КОД ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

25-28 июля 2019
Сочи

КАК ОСУЩЕСТВИТЬ ЗАЩИТУ ПЕРСОНАЛЬНЫХ И ФИНАНСОВЫХ ДАННЫХ В БАНКОВСКОЙ СИСТЕМЕ РФ

ООО «АйДиСистемс»

Генеральный директор,
Федорец Андрей Олегович

ТЕЛЕФОН: +7 (499) 707-19-40

EMAIL: post@id-sys.ru

#CODEIB

Суперконкурентоспособность

Собственные решения крупных Банков

Большие затраты по:

- времени
- ресурсам
- финансам

Итог

Суперконкурентоспособный Банк

Комплексное решение iCam

- Быстрая интеграция
- Экономия за счет приобретения комплексного решения: БИ+СБП+Маркетплэйс

Итог

Суперконкурентоспособный Банк

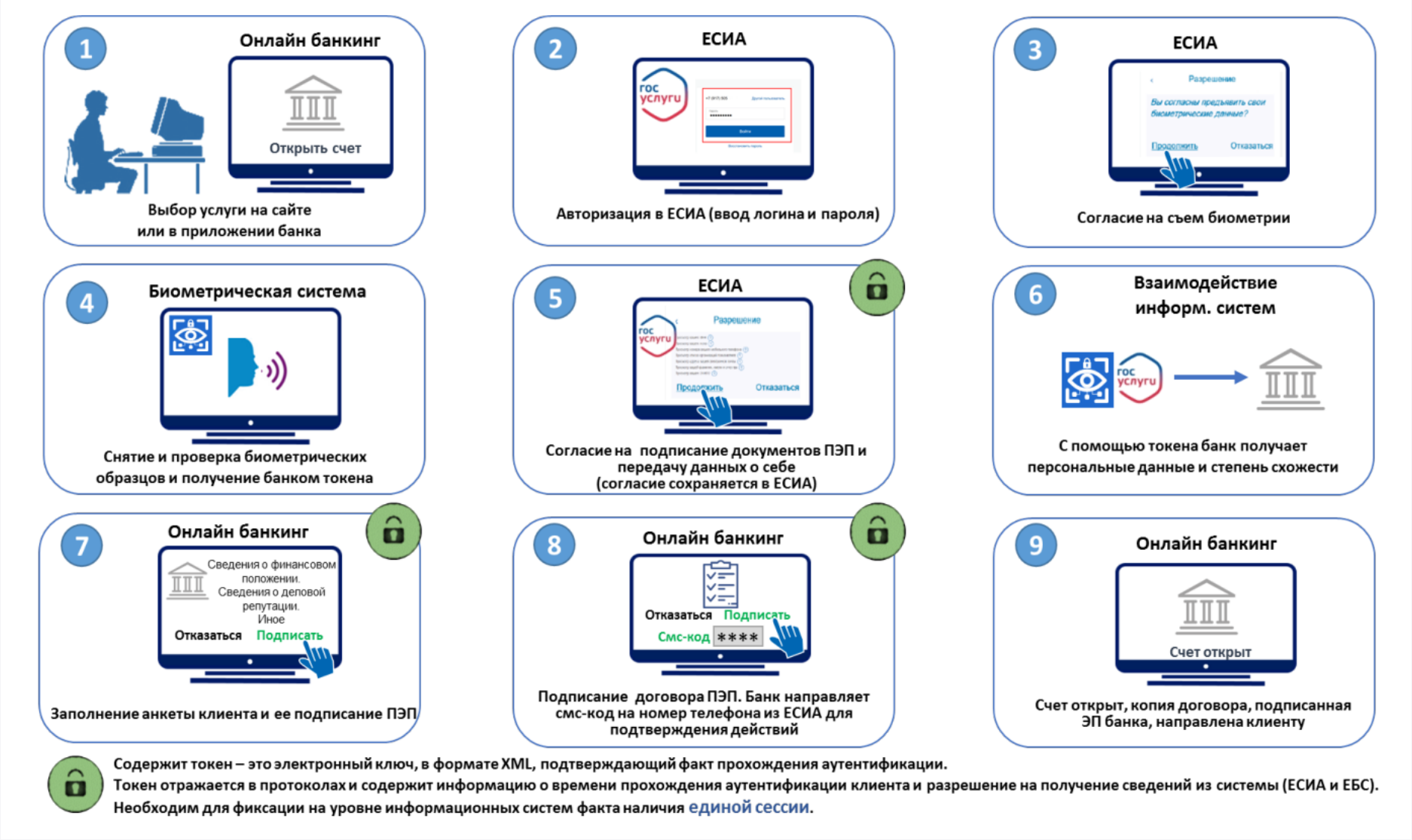
Бессистемный подход

- Непродуманная экономия
- Спонтанные внедрения
- Длительность внедрения до нескольких лет

Итог

Всё напрасно. Банк неконкурентоспособный

Процесс УпрИД и УБИ



4859-у ЦБ РФ. Перечень угроз

2 вида защищаемой информации:

- ✓ Биометрические персональные данные (БО);
- ✓ Информация о степени соответствия биометрических данных (ССБО)

4 типа угроз:

Угроза	Перевод на русский	Как реализовать?
Нарушение целостности	Подмена, удаление данных от линзы камеры	Подпись при формировании БО
Нарушение конфиденциальности	Компрометация	Шифрация при передаче БО
Нарушение достоверности	Внесение фиктивных данных	Передача подписанных и шифрованных БО
Нарушение доступности	Блокирование передачи данных	Сисадмин рулит, Кластеры и т.п.

4859-у. Перечень угроз (продолжение)

Где?	Угроза - Класс защиты
1. Обработка БО и ССБО на устройстве клиента ФЛ:	Целостность БО - КС1 Целостность ССБО - КС1 Конфиденциальность БО - КС1
2. Сбор БО в банке, передача БО между стуктурными подразделениями банка:	Целостность БО - КС2+СЗИ4 или КС3 Достоверность БО - КС2+СЗИ4 или КС3 Конфиденциальность БО - КС2+СЗИ4 или КС3
3. Передача БО между банком и ЕБС:	**Целостность БО - КВ** **Достоверность БО - КВ** Конфиденциальность БО - КС3
4. Обработка ССБО в банке:	**Целостность ССБО – КВ**
5. Передача ССБО между банком и ЕБС:	**Целостность ССБО - КВ** Конфиденциальность ССБО - КС3
6. Обработка БО и ССБО в ЕБС **Это сама ЕБС, а не банковская часть!**	**Целостность, достоверность и конфиденциальность БО, целостность и доступность ССБО – КВ.**

Рекомендации 4-МР

1 Квалифицированный Сертификат ключа проверки ЭП Банка КВ2

2 Встраивание HSM в подсистему обработки БПДн

3 Создание и использование доверенной среды функционирования:

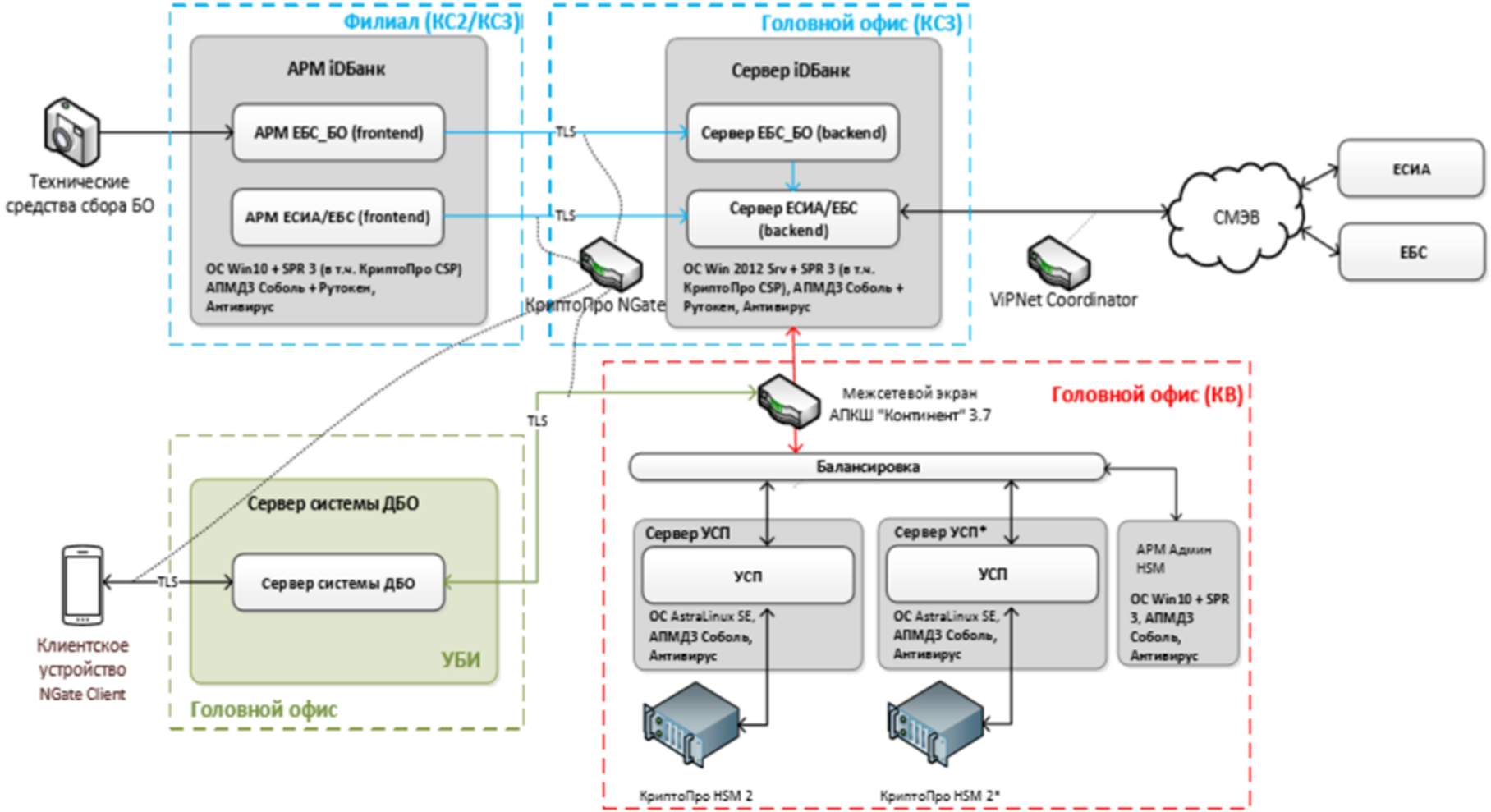
- ОС, 3-го класса защищенности, 2-го уровню контроля НДВ;
- МСЭ, ФСТЭК 3-й класс защищённости,
- СОВ 3-й класс защищенности;
- АПМДЗ 2-й класс защиты.

4 -ППО – проверка на отсутствие НДВ по 4-ому уровню контроля или сертифицированного ФСТЭК или анализ уязвимостей по требованиям ОУД 4;
-ТИ по оценке влияния на HSM класса КВ;

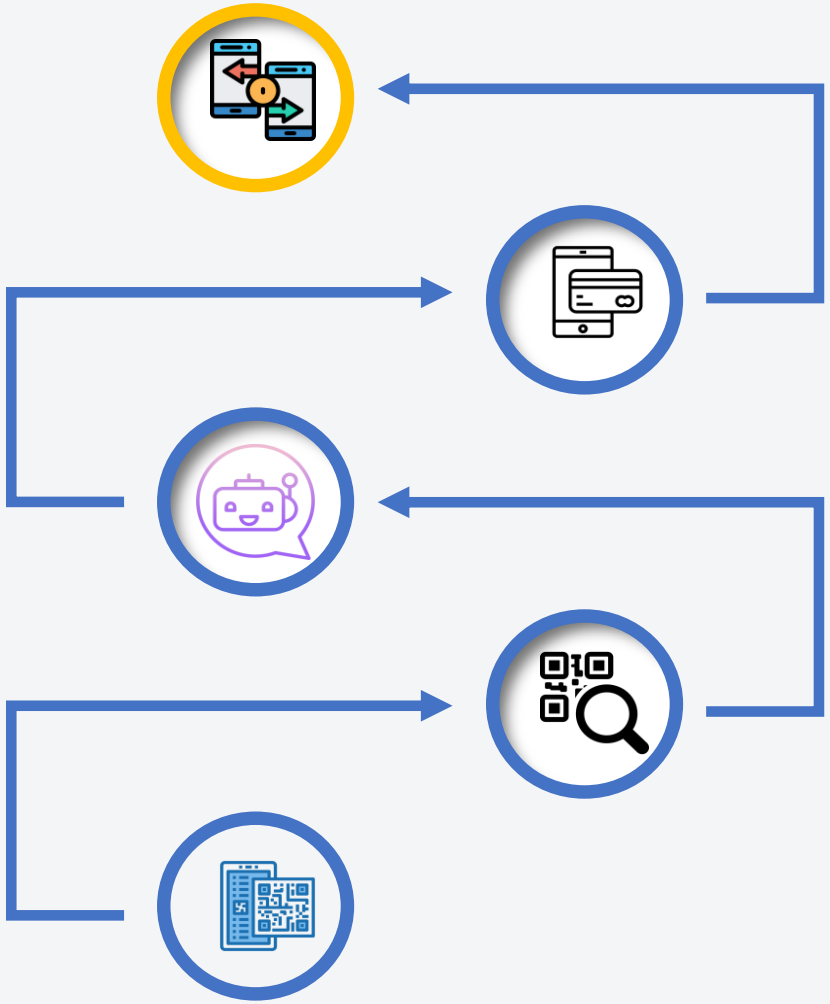
5 Документация

Типовая схема системы защиты персональных данных

Схема развертывания компонентов решения для регистрации БО в ЕСИА/ЕБС



СБП. Сценарий C2B

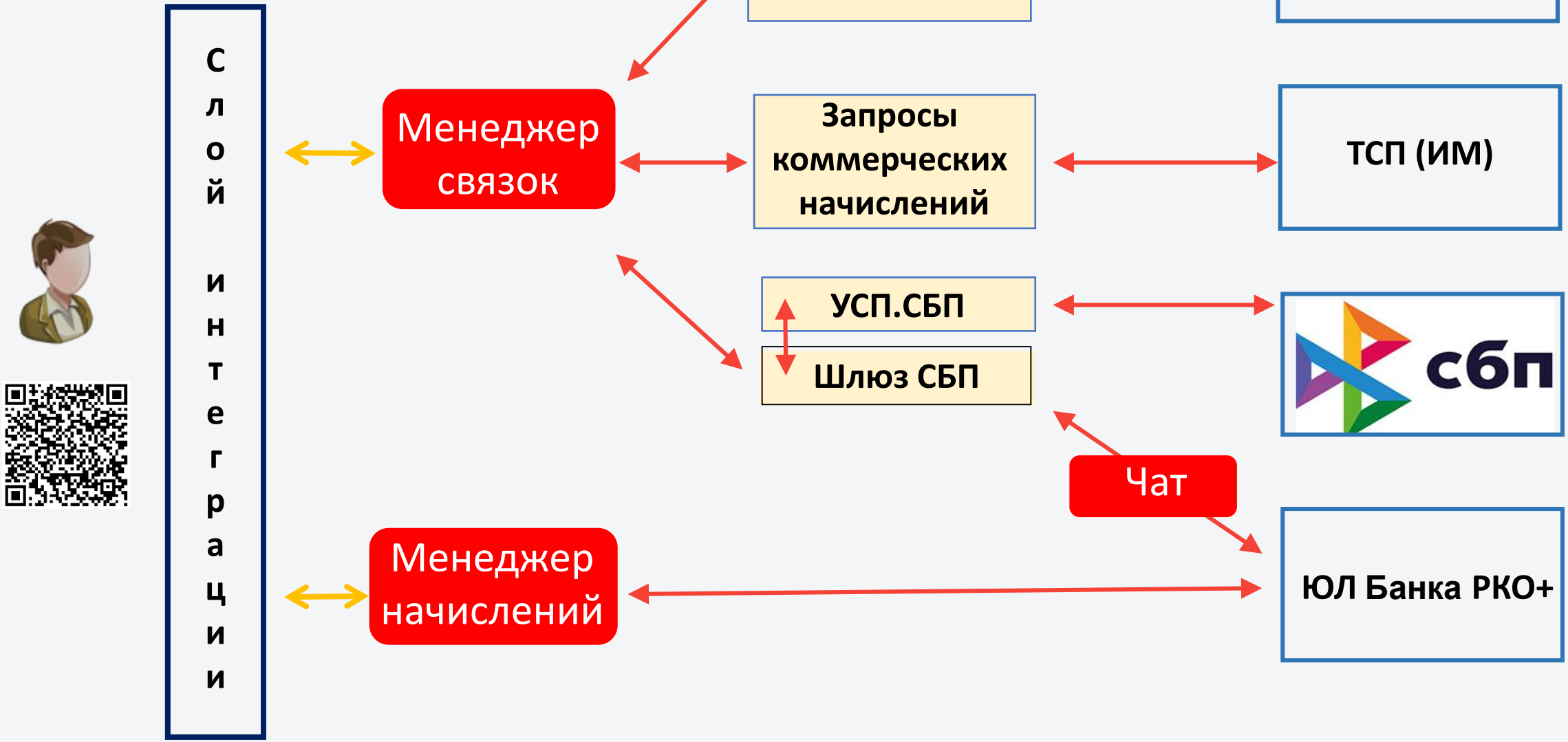


При совпадении Банка получателя и плательщика может работать ветка внутрибанковского перевода

Не дожидаемся фактического пополнения счёта и информируем получателя об оплате по QR. Идеальный инструмент – чат…

Чтение QR-кода

Генерация QR-кода


Слой интеграции
Менеджер связок
Менеджер начислений
Запросы начислений
Запросы коммерческих начислений
УСП.СБП
Шлюз СБП
Чат
ГИС ГМП
ГИС ЖКХ
ТСП (ИМ)
сбп
ЮЛ Банка РКО+

Нормативка

382-П, 552-П, ГОСТ Р 57580.1-2017, Р 57580.2-2017 и др.

Из последнего - Положение № 683-П “**Об** установлении **обязательных** для кредитных организаций **требований** к **обеспечению защиты** информации при осуществлении банковской деятельности **в целях противодействия** осуществлению **переводов** денежных средств **без согласия клиента**».

Выделим:

- Кредитные организации должны обеспечивать подписание электронных сообщений способом, позволяющим обеспечить целостность и подтвердить составление указанного электронного сообщения уполномоченным на это лицом.

- Ежегодное тестирование на проникновение и анализ уязвимостей информационной безопасности объектов информационной инфраструктуры.

- Банкам необходимо обеспечить уровень соответствия согласно ГОСТ Р 57580.2-2017 не ниже третьего с 01.01.2021, а в дальнейшем, с 01.01.2023 обеспечить уровень соответствия не ниже четвертого в соответствии с ГОСТ Р 57580.2-2017.

- Согласно пункту 9 Положения № 683-П с 01.01.2021 банкам необходимо реализовать проведение оценки соответствия установленному уровню защиты информации не реже одного раза в два года с привлечением организации, имеющей лицензию на деятельность по ТЗКИ.

СПАСИБО ЗА ВНИМАНИЕ!

КОД ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

25-28 июля 2019
Сочи

#CODEIB

ООО «АйДиСистемс»

Генеральный директор,
Федорец Андрей Олегович

ТЕЛЕФОН: +7 (499) 707-19-40

EMAIL: post@id-sys.ru

FACEBOOK: @IDSystemz

САЙТ: www.id-sys.ru

YOUTUBE: iCAM Group