



АУТСОРСИНГ ИНФРАСТРУКТУРЫ ДЛЯ РАБОТЫ С ЕДИНОЙ БИОМЕТРИЧЕСКОЙ СИСТЕМОЙ С ТОЧКИ ЗРЕНИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ: ОПЫТ ЦФТ

Алексей ЛЕОНОВ,
Директор дирекции информационной безопасности, ГК ЦФ

О КОМПАНИИ

Группа Компаний ЦФТ – провайдер решений для финансового рынка РФ и СНГ

ГОД ОСНОВАНИЯ	1991
ПОЗИЦИИ НА РЫНКЕ	ЦФТ входит в TOP-5 крупнейших разработчиков ПО в России
СПЕЦИАЛИЗАЦИЯ	Программное обеспечение и сервисы для <ul style="list-style-type: none">• всех видов банковской деятельности• участия банков на платежном рынке• страховых компаний, казначейств, корпораций Аутсорсинг <ul style="list-style-type: none">• поддержки и развития систем ЦФТ• ЦОД ЦФТ для размещения программного обеспечения
КЛИЕНТЫ Аутсорсинга АБС	>8 банков, 1 банк Казахстан, 1 Страховая компания, Системы АБС для обучения в ВУЗе
ОФИСЫ	<ul style="list-style-type: none">• Москва – центр разработки, сопровождения, внедрения, продаж• Новосибирск – главный центр разработки ПО, сопровождения• 12 филиалов в ведущих экономических регионах РФ• Зарубежные представительства в Алматы, Душанбе, Кишиневе
СОТРУДНИКИ	Более 3000 человек

ЦФТ НА РЫНКЕ ОБЛАЧНЫХ РЕШЕНИЙ ДЛЯ ФИНАНСОВОГО СЕКТОРА

- ИТ-аутсорсинг – одна из ведущих компетенций компании
- ЦФТ развивает услуги ИТ-аутсорсинга по следующим направлениям:
 - CORE BANKING
 - ИНТЕРНЕТ-СЕРВИСЫ
 - КАРТОЧНЫЕ ПРОДУКТЫ



ЦФТ - ПЕРВАЯ РОССИЙСКАЯ СОФТВЕРНАЯ КОМПАНИЯ, УСПЕШНО РЕАЛИЗОВАВШАЯ СЕРИЮ ПРОЕКТОВ ПО ПРЕДОСТАВЛЕНИЮ ПАРТНЕРАМ **CORE BANKING SYSTEM** НА УСЛОВИЯХ АУТСОРСИНГА

2010 год | старт реализации проектов по аутсорсингу

2018 год | старт реализации проекта по аутсорсингу инфраструктуры для работы с ЕБС



С ЧЕГО ВСЕ НАЧИНАЛОСЬ... ДЛЯ INHOUSE

Для работы с ЕБС Банку требуется:

- **ПРОГРАММНОЕ ОБЕСПЕЧЕНИЕ**
 - Разработали ПО АРМ «ЦФТ-ГОСУСЛУГИ»
- **ОБОРУДОВАНИЕ**
 - В комплекс услуг включили «поставка ПО и оборудования» + настройка
- **«БЕЗОПАСНОСТЬ»**
 - В решении учли только рекомендованное регулятором сертифицированное ПО
 - Процессы с встраиванием СКЗИ и сертификацией взяли на себя



С ЧЕГО ВСЕ НАЧИНАЛОСЬ: АРМ «ЦФТ-ГОСУСЛУГИ»

Программное обеспечение АРМ «ЦФТ-ГОСУСЛУГИ»

ПРЕИМУЩЕСТВА ДЛЯ БАНКОВ В НАШЕМ ПОДХОДЕ:

- «Невидимая» регистрация клиентов
- Процесс максимально автоматизирован
- Интуитивно-понятный интерфейс
- История работы с клиентами
- Шаблоны документов
- Минимальное время на настройку решения
- Инструкции и консультации
- Удобное администрирование
- Понятное ПО
- Несколько вариантов обеспечения ИБ
- Не требуется проходить контроль встраивания
- Готовый список необходимого оборудования
- Услуги по обеспечению ИБ (настройка защищенных каналов и т.д.)

НАПРАВЛЕНИЯ РАБОТЫ С ЕБС: INHOUSE

МОДЕЛЬ	ХАРАКТЕРИСТИКИ	ОСОБЕННОСТИ
«ИНХАУС»	ИТ-инфраструктура размещается в ЦОДе Банка. ЦФТ выступает поставщиком решения (ПО) для работы с ЕБС + сопровождение (доработки, обновления, исправление ошибок) решения ЦФТ	<ul style="list-style-type: none">• Данную модель выбирают крупные банки• Банк отвечает за всю техническую наполненность ЦОДа и дополнительные средства защиты• ЦФТ проводит контроль встраивания СКЗИ для своего решения• Банк ежегодно проводит оценку соответствия решения требованиям по безопасности (в периметр попадает вся ИТ-инфраструктура с пользовательскими местами)

ФУНКЦИИ, ВЫПОЛНЯЕМЫЕ В РАМКАХ ИТ-АУТСОРСИНГА



- **БИЗНЕС-ФУНКЦИИ:** автоматизация бизнес-процессов по основным направлениям деятельности, задачи по модификации, развитию, адаптации продуктов ИТ под требования Банка и регуляторов



- **ИТ-ФУНКЦИИ:** администрирование аппаратно-программного комплекса, услуги по поддержке пользователей, эксплуатации, сопровождению и развитию



- **ОБЕСПЕЧЕНИЕ БЕЗОПАСНОСТИ:** реализация комплекса мер по физической безопасности, пожарной безопасности, информационной безопасности, управление правами пользователей, контроль встраивания, аудит безопасности

НАПРАВЛЕНИЯ РАБОТЫ С ЕБС: ОБЛАКО

МОДЕЛЬ	ХАРАКТЕРИСТИКИ	ОСОБЕННОСТИ
«ОБЛАКО»	Вся ИТ-инфраструктура находится на стороне Аутсорсера, на стороне Банка только пользовательские ПК (рабочие места контролера, администратора, операциониста-оператора).	<ul style="list-style-type: none">• Аутсорсер отвечает за всю техническую наполненность ЦОДа и за наличие средств защиты (FW, AV, оборудование для построения защищенного канала связи с Банком, СЗИ, HSM, КриптоПро DSS и т.д.),• Аутсорсер выполняет согласование СИСТЕМНОГО ПРОЕКТА облачного решения с ЦБ РФ и с 8 центром ФСБ,• Аутсорсер проводит контроль встраивания СКЗИ в свое облачное решение• Аутсорсер проводит аудит своей облачной инфраструктуры по 2-му уровню защиты информации согласно ГОСТ Р 57580.1-2017• Банк ежегодно проводит оценку соответствия требованиям по ЗИ только по пользовательским местам

ОБЕСПЕЧЕНИЕ БЕЗОПАСНОСТИ – ОСНОВНЫЕ НАПРАВЛЕНИЯ В ИТ-АУТСОРСИНГЕ

БАЗОВЫЙ УРОВЕНЬ:

1. **Физическая безопасность ЦОДов.** Охрана и контроль доступа обеспечивается спецподразделением охраны, реакция ГБР в течение 5 минут с момента поступления сигнала на пост охраны
2. **Система контроля доступа в ЦОД.** В ЦОДа реализован доступ по персонифицированным картам. При этом для входа реализован шлюзовой доступ в ЦОД (вход только по одному человеку с доп.подтверждением доступа со стороны охраны)
3. **Система видеонаблюдения.** Внутренний и внешний периметр ЦОДов находится под непрерывном контролем со стороны видеонаблюдения с датчиками движения/присутствия/взлома
4. **Резервное копирование.** Все критичные сервера на ежедневной основе бэкапируются на защищенные библиотеки (хранение информации в зашифрованном виде)

ОБЕСПЕЧЕНИЕ БЕЗОПАСНОСТИ – ОСНОВНЫЕ НАПРАВЛЕНИЯ В ИТ-АУТСОРСИНГЕ

ОБЩИЙ УРОВЕНЬ:

1. **Дублирующий ЦОД (резервный).** Для обеспечения непрерывности деятельности в инфраструктуре существуют два ЦОДа, удаленно разнесенных между собой. Территория размещения ЦОДов не подвержена риску землетрясения и наводнения
2. **ЦОДы созданы по уровням надежности Tier III стандарта TIA-942.** Сертификацию не проходили
3. К каждой из площадок подключено по 4 магистральных интернет провайдера - РОСТЕЛЕКОМ, ТТК, АВАНТЕЛ, РТКОММ- СИСБИРЬ.
+ по два в каждой площадке локальных провайдера

ОБЕСПЕЧЕНИЕ БЕЗОПАСНОСТИ – ОСНОВНЫЕ НАПРАВЛЕНИЯ В ИТ-АУТСОРСИНГЕ

ОСОБЕННОСТИ РЕШЕНИЯ:

1. **Выделенный сетевой сегмент** специально созданный за МЭ класса 3 защищенности.
2. **Защита каналов связи** между Банков и ЦОДом Аутсорсера
СКЗИ класса КС3
3. **Идентификация оператора/контролера/администратора в Системе** с использованием УКЭП КС3,
либо УКЭП КС2 + *СЗИ от НСД на основании N 4859-У п.1.2* для идентификации и контроля целостности запросов,
содержащих биом. ПДн
4. **Идентификация Банка** УКЭП КВ2 для подписи данных биом. ПДн
УКЭП по КВ2 от НИИ «Восход»
5. **Защита данных при сборе биом. ПДн (контроль целостности)**
Класс СКЗИ - КВ2
6. **Хранение подписи КВ** ПАК КриптоПро HSM 2.0 СКЗИ класса КВ, (к средствам ЭП класса КВ2)

ИТ-АУТСОРСИНГ: ПРЕИМУЩЕСТВА ДЛЯ БАНКОВ



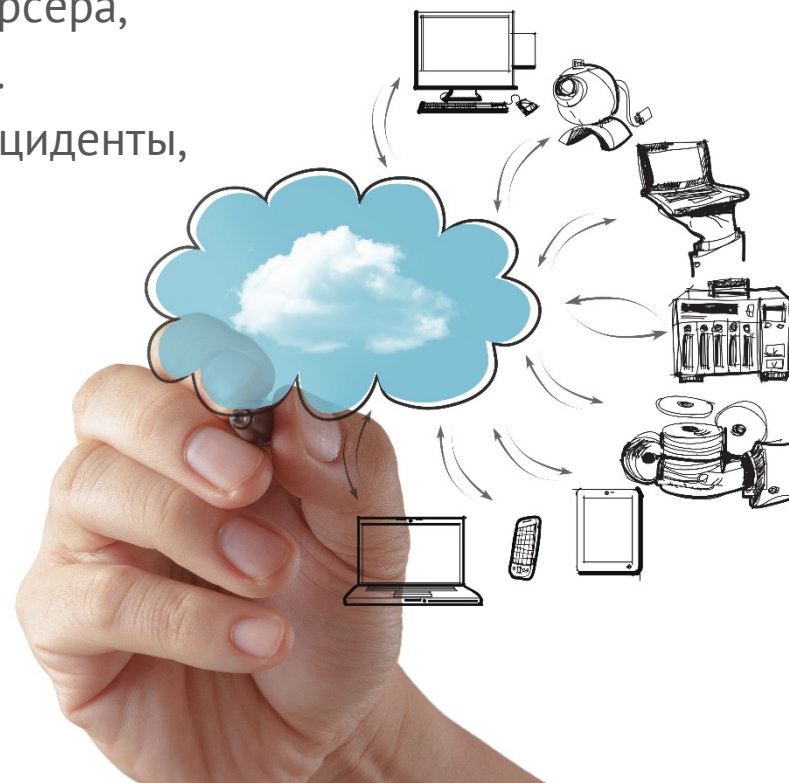
- В реализованном проекте мы обеспечили снижение затрат на содержание собственной ИТ-инфраструктуры для Банка
- Оптимизация бизнес-процессов
- Предсказуемость расходов и возможность оперативного изменения состава услуг аутсорсинга
- Прохождение оценки соответствия по требованиям защиты информации только для рабочих станций – снижение ежегодных издержек на сопровождение решения

**экономия
на ИТ-инфраструктуре
на сумму
от 4-5 млн руб**

ИТ-АУТСОРСИНГ: ПРЕИМУЩЕСТВА ДЛЯ БАНКОВ



- Ускоренное внедрение новых «фич» за счет того, что они уже были реализованы в ПО в единой платформе
- Полный контроль со стороны Банка за действиями аутсорсера, что дает уверенность в безопасности получаемой услуги. Контроль доступа, журналирование, реагирование на инциденты, мониторинг



ВЫВОДЫ

- ИТ-аутсорсинг – приемлемая для банков схема работы. Регулятор также поддерживает данное решение о чем свидетельствует вышедшие в пятницу «Методические рекомендации...», где в частности облачная схема работы с ЕБС «легализована»,
- Мы находимся на этапе согласования Системного проекта для облачного решения и ожидаем в ближайшее время получения экспертного заключения от независимой лаборатории (КриптоПро) и согласования 8-м центром ФСБ.
- После согласования Системного проекта мы переходим к следующей стадии – процедуре «контроля встраивания» СКЗИ в свое решение.
- И последний этап в этой части – аудит по 2 уровню защиты информации согласно **ГОСТ Р 57580.1-2017**

ЦФТ ЦЕНТР
ФИНАНСОВЫХ
ТЕХНОЛОГИЙ

www.cft.ru

www.group.cft.ru

СПАСИБО ЗА ВНИМАНИЕ!
ВОПРОСЫ?

Алексей ЛЕОНОВ,

Директор дирекции информационной безопасности, ГК ЦФ

A.Leonov@cft.ru