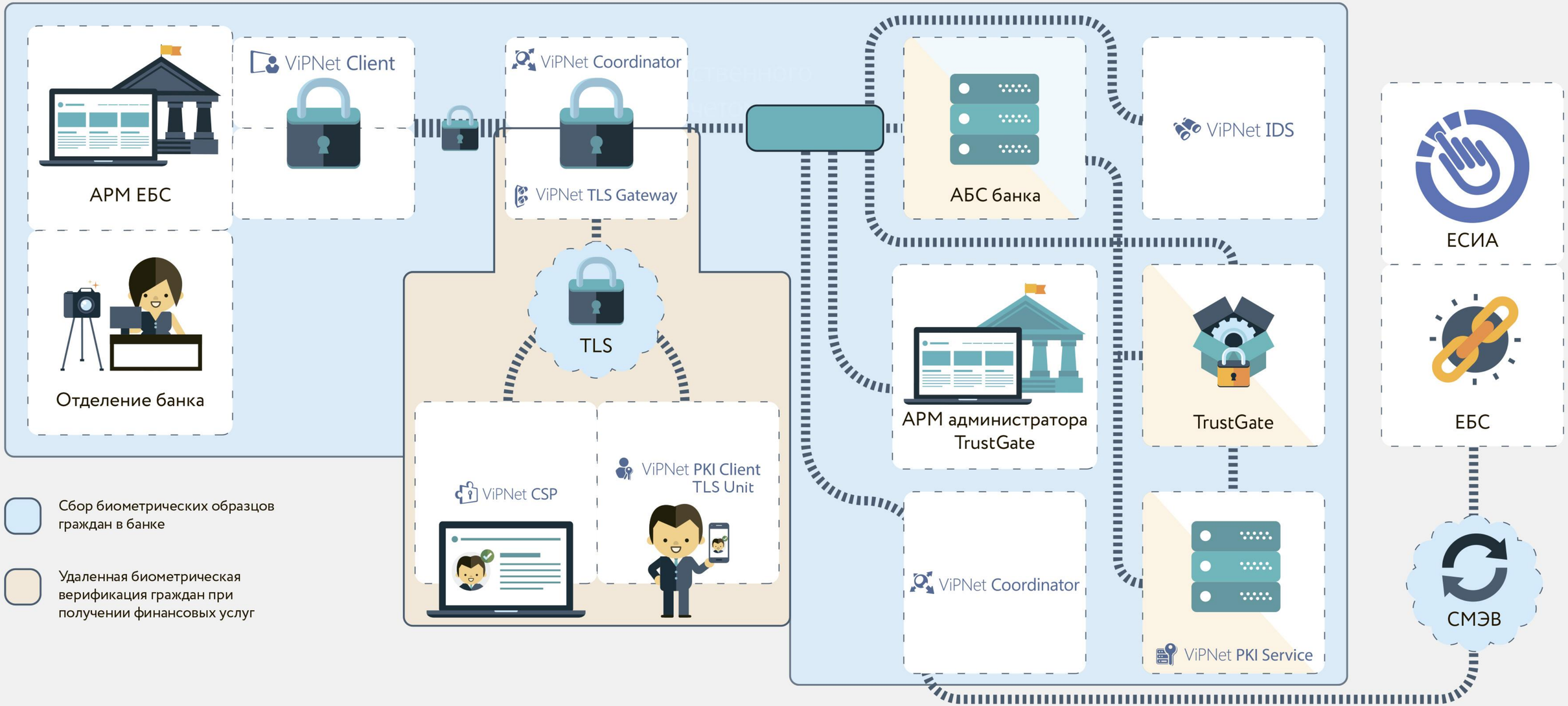
- получение СКЭП, созданного ГУЦ с применением средств класса не ниже КВ2
- встраивание в подсистему обработки БПДн программно-аппаратного модуля криптографической защиты, сертифицированного в качестве СКЗИ класса КВ/СЭП по классу КВ2
- Создание и использование доверенной среды функционирования информационной системы, взаимодействующей с программно-аппаратным модулем криптографической защиты

Доверенная среда функционирования информационной системы

Создание доверенной среды обеспечивается:

- использованием ППО на сертифицированной операционной системе
- применением средств межсетевого экранирования
- применением средств защиты от компьютерных атак
- применением АПМДЗ уровня платы расширения
- использованием прошедшего проверку на анализ уязвимостей ППО
- проведением тематических исследований по оценке влияния ППО на СКЗИ/СЭП
- разработкой эксплуатационной документации на объекты информационной инфраструктуры

Обеспечение безопасности биометрических ПДн граждан на всех этапах функционирования ЕБС



ИНФОТЕКС ТРАСТ

Комплексный подход к реализации регистрации биометрических образцов в ЕБС

Прикладное ПО и СКЗИ	**ПО TrustGate** — сбор и проверка качества биометрических образцов (БО) — взаимодействие с ЕСИА — регистрация БО в ЕБС	**СКЗИ для защиты каналов по КС2/КС3** — компоненты сетей ViPNet — ViPNet TLS Gateway и ViPNet PKI Client	**СЭП для подписи БО по КВ2** — ПАК ViPNet PKI Service
Построение КСЗИ и оценка соответствия требованиям ИБ	**Указание Банка России №4859-У** — защита каналов связи по КС2/КС3 — подпись собранных биометрических образцов по КВ (с обязательной оценкой влияния прикладного ПО на СКЗИ ViPNet PKI Service)	**Приказ Минкомсвязи №321 от 25.06.2018** — аттестация ИСПДн — проведение ежегодной оценки соответствия требованиям	**ГОСТ Р 57580.1-2017** **Подсистемы КСЗИ:** — управления доступом — антивирусной защиты — межсетевого экранирования — обеспечения целостности БПДн, передаваемых в ЕБС — обнаружения вторжений — анализа защищенности
Необходимые компетенции	Лицензии ФСБ России и ФСТЭК России	Опыт разработки прикладных систем с учетом требований регуляторов	Опыт тематических исследований и сертификации прикладных систем и СЗИ

ИНФОТЕКС ТРАСТ

Преимущества нашего решения

- Типовое решение согласовано ФСБ России
- СПО Trust Gate имеет положительное заключение по оценке влияния на ViPNet PKI Service
- Глубокая проработанность в связи с наличием требующих компетенций в рамках ГК «ИнфоТеКС» (СЭП КВ2, МСЭ , IDS, аккредитованная лаборатория, оценка соответствия по ГОСТ Р 57580.2)
- Отсутствие жестких ограничений по варианту реализации относительно Рекомендаций 4-МР («собственное» и/или ««типовое)
- Преимущества ПАК ViPNet PKI Service перед набором компонент от конкурента

ИНФОТЕКС ТРАСТ

Спасибо за внимание!

Вопросы?

ОАО «Инфотекс Интернет Траст»

Антон Сергеевич Мелузов
Руководитель департамента развития услуг и продуктов
к.ф.-м.н.
+7 967 294-58-60

Москва, Старый Петровско-
Разумовский проезд, 1/23, стр. 1

8 800 250-8-265
iitrust.ru