20/02/2019

ИБ БАНКОВ ПРИ РАБОТЕ С ЕБС

РАЗБОР МЕТОДИЧЕСКИХ РЕКОМЕНДАЦИЙ ЦБ

Андрей Янкин

Директор Центра информационной безопасности
Email: av.yankin@jet.msk.su, тел: +7(926)159-86-94

О ЧЕМ РЕЧЬ?

ЦЕНТРАЛЬНЫЙ БАНК РОССИЙСКОЙ ФЕДЕРАЦИИ
(БАНК РОССИИ)

Методические рекомендации
по нейтрализации банками угроз безопасности, актуальных при обработке, включая сбор и хранение, биометрических персональных данных, их проверке и передаче информации о степени их соответствия предоставленным биометрическим персональным данным гражданина Российской Федерации

14.02.2019 № 4-МР

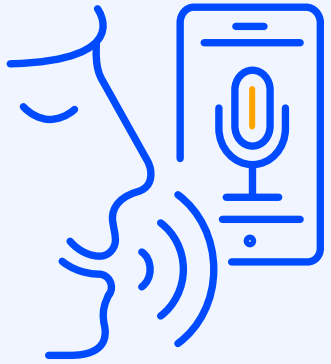
РАСПРЕДЕЛЕНИЕ РОЛЕЙ

Банк

Первичный сбор БДн

Использование сервисов ЕБС и ЕСИА

Ростелеком



Единая биометрическая система (ЕБС)

Хранение БДн

Сервисы идентификации и аутентификации

госуслуги

Единая система идентификации и аутентификации (ЕСИА)

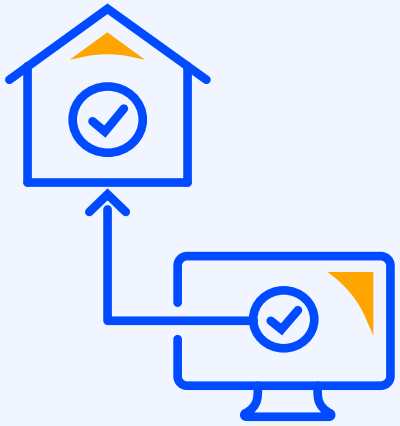
Сервисы идентификации и аутентификации на базе Госуслуг

ТЕХНОЛОГИЧЕСКИЕ УЧАСТКИ: ПЕРВИЧНЫЙ СБОР БДН

ТУ сбора
Первичный сбор БДн физических лиц

ТУ передачи
Передача БДн между структурными подразделениями банка

ТУ обработки
Обработка БДн перед передачей в ЕБС



ТУ передачи
Передача БДн в ЕБС через СМЭВ

ТЕХНОЛОГИЧЕСКИЕ УЧАСТКИ: ТУ ОБРАБОТКИ

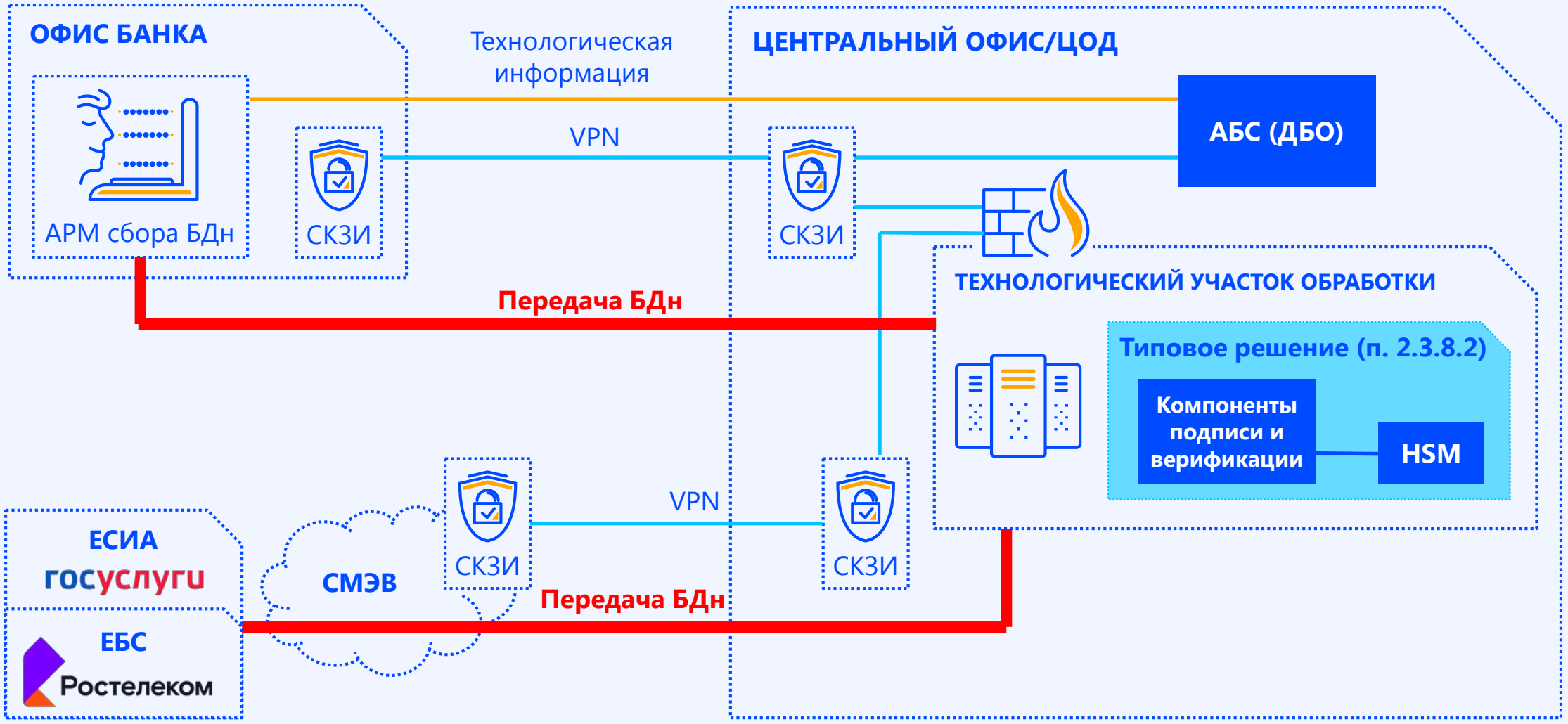
Удостоверение, контроль целостности, подтверждение подлинности – **СКЗИ класса КВ**

Самостоятельно

Типовое решение

Облачное решение

ТЕХНОЛОГИЧЕСКИЕ УЧАСТКИ: ПЕРВИЧНЫЙ СБОР БДН



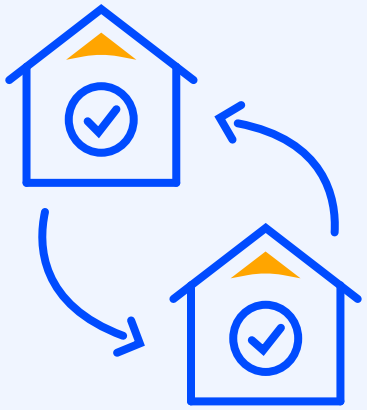
ТЕХНОЛОГИЧЕСКИЕ УЧАСТКИ: УДАЛЕННАЯ ИДЕНТИФИКАЦИЯ

ТУ взаимодействия с клиентом

Мобильное приложение, портал ДБО и т.п.

ТУ удаленной идентификации

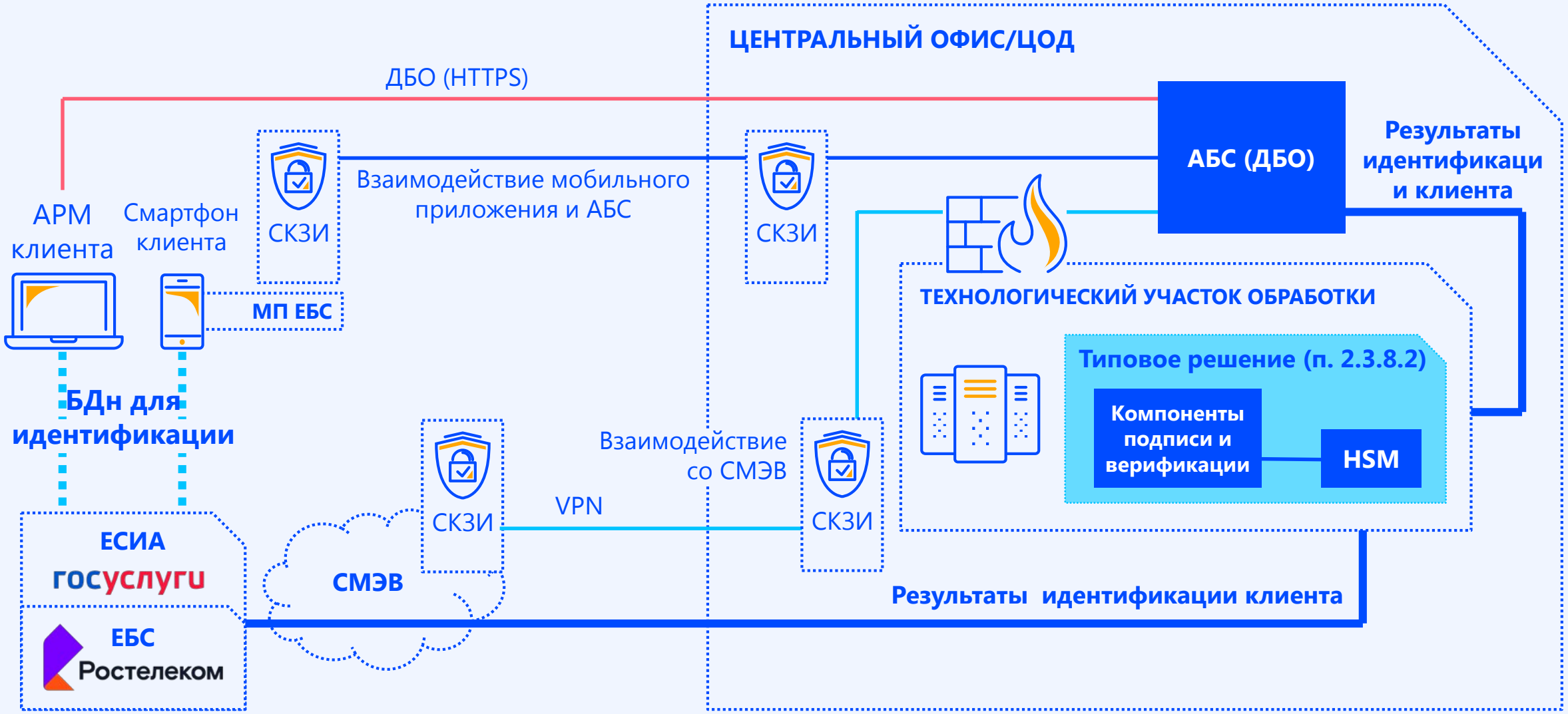
Проверка результатов удаленной идентификации с использованием ЕСИА



ТУ взаимодействия с ЕСИА и ЕБС

Взаимодействие с ЕСИА и ЕБС через СМЭВ

УДАЛЕННАЯ ИДЕНТИФИКАЦИЯ



УДАЛЕННАЯ ИДЕНТИФИКАЦИЯ: МОБИЛЬНОЕ ПРИЛОЖЕНИЕ

Свое приложение

Анализ уязвимостей и контроль **НДВ**

или

Анализ уязвимостей **ОУД4** (ГОСТ Р 15408-3-2013)

Готовое решение

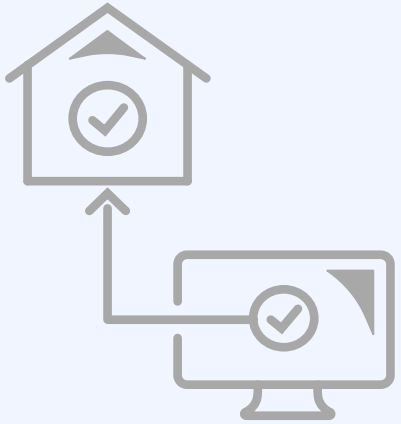
Ключ - Ростелеком

ОБЩИЕ ТРЕБОВАНИЯ ПО ИБ

ТУ сбора

ТУ передачи

ТУ обработки



ТУ передачи

ГОСТ Р 57580.1-2017
Безопасность финансовых (банковских) операций. Защита информации финансовых организаций. Базовый состав организационных и технических мер – более **300 требований**

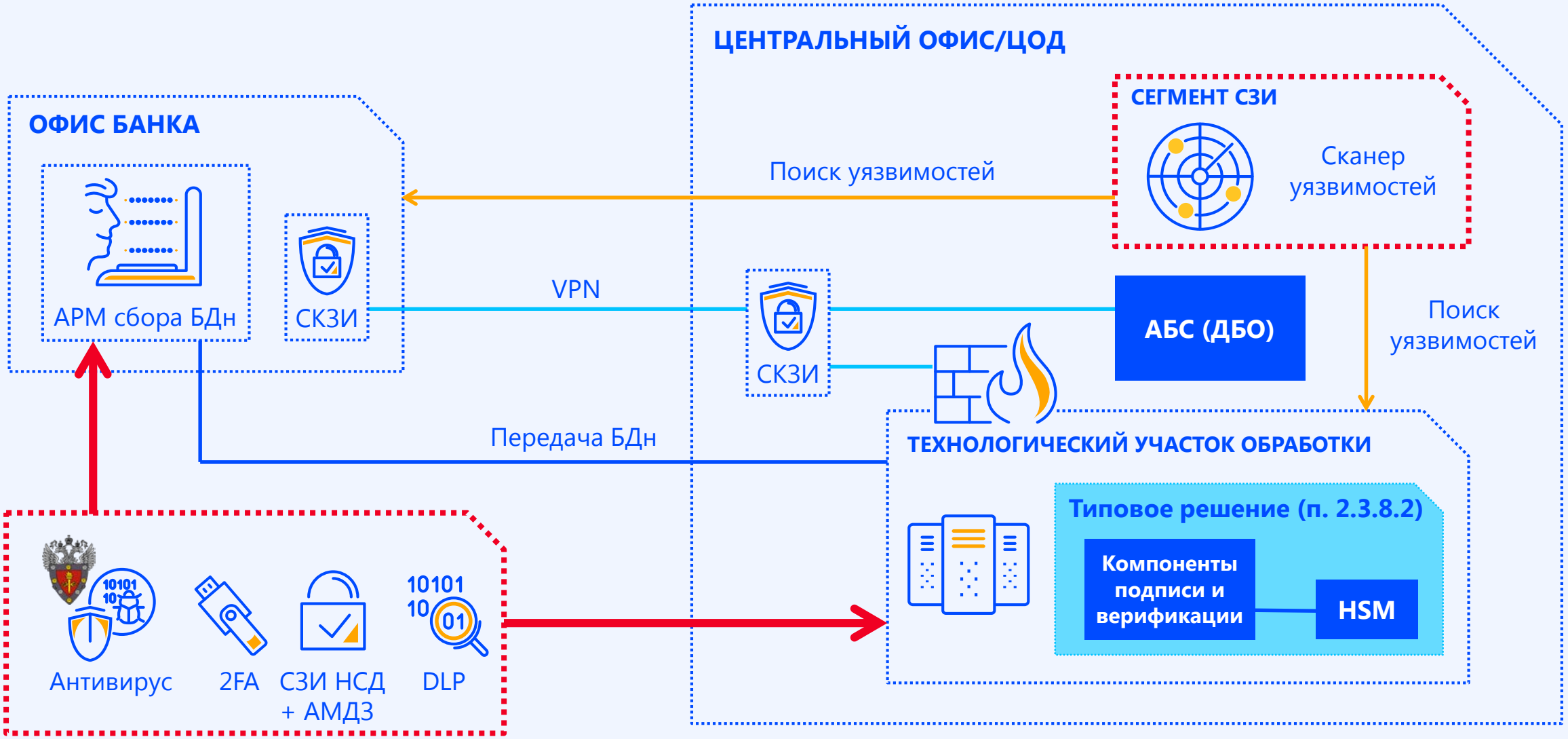
\+ **Выделенные сетевые сегменты** \+ **Сертифицированные СЗИ**

ОБЩИЕ ТРЕБОВАНИЯ ПО ИБ

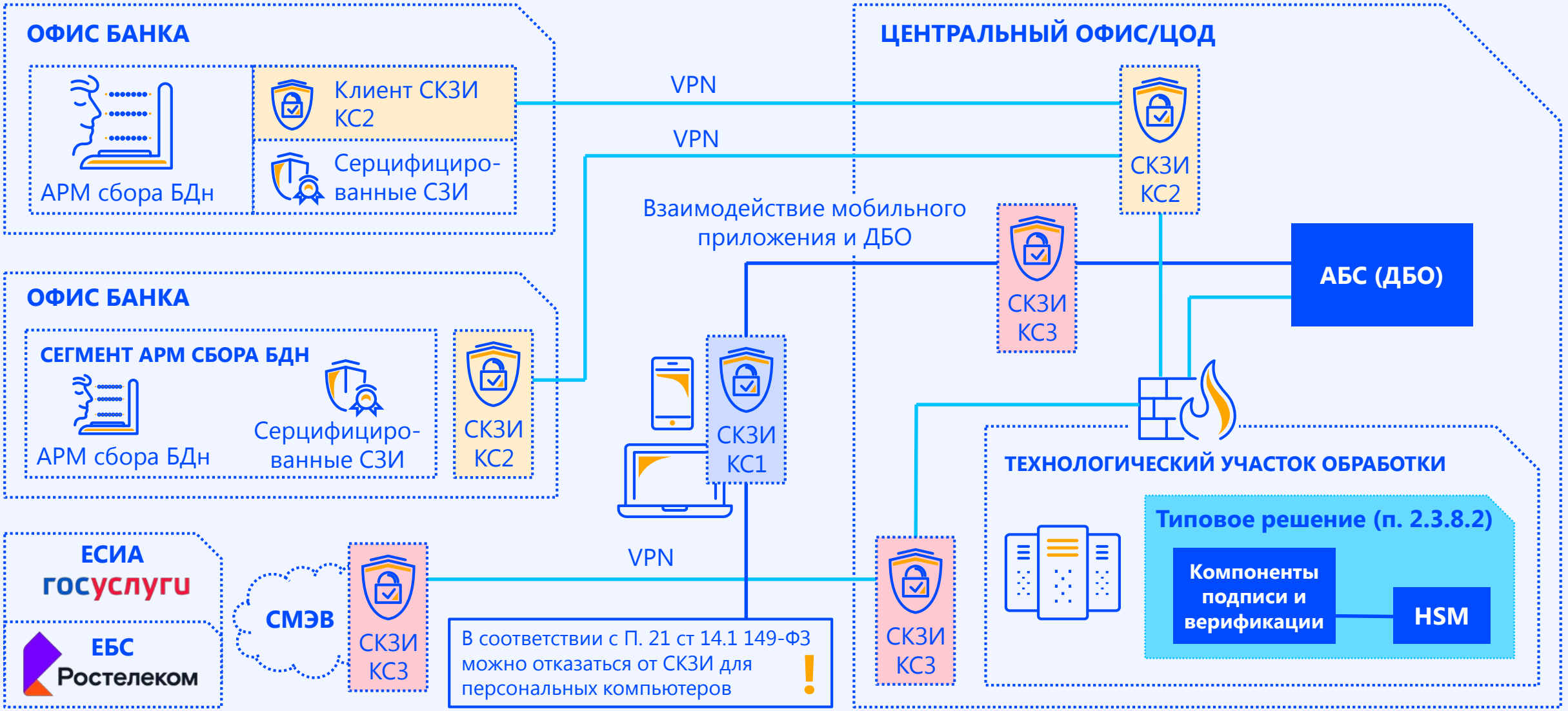
	ГОСТ Р 57580.1-2017		Сертифицированные СЗИ: • СЗИ от НСД • Антивирус • МЭ • СОВ	
	ТУ сбора	**ТУ обработки**	**ТУ сбора**	**ТУ обработки**
Системно значимые кредитные организации	Стандартный (У2)	**Усиленный (У1)**	5 класс*	**4 класс**
Прочие кредитные организации	Стандартный (У2)	Стандартный (У2)	5 класс*	5 класс

* 4 класс СЗИ от НСД для СКЗИ класса КС2

ЗАЩИТА ENDPOINT И ППО



КРИПТОГРАФИЧЕСКАЯ ЗАЩИТА



ЛОГИРОВАНИЕ И МОНИТОРИНГ ИБ

Логирование:

- Технические данные от ППО и СЗИ
- Действия персонала
- События взаимодействия с ЕСИА и ЕБС
- События проверки результатов идентификации

Данные об инцидентах в ФинЦЕРТ ЦБ в течение 1 раб. дня

ГДЕ РАНЕЕ ВСТРЕЧАЛИСЬ ТРЕБОВАНИЯ

РАБОТЫ ПО ОБЕСПЕЧЕНИЮ ИБ (БЕЗ УЧЕТА ППО)

РАЗОВЫЕ РАБОТЫ

Внедрение подсистемы ИБ (3-6 мес.):

- Обследование
- Проектирование
- Внедрение
- ОРД и процессы

РЕГУЛЯРНЫЕ РАБОТЫ

Ежегодный внешний аудит:

- 321 приказ Минцифры
- Лицензиат ФСТЭК (ТЗКИ)

Ежегодный пентест:

- Требование ГОСТ Р 57580.1-2017
- Лицензиат ФСТЭК (ТЗКИ)

20/02/2019

СПАСИБО ЗА ВНИМАНИЕ!

Т. +7 495 411-76-01 | E. INFO@JET.SU | WWW.JET.SU | 127015, РОССИЯ, МОСКВА, УЛ. БОЛЬШАЯ НОВОДМИТРОВСКАЯ, 14С1, БЦ «НОВОДМИТРОВСКИЙ»