РОССИЙСКИЕ НАУКОЁМКИЕ ТЕХНОЛОГИИ

СОА как основа построения системы противодействия кибератакам в финансовой сфере. Безопасность перспективных систем передачи и обработки финансовой информации. Взаимодействие с ФинЦЕРТ и ГосСОПКА

Андрей Курило
Заместитель генерального директора компании «РНТ»

Михаил Воробьев
Начальник отдела Центра разработки технологий компании «РНТ»

Владимир Лаптев
Руководитель проектов МТК «КОМКОР»


ФОРПОСТ
МОНИТОРИНГ И ЗАЩИТА ОТ КИБЕРАТАК

Возможности и предотвращаемые угрозы

ЛИНЕЙКА ПРОДУКТОВ

«ФОРПОСТ»

- Мониторинг и управление комплексом технических средств АИС
- Обнаружение компьютерных атак
- Блокирование доступа источников компьютерных атак
- Выявление аномальной активности на контролируемых ресурсах
- Регулярное обновление базы решающих правил (сигнатур)

Состав комплексного решения «ФОРПОСТ»

КОНТРОЛЬ СЕТЕВОГО ТРАФИКА НА ГРАНИЦЕ И ВНУТРИ

СОА «ФОРПОСТ»

СПА «ФОРПОСТ»

«ФОРПОСТ HIPS»

ПРЕДУПРЕЖДЕНИЕ, ВЫЯВЛЕНИЕ, КОНТРОЛЬ

«ФОРПОСТ Мониторинг»

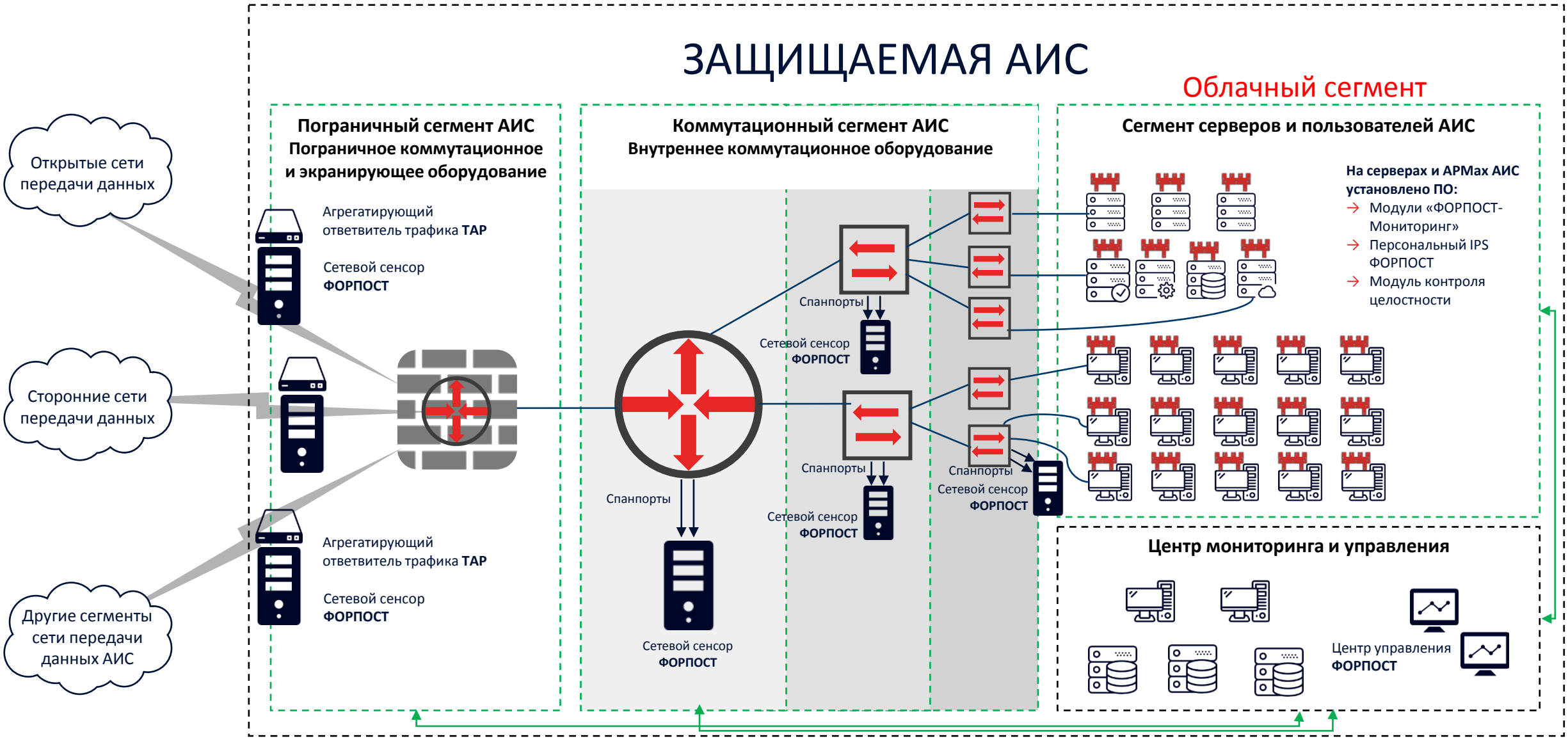
ЗАЩИЩАЕМЫЕ РЕСУРСЫ

МОДУЛЬ
ПОВЕДЕНЧЕСКОГО АНАЛИЗА

МОДУЛЬ ИНТЕГРАЦИИ
СО СТОРОННИМИ SIEM

ПЕРЕДАЧА ДАННЫХ
В ГосСОПКА/ФинЦЕРТ

Типовое размещение в АИС элементов ПАК «ФОРПОСТ»



Опыт применения, сертификаты и требования

Сертификат соответствия ФСТЭК России № 2845 от 18 марта 2013 г.

… удостоверяет, что система обнаружения компьютерных атак «Форпост», версия 2.0, … соответствует требованиям документов **«Требования к системам обнаружения вторжений» (ФСТЭК России, 2011) - по 3 классу защиты**, **«Профиль защиты систем обнаружения вторжений уровня сети третьего класса защиты ИТ.СОВ.С3.ПЗ»** (ФСТЭК России, 2012). Срок действия: до 18 марта 2019 г., планируется к продлению.

Сертификаты соответствия ФСБ России №№ СФ/СЗИ-0047, № СФ/СЗИ-0048 от «05» июня 2015 г. на изделие Система обнаружения

компьютерных атак «ФОРПОСТ», версия 2.0, 2.0.1 которые соответствуют **требованиям ФСБ России к системам обнаружения компьютерных атак класса Б** и могут использоваться в органах государственной власти Российской Федерации в АИС, обрабатывающих информацию, не содержащую государственную тайну. (действителен до «30» июня 2018 г., продлевается)

В новых версиях (в настоящее время на сертификации):

- Работа в среде Linux
- Наличие WEB-интерфейса
- Работа в виртуальной среде со следующими платформами: KVM, ESX, Hyper-V.
- Возможность подключения к системе мониторинга всех основных продуктов, присутствующих на рынке

ПРИ РАЗРАБОТКЕ ЛИНЕЙКИ ПРОДУКТОВ «ФОРПОСТ» АО «РНТ» ОРИЕНТИРОВАЛОСЬ НА ТРЕБОВАНИЯ В ЧАСТИ, КАСАЮЩЕЙСЯ ФУНКЦИОНАЛЬНОСТИ НА ТРЕБОВАНИЯ СЛЕДУЮЩИХ ДОКУМЕНТОВ:

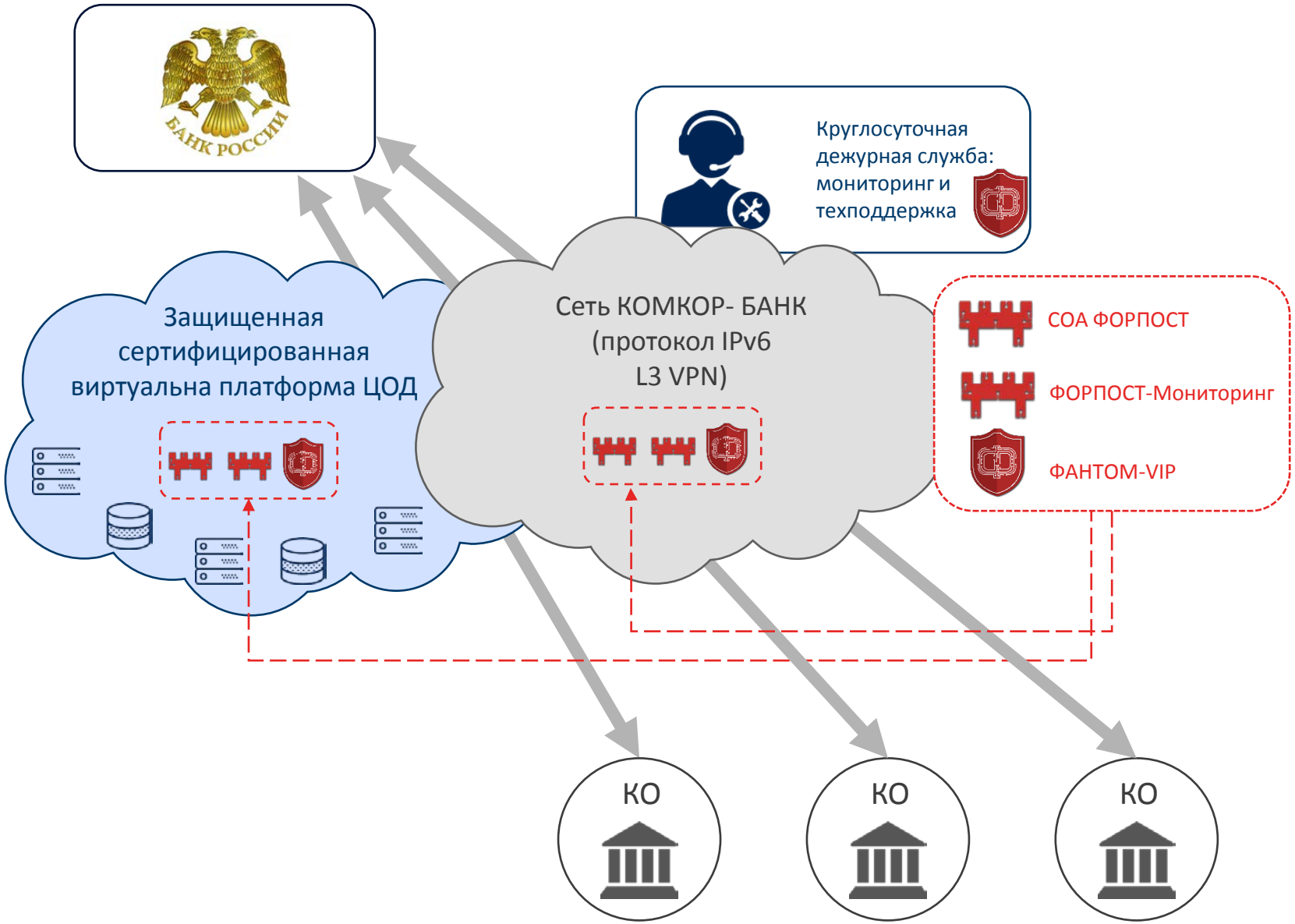
- **ГОСТ Р 57580.1-2017** (Безопасность финансовых (банковских) операций . Защита информации финансовых организаций. Базовый состав организационных и технических мер.),
- **Рекомендации в области стандартизации Банка России РС БР ИББС-2.8-2015**, (Обеспечение информационной безопасности организаций банковской системы Российской Федерации. Обеспечение информационной безопасности при использовании технологии виртуализации)
- **Приказ ФСТЭК России №17** от 11 февраля 2013 года (Об утверждении Требований о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах),
- **Приказ ФСТЭК России №27** от 15 февраля 2017 года (О внесении изменений в Требования о защите информации, не составляющей государственную тайну, содержащейся государственных информационных системах, утвержденные приказом Федеральной службы по техническому и экспортному контролю от 11 февраля 2013 г. №17)

ФОРПОСТ

ФАНТОМ-VIP

ПРОВЕРКА РАБОТОСПОСОБНОСТИ В СЕТИ ОАО «Московская телекоммуникационная корпорация «КОМКОР»

Схема размещения ПАК «ФОРПОСТ» и ПК «Фантом-VIP» на сети АО «КОМКОР»



ОСНОВНЫЕ ХАРАКТЕРИСТИКИ СЕТИ «КОМКОР-Банк»

Число кредитных организаций, казначейств, особых клиентов :
250
Шифрование:
Точка-точка
Количество сетевого оборудования:
2 высокоскоростных катастрофоустойчивых узла доступа (по 2 независимых ВОЛС на каждый) и холодный резерв сетевого оборудования
Средняя задержка: **4 мс**
Скорость:
по требованию клиентов
Доступность для крупных банков, например, Сбербанка:
99,97

→ Цель - сокращение времени реакции персонала на инциденты ИБ и снижение рисков ИБ в сети КОМКОР- БАНК, в том числе, полной потери доступности платежной системы Банка России

Основные цели и задачи

ОСНОВНЫЕ ЦЕЛИ В РАМКАХ ВЗАИМОДЕЙСТВИЯ АО «РНТ» И ОАО «КОМКОР»

1. Повышение уровня безопасности сети оператора, предоставляющего услуги кредитным организациям путем реализации требований регуляторов по доступности, качеству услуг и безопасности инфраструктуры
2. Выполнение требований ФЗ № 187 от 26.06.2017 г. «О безопасности КИИ РФ»
3. Обеспечение заданных показателей доступности перспективной платежной системы ЦБ РФ (99,999) и системообразующих банков (99,99) на основе спецоператора ФИНТЕЛЕКОМ (99,99)
4. Подготовка платформы и создание прототипа защищенного «облачного сервиса» с целью :
   - → обеспечения возможности размещения в защищенном облаке информационных ресурсов организаций,
   - → выполнения в полном объеме обработки информации, включая хранение ЭД с обеспечением юридической силы.
   - → решения задачи удобного и безопасного электронного взаимодействия на финансовом рынке
5. Предоставление ФинЦЕРТ возможности взаимодействия с присоединившимися организациями в режиме реального времени с использованием защищенных каналов связи и аккредитованного корпоративного центра ГосСОПКА АО РНТ
6. Обеспечение импортозамещения на основе российских сертифицированных телекоммуникационных средств, виртуальной среды (Горизонт-ВС), линейки продуктов «ФОРПОСТ», «ФАНТОМ» и российской сертифицированной криптографии.
7. Подготовка предложений по типовому решению обеспечения информационной безопасности глобальных и региональных телекоммуникационных операторов существующей и перспективной платежной системы Банка России

ЦЕЛИ И ЗАДАЧИ В РАМКАХ ПРОВЕРОК:

1. Контроль доступности сетевого оборудования КОМКОР и подключенных клиентов
2. Контроль неизменности прошивок и конфигураций сетевого оборудования КОМКОР
3. Агрегация сообщений, генерируемых сетевым оборудованием КОМКОР
4. Выявление сетевого трафика, передаваемого в нешифрованном виде и его источников
5. Выявление компьютерных атак, направленных на сетевое оборудование и Центр управления сетью
6. Проверка работоспособности и бесперебойного функционирования всех компонентов ПАК «ФОРПОСТ» в виртуальной среде

Результаты испытаний и выводы

С ИСПОЛЬЗОВАНИЕМ ЛИНЕЙКИ ПРОДУКТОВ ПАК «ФОРПОСТ» и ПК «ФАНТОМ- VIP» РАЗРАБОТКИ АО «РНТ», ПРОВОДИЛИСЬ ПРОВЕРКИ :

- На действующем телекоммуникационном оборудовании АО «Комкор» в рамках сети «Комкор-банк» ;
- На ЦОД «Комкор», на российской сертифицированной ФСТЭК России платформе виртуализации «Горизонт-ВС»

По результатам испытаний подготовлен соответствующий протокол.

РЕЗУЛЬТАТЫ ИСПЫТАНИЙ:

- Показана работоспособность ПАК «Форпост» и «ФАНТОМ - VIP» при их размещении в сети «Комкор-Банк», в двух вариантах (ПАК, виртуальная среда ЦОД).
- Заявленные в эксплуатационной документации функции ПАК «ФОРПОСТ», в том числе реализация собственных механизмов защиты, реализуются полностью.
- Проверки заявленной функциональности по базовым требованиям ГОСТР 57580.1-2017 прошли успешно.
- Линейка ПАК «Форпост» не уступает по характеристикам используемому в настоящий момент импортному ПО, контролирующему состояние сети Комкор-Банк.
- Обеспечивается информационная безопасность рабочих мест операторов от НСД и кибератак атак на базе ПАК «Фантом-VIP»
- Целесообразно и возможно использовать ПАК «Фантом-VIP» в качестве универсальной платформы для защищенного доступа клиентов (абонентов) к облачным сервисам.

УСТАНОВКА НА ОБОРУДОВАНИИ ОАО «КОМКОР» ПАК «ФОРПОСТ» И «ФАНТОМ - VIP» ПОЗВОЛЯЮТ РЕШИТЬ СЛЕДУЮЩИЕ ЗАДАЧИ:

- Обеспечить выполнение требований статей 4, 10 и 11 ФЗ № 187-ФЗ «О безопасности критической информационной инфраструктуры Российской Федерации», а также положений нормативных актов ФСТЭК и государственных стандартов Российской Федерации.
- Обеспечить достаточный уровень защищенности от кибератак инфраструктуры телекоммуникационного оператора, предоставляющего услуги финансовым структурам и Банку России (каналы связи и ЦОД) и как следствие – обеспечивается требуемая доступность сервисов с использованием СОА ПАК «Форпост» и ПАК «ФАНТОМ - VIP» не ниже 99,99.
- Предложить новый экономически выгодный сервис защиты от компьютерных атак с использованием уже имеющихся каналов связи и размещаемых в защищенном ЦОД оператора связи ПАК «Форпост» и ПАК«ФАНТОМ»
- Обеспечить возможность предоставления финансовым организациям облачных защищенных сервисов для решения задачи обеспечения взаимодействия на финансовом рынке, включая сервисы защищенного доступа и полноценной функциональности (аутентификация, внешний и внутренний документооборот, платежи, электронная подпись, долговременное хранение электронных документов, технологии блокчейн).

Перспективная система оператора финансового сектора

РОССИЙСКИЕ НАУКОЁМКИЕ ТЕХНОЛОГИИ

Требования по безопасности к перспективной системе

Предоставление потребителю дополнительных централизованных сервисов безопасности:

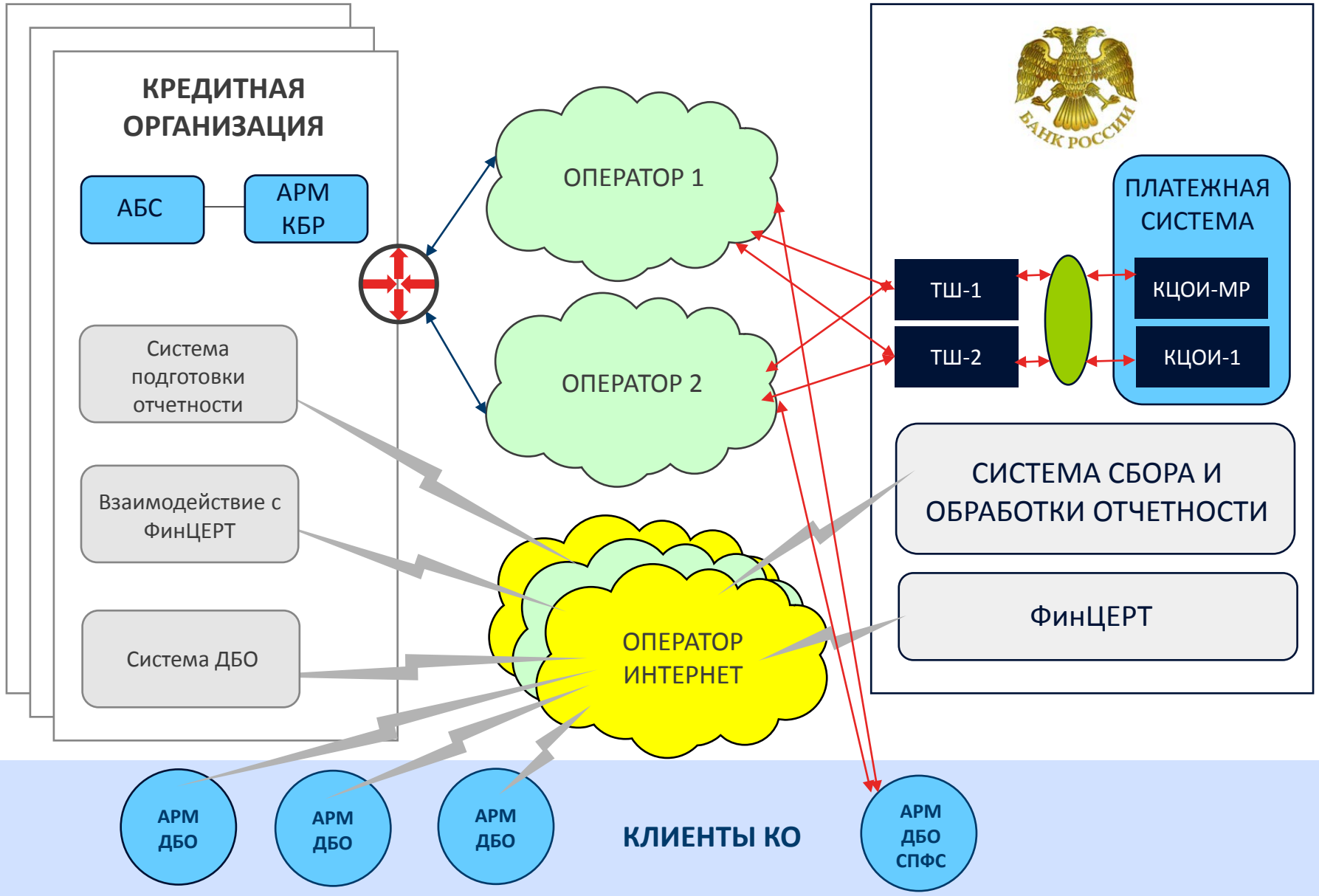
- → Защита от компьютерных атак, обнаружение аномальных активностей
- → Очищенный от вирусов трафик Интернет
- → Защита от DDoS – атак
- → Защищенный доступ в систему
- → Использование ЭП, в том числе облачной ЭП
- → Обеспечение юридической силы хранимых электронных документов

Выполнение требований статей 4, 10 и 11 ФЗ № 187-ФЗ «О безопасности критической информационной инфраструктуры Российской Федерации»

- → Обеспечение доступности (99,99)
- → Обеспечение целостности
- → Обеспечение конфиденциальности
- → Соответствие требованиям по импортозамещению
- → Наличие аттестата соответствия в системе аттестации ФСТЭК

Документы, устанавливающие требования по защите и фиксирующие состояние защищенности системы			
Базовые требования по безопасности	Требования к ГИС	Требования ФЗ № 187-ФЗ	Свидетельства доверия
ГОСТР 57580.1—2017	Приказ ФСТЭК России от 11 февраля 2013 г. № 17 Приказ ФСТЭК России от 15 февраля 2017 г. № 27	18 НПА ФСТЭК, ФСБ и МКС	Свидетельства компетенции организации, выполняющей работы по безопасности
Проект ГОСТ Р Методика оценки соответствия»			Сертификаты на системы, средства обеспечения безопасности и контроля
ГОСТР 56938-2016			Аттестат соответствия на систему
СТО БР ИББС-1.0 — 2014 СТО БР ИББС-1.1-2007»			
Положение Банка России от 9 июня 2012 г. № 382-П			Периодическая оценка соответствия
Положение Банка России от 24 августа 2016 г. № 552-П			

Существующая система взаимодействия ЦБ с КО и их Клиентами



ЗАДЕЙСТВОВАННЫЕ ОПЕРАТОРЫ СВЯЗИ

ВНУТРЕННИЙ ОПЕРАТОР ЦБ (с опорой собственные и на внешние каналы)
Доступность:
99,999

ОПЕРАТОР 1
Доступность:
99,99

ОПЕРАТОР 2
Доступность:
99,9

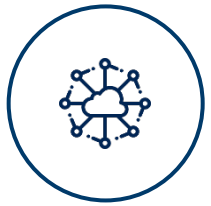
ОПЕРАТОР ИНТЕРНЕТ
Доступность:
97,0

Предпосылки перехода на новую транспортную систему

ПО МНЕНИЮ ЦЕНТРАЛЬНОГО БАНКА, ПРЕДПОСЫЛКИ ПЕРЕХОДА НА ЦЕНТРАЛИЗОВАННУЮ СХЕМУ ДОСТУПА К ПЛАТЕЖНОЙ СИСТЕМЕ БАНКА РОССИИ СЛЕДУЮЩИЕ:

Концентрация размещения центров обработки информации клиентов

Переход на единый расширенный регламент и предоставление клиентам равнодоступности услуг платежной системы Банка России независимо от местонахождения клиентов



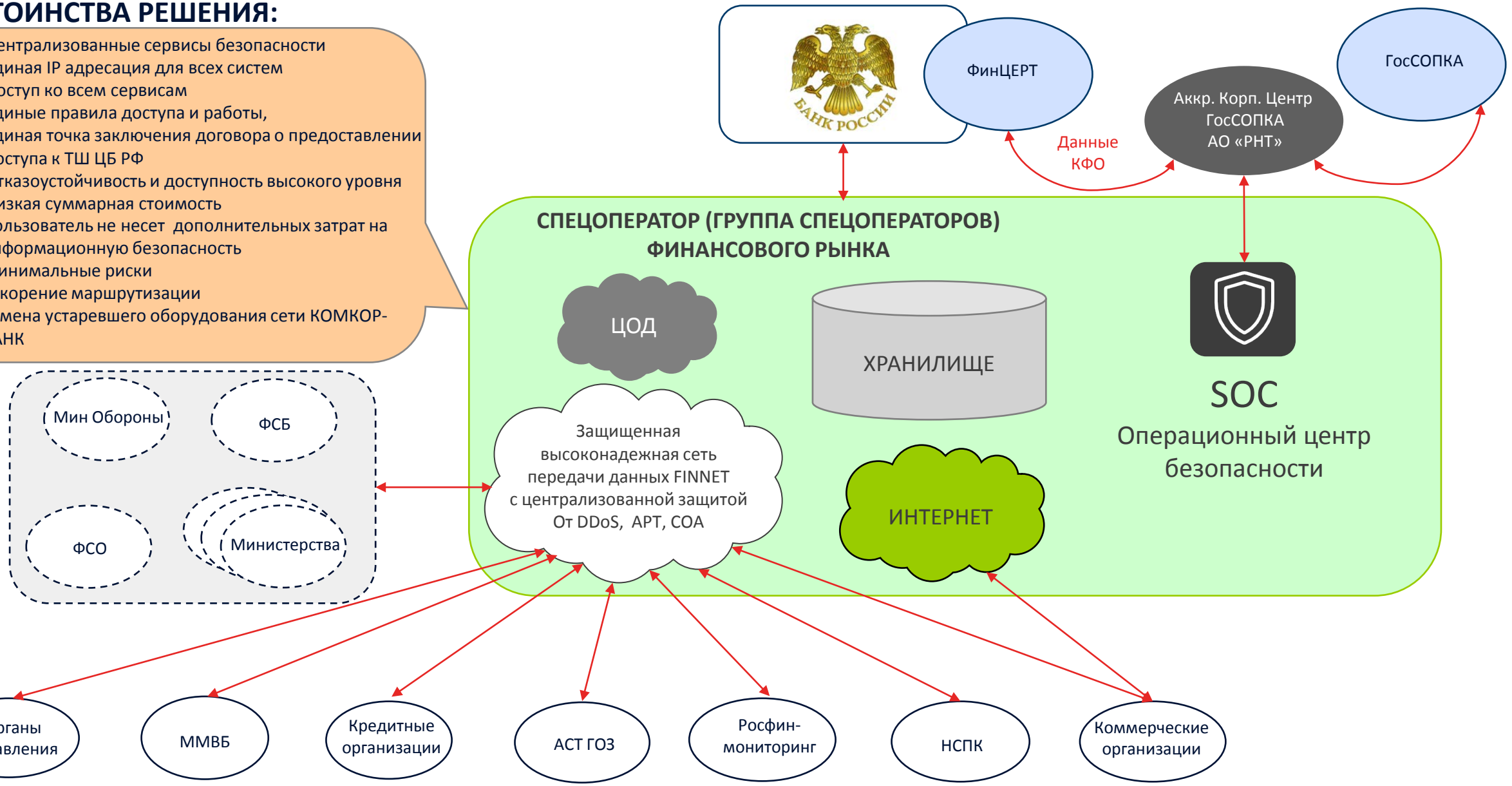
Обеспечение подключения к Транспортной системе Банка России на основе современных технологий

Обеспечение высокой доступности подключения к Платежной системе Банка России

Перспективная система оператора финансового сектора

ДОСТОИНСТВА РЕШЕНИЯ:

- Централизованные сервисы безопасности
- Единая IP адресация для всех систем
- Доступ ко всем сервисам
- Единые правила доступа и работы,
- Единая точка заключения договора о предоставлении доступа к ТШ ЦБ РФ
- Отказоустойчивость и доступность высокого уровня
- Низкая суммарная стоимость
- Пользователь не несет дополнительных затрат на информационную безопасность
- Минимальные риски
- Ускорение маршрутизации
- Замена устаревшего оборудования сети КОМКОР-БАНК

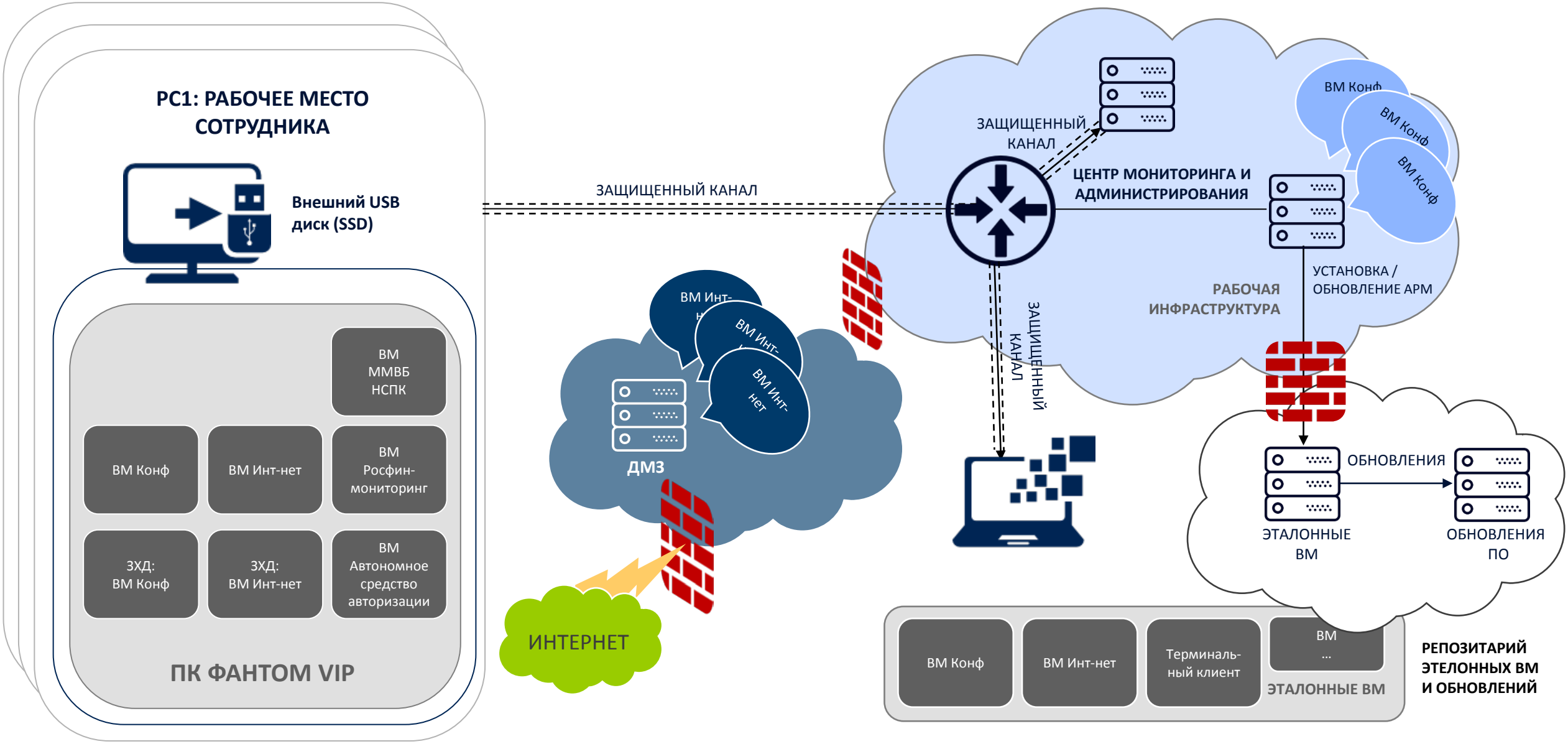


SOC в «облаке» оператора финансового сектора

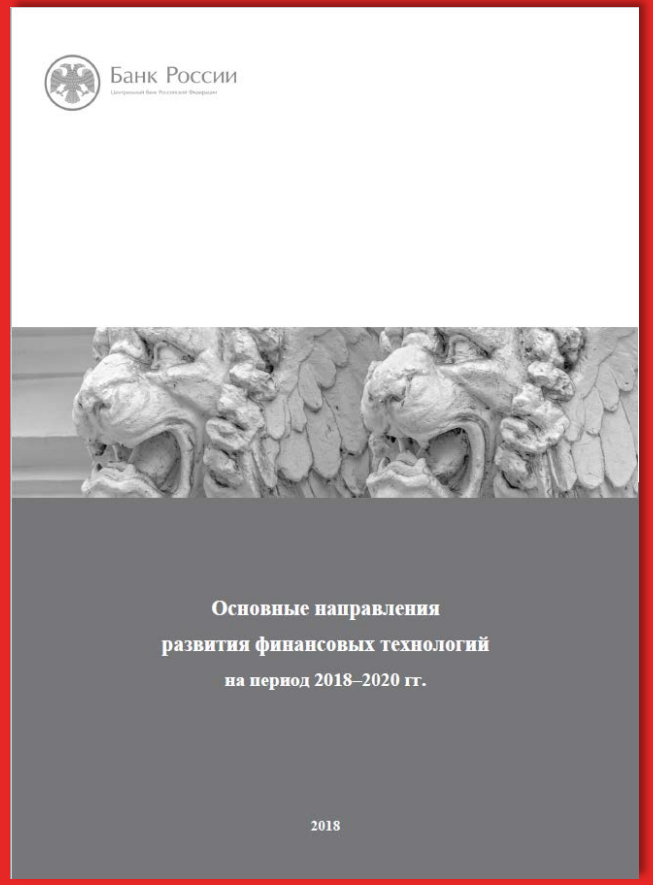
РЕШАЕМЫЕ ЗАДАЧИ

1. обнаружение и блокирование кибератак на защищаемые сегменты АБС, включая сегмент КБР, КБР М
2. выявление аномальной активности подконтрольных объектов
3. сбор и хранение информации о работе систем безопасности подконтрольных объектов
4. предоставление доступа ФинЦЕРТ к данным мониторинга подконтрольных систем
5. инвентаризация и мониторинг состояния подконтрольных объектов АБС
6. контроль защищенности ресурсов, обрабатывающих соответствующую информацию
7. анализ данных об актуальных угрозах ИБ и информирование соответствующих подразделений
8. анализ событий ИБ, решение задачи предупреждения кибератак
9. передача данных о состоянии информационной безопасности подконтрольного объекта, выявленных инцидентах ИБ и уязвимостях в ФинЦЕРТ или напрямую в ГосСОПКУ
10. доведение полученной информации до подконтрольных объектов в режиме реального времени

Подключение удаленных пользователей к защищенным облачным сервисам с использованием ПАК «ФАНТОМ-VIP»



Основные направления развития финансовых технологий на период 2018–2020 гг. (ЦБ)



КРАТКАЯ СУТЬ

Создание платформы для облачных сервисов

- направлено на сокращение затрат, связанных с созданием и использованием ИТ-инфраструктуры, для участников финансового рынка.
- Планируется подготовка предложений по созданию инфраструктуры облачных сервисов совместно с провайдерами ИТ-услуг, а также разработка
- рекомендаций по использованию облачных технологий участниками финансового рынка.

Платформа на основе технологии распределенных реестров

- вывод на рынок финансовых сервисов на базе технологии распределенных реестров совместно с участниками финансового рынка («Мастерчейн», иные).

Переход на электронное взаимодействие

- Расширение доступа финансовых организаций к государственным информационным ресурсам
- Электронный документооборот между Банком России, участниками финансового рынка, физическими и юридическими лицами
- Хранение и использование юридически значимых электронных документов, цифровизация документов на бумажном носителе
- Расширение использования простой и усиленной квалифицированных электронных подписей

Обеспечение безопасности и устойчивости при применении финансовых технологий

- проведение комплекса мероприятий по повышению технологической устойчивости, бесперебойности и безопасности при применении финансовых технологий, а также мониторингу состояния информационных систем финансовых организаций.

- Упрощение работ по контролю и аудиту
- Существенное снижение расходов самих организаций

Взаимодействие в рамках ГосСОПКИ

- Идет работа по созданию SOC в рамках системы лицензирования ФСТЭК по ТЗКИ (п. «в»).
- Получение статуса корпоративного центра ГосСОПКА.
- Заключение соглашения об информационном взаимодействии ЦБ по вопросам противодействия компьютерным атакам
- Подготовка к созданию коммерчески завершенного продукта – базы данных компьютерных атак.
- Дополнительная поддержка передовыми центрами выявления, отслеживания и реагирования на угрозы ИБ.
- Отработка вопросов мониторинга ИБ на стенде и внедрение продуктов в сеть Финтелеком.

ГОТОВНОСТЬ К ВНЕДРЕНИЮ РЕШЕНИЯ В ФИНАНСОВОМ СЕКТОРЕ И ВЗАИМОДЕЙСТВИЮ С ФинЦЕРТ В РЕЖИМЕ ОНЛАЙН.

ГОТОВНОСТЬ К ПРОХОЖДЕНИЮ ПРОЦЕДУРЫ АТТЕСТАЦИИ «ОБЛАЧНОГО СЕРВИСА» ПО ТРЕБОВАНИЯМ ФСТЭК и МКС

ТЕРРИТОРИЯ БЕЗОПАСНОСТИ

129515, Москва,
2-я Останкинская улица, д.6
+7 (495) 777 75 77
rnt@rnt.ru
www.rnt.ru

РОССИЙСКИЕ НАУКОЁМКИЕ ТЕХНОЛОГИИ