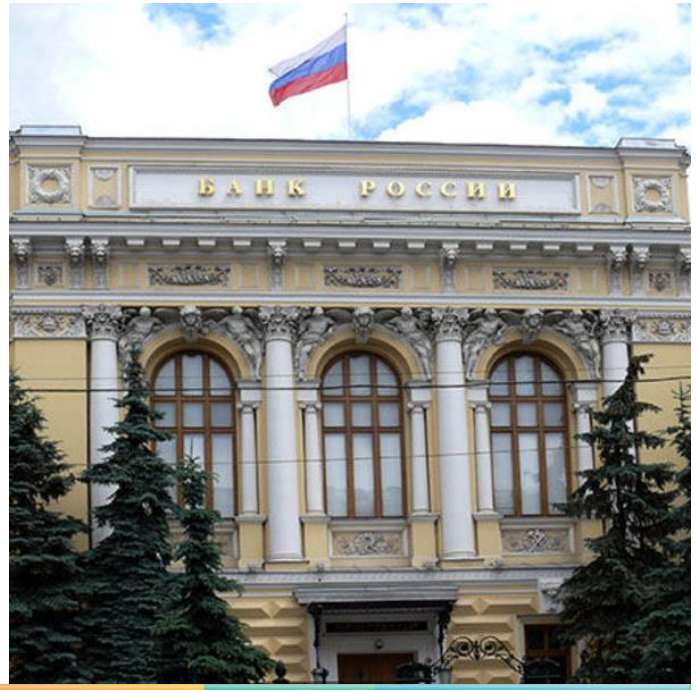


Руководитель ФинЦЕРТ Банка России
Калашников Артем Игоревич

IBS. Директор Отделения
информационной безопасности
Романченко Дмитрий Владимирович

Реализация АСОИ ФинЦЕРТ. Технологическая платформа

Основные цели деятельности ФинЦЕРТ

Динамика развития ФинЦЕРТ

- Автоматическое online получение данных из SIEM-систем
- Автоматизация всех процессов деятельности
- Расширенные показатели назначения
- Online анализ дампов трафика
- Максимально широкая экспертная база, автоматически пополняемая от российских и иностранных поставщиков
- Обеспечение неотказуемости (использование ЭП)
- Взаимодействие с иностранными участниками

2018

2-я очередь АСОИ ФинЦЕРТ

2017-2018

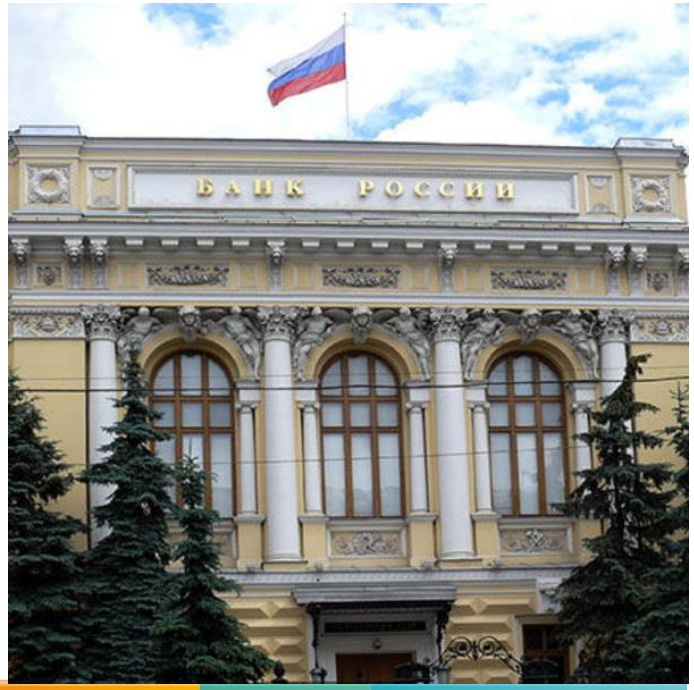
1-я очередь АСОИ ФинЦЕРТ

- Обмен с участниками через интегрированный защищенный портал и e-mail (получение информации в форматах XLSx и JSON)
- Автоматизация ключевых процессов
- Достаточные показатели назначения
- Автоматическое взаимодействие с ГосСОПКА
- Возможность взаимодействия с иностранными участниками

Настоящее время

Текущая инфраструктура ФинЦЕРТ

- Обмен с участниками по e-mail (получение информации в формате XLSx)
- Локальная автоматизация работы экспертов
- Функционирование базовых процессов



Общие сведения об АСОИ ФинЦЕРТ

Цели и задачи создания технологической платформы АСОИ ФинЦЕРТ

Создание единого механизма автоматизированного защищенного доверенного взаимодействия Банка России и Участников

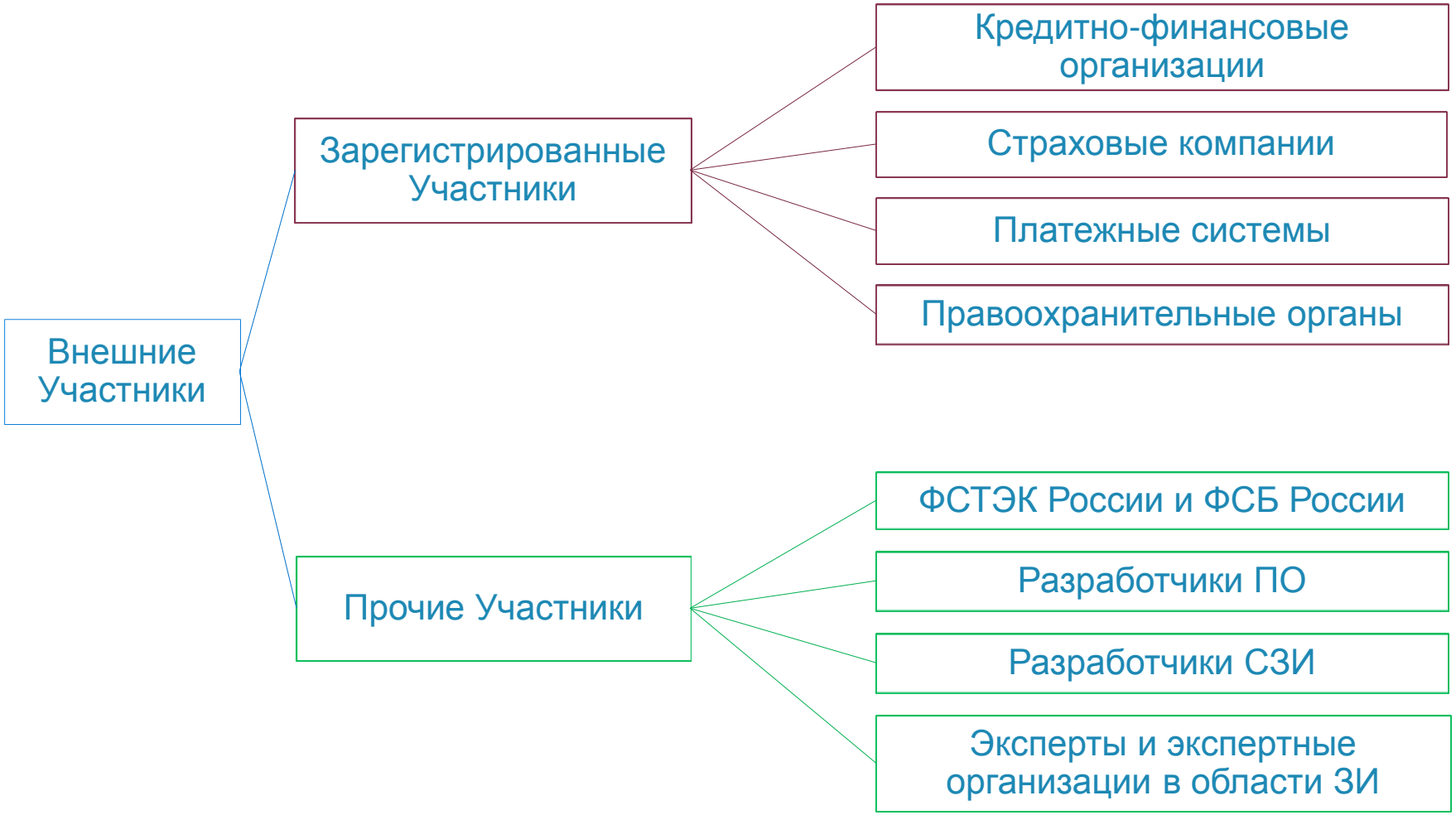
Технологическая поддержка процессов функционирования ФинЦЕРТ

Оперативное информирование Участников об актуальных угрозах ИБ в предметной области

Задачи АСОИ ФинЦЕРТ

- Создание информационно-сервисного портала Участников, Экспертов
- Обеспечение инфраструктуры защищенного доверенного взаимодействия
- Автоматизация обработки сведений об инцидентах, поступающих от Участников
- Обеспечение взаимодействия с ГосСОПКА
- Ведение базы знаний по уязвимостям, индикаторам компрометации, “паттернам” атак
- Ведение архива расследований инцидентов ИБ
- Мониторинг электронных СМИ с целью выявления информации, связанной с подготовкой и реализацией атак на организации кредитно-финансовой сферы

Участники информационного обмена АСОИ ФинЦЕРТ



Основные виды событий / атак, обрабатываемых в ФинЦЕРТ

- Реагирование на осуществление DDoS-атак
- Реагирование на хищение денежных средств (в т.ч. план реагирования)
- Реагирование на неправомерный доступ к КИ
- Реагирование на мошенничества с ДБО
- Реагирование на вредоносное ПО
- Реагирование на мошенничество с использованием фишинговых / мошеннических сайтов
- Реагирование на мошенничество с использованием средств связи (сотовой, 8-800)

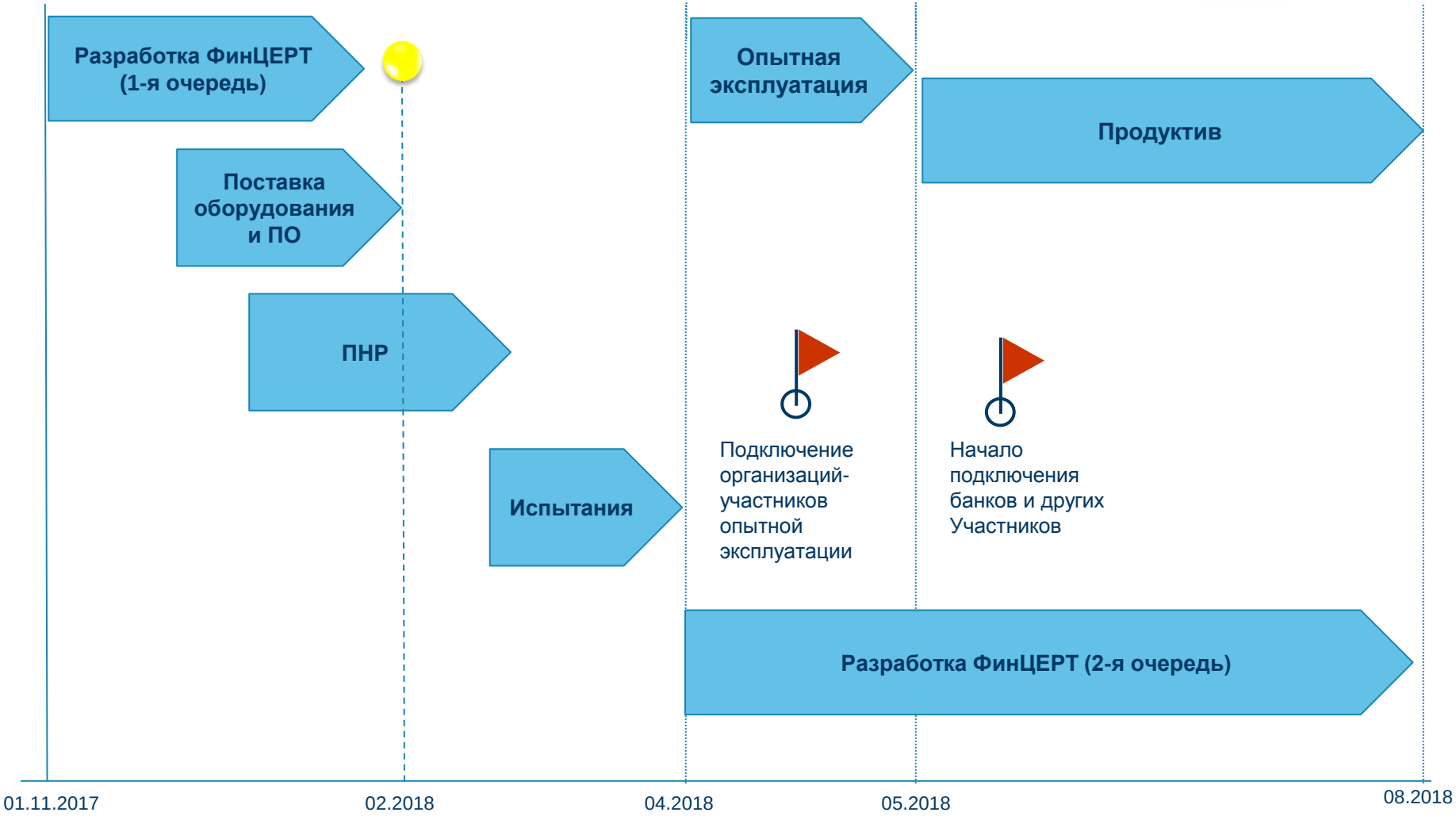
Основные прикладные процессы АСОИ ФинЦЕРТ

Получение информации (данных) от Участника	▪ Получение данных от Участника через ЛК ▪ Получение данных от Участника через e-mail ▪ Получение данных от Участника в автоматическом режиме (2-я очередь) ▪ Получение данных по телефону
Проведение мониторинга информационных ресурсов Интернет	▪ Мониторинг социальных сетей и ресурсов сети Интернет; ▪ Мониторинг СМИ и анализ распространителей информации (2-ая очередь)
Обработка информации о компьютерных атаках	▪ Выполнение процедур реагирования ▪ Проведение расследования (в т.ч. подготовка информации с правоохранительными органами) ▪ Взаимодействие с регистраторами и хостерами по блокировке мошеннических и вредоносных ресурсов
Формирование отчетности	▪ Подготовка и отправка оперативных уведомлений и бюллетеней ФинЦЕРТ ▪ Формирование отчетности по работе

Показатели назначения АСОИ ФинЦЕРТ

Показатель	1-я очередь	2-я очередь
Штатный режим работы	24x7x365	24x7x365
Количество принятых ЭСУ (электронное сообщение участника)	не менее 1000 в сутки (объем ЭСУ до 100 Кб)	не менее 10000 в сутки (объем ЭСУ до 100 Кб)
Пиковое значение принятых ЭСУ (до 100 Кб)	не более 250 в час	не более 2500 в час
Объем принимаемых файлов через личный кабинет	до 2 Гб	до 2 Гб
Количество одновременных сессий пользователей	до 1000	не менее 4000
Количество созданных тикетов	до 50 в минуту	
Объем принимаемого файла образа диска ПЭВМ (передаётся на физическом носителе)		до 5 Тб
Объем файла с дампом «грязного» трафика, принимаемого на исследования		до 50 Гб

План реализации АСОИ ФинЦЕРТ

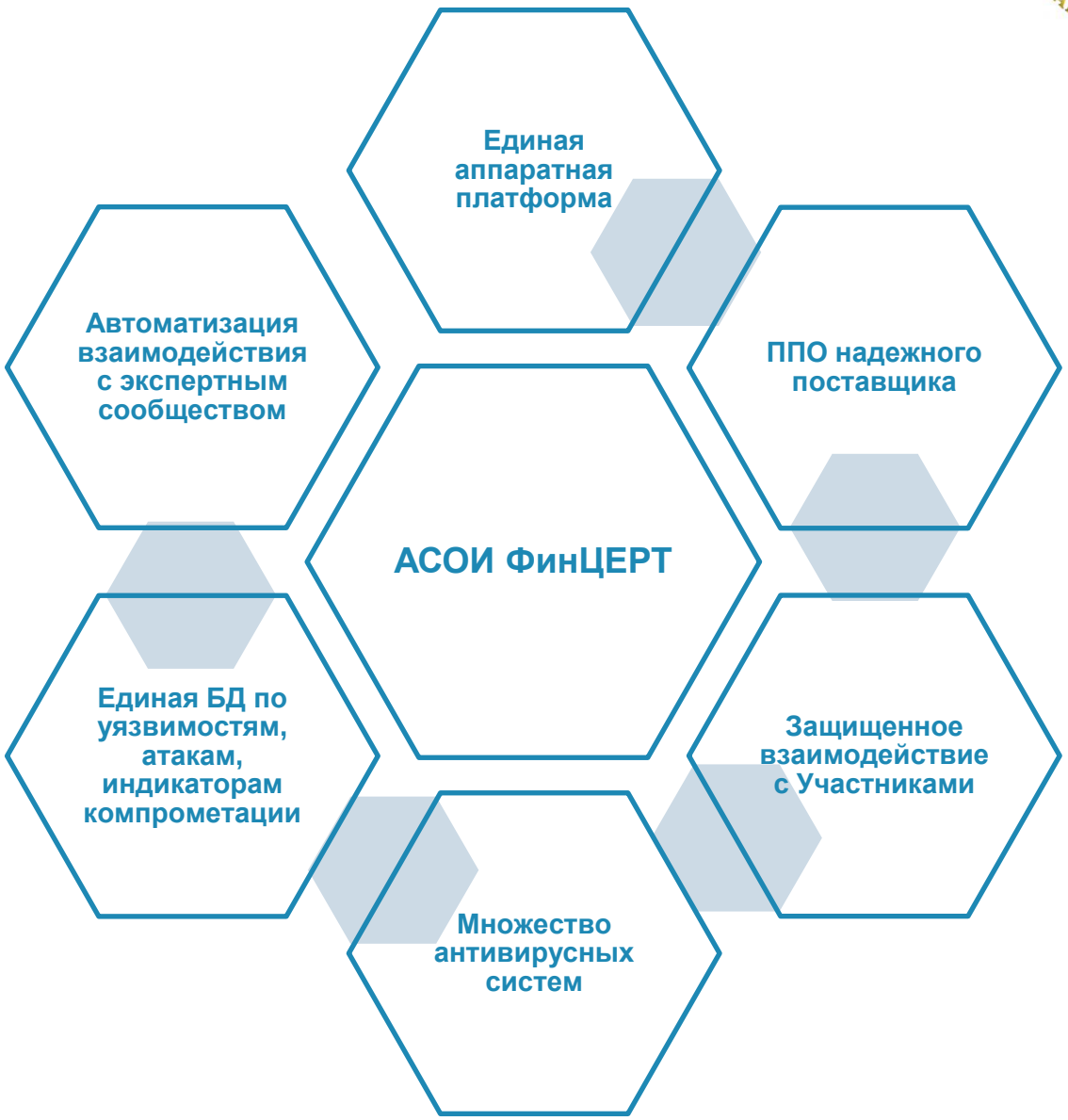


Этапы создания

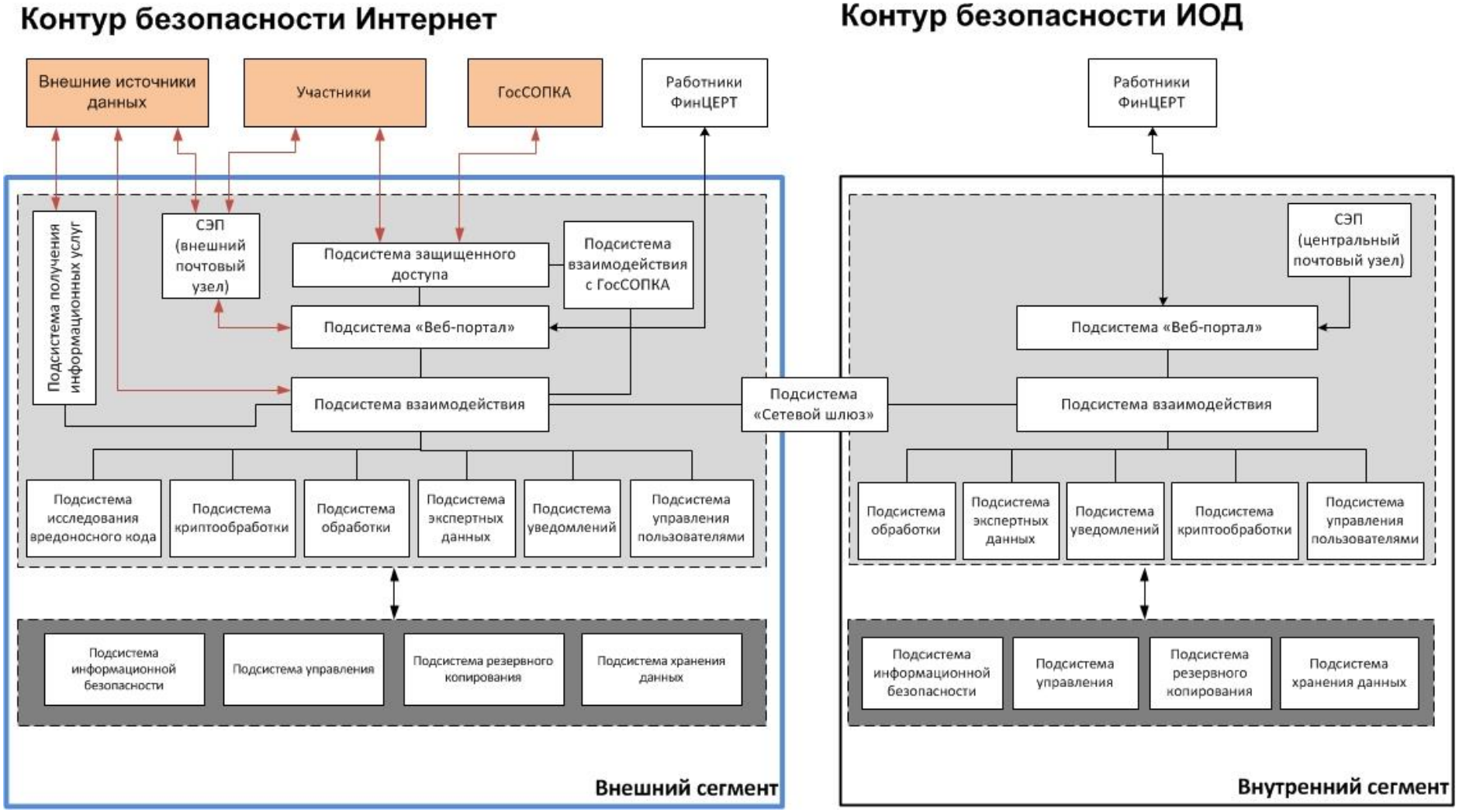
Текущий статус

Функционально-техническая архитектура ФинЦЕРТ

Основные принципы реализации АСОИ ФинЦЕРТ



Функциональная схема АСОИ ФинЦЕРТ



I.Состав функциональных подсистем АСОИ ФинЦЕРТ

№	Подсистема	Назначение
1	Подсистема «Веб-портал»	Информационное взаимодействие с Участниками и работниками Центра путем предоставления им авторизованного персонифицированного доступа к информационным ресурсам и сервисам АСОИ ФинЦЕРТ
2	Подсистема взаимодействия	Взаимодействие с внешними источниками данных и компонентов АСОИ ФинЦЕРТ между собой
3	Подсистема взаимодействия с ГосСОПКА	Взаимодействие АСОИ ФинЦЕРТ с ГЦ ГосСОПКА
4	Подсистема защищенного доступа	Организация защищенного канала обмена данными между АСОИ ФинЦЕРТ и Участниками
5	Подсистема обработки	Сервисы предварительной обработки ЭС и приведения их к виду, пригодному для обработки в АСОИ ФинЦЕРТ
6	Подсистема экспертных данных	Ведение базы знаний уязвимостей, признаков компрометации и иных экспертных данных
7	Подсистема исследования вредоносного кода	Прием и обработка контейнеров Образцов, их автоматизированный анализ, формирование отчетов по результатам анализа
8	Подсистема получения информационных услуг	Мониторинг внешних источников данных по заданным тематикам

II.Состав инфраструктурных подсистем АСОИ ФинЦЕРТ

№	Подсистема	Назначение
1	Подсистема «Сетевой шлюз»	Защищенное взаимодействие между внешним и внутренним сегментами АСОИ ФинЦЕРТ
2	Подсистема хранения данных	Ресурсы хранения данных АСОИ ФинЦЕРТ
3	Подсистема уведомлений	Обеспечивает рассылку уведомлений Участникам и работникам ФинЦЕРТ
4	Подсистема управления пользователями	Управление пользователями, их правами доступа в АСОИ ФинЦЕРТ
5	Подсистема информационной безопасности	Обеспечивает защиту информации от НСД и изменения (модификации, уничтожения), а также гарантирует неотказуемость операций (протоколирования действий персонала)
6	Подсистема резервного копирования	Резервное копирование и восстановление информации АСОИ ФинЦЕРТ
7	Подсистема управления	Обеспечивает управление и мониторинг функционирования ИТ-инфраструктуры и сервисов АСОИ ФинЦЕРТ, оперативного извещения персонала в случае отказов

Ключевые программные продукты, используемые в АСОИ ФинЦЕРТ

№	Ключевой функционал АСОИ ФинЦЕРТ	Техническое решение
1	Информационно-сервисный портал	▪ Positive Technologies Financial Cyber Security Platform
2	Автоматизация обработки инцидентов, поступающих от Участников	▪ Positive Technologies Financial Cyber Security Platform
3	Внутренняя система проверки файлов на наличие вредоносного ПО (включая специализированную песочницу)	▪ Positive Technologies Multiscanner ▪ Positive Technologies Financial Cyber Security Platform
4	Подсистема экспертных данных	▪ Positive Technologies Knowledge Base
5	Внешний сервис проверки файлов на наличие вредоносного ПО (включая специализированную песочницу)	▪ Сервис VirusLocal, Pushok (RU-CERT)
6	Взаимодействие с ГосСОПКА	▪ Positive Technologies Financial Cyber Security Platform
7	Инфраструктура доступа для участников информационного обмена к АСОИ ФинЦЕРТ	▪ Криптошлюзы защищенного удаленного доступа SSL/TLS
8	Сервис мониторинга СМИ и социальных сетей для обеспечения аналитической работы	▪ Различные сервисы, в том числе сервис «Крибрум»

Информационные источники АСОИ ФинЦЕРТ

Информационные источники*

Антивирусные движки

- PT MultiScanner
  - F-Secure
  - Dr.Web
  - Symantec
  - Avast
  - ESET NOD32
  - Avira
  - BitDefender
  - ClamAV
- PT Honeypot
- VirusLocal, Pushok (RU-CERT)

Репозитории уязвимостей

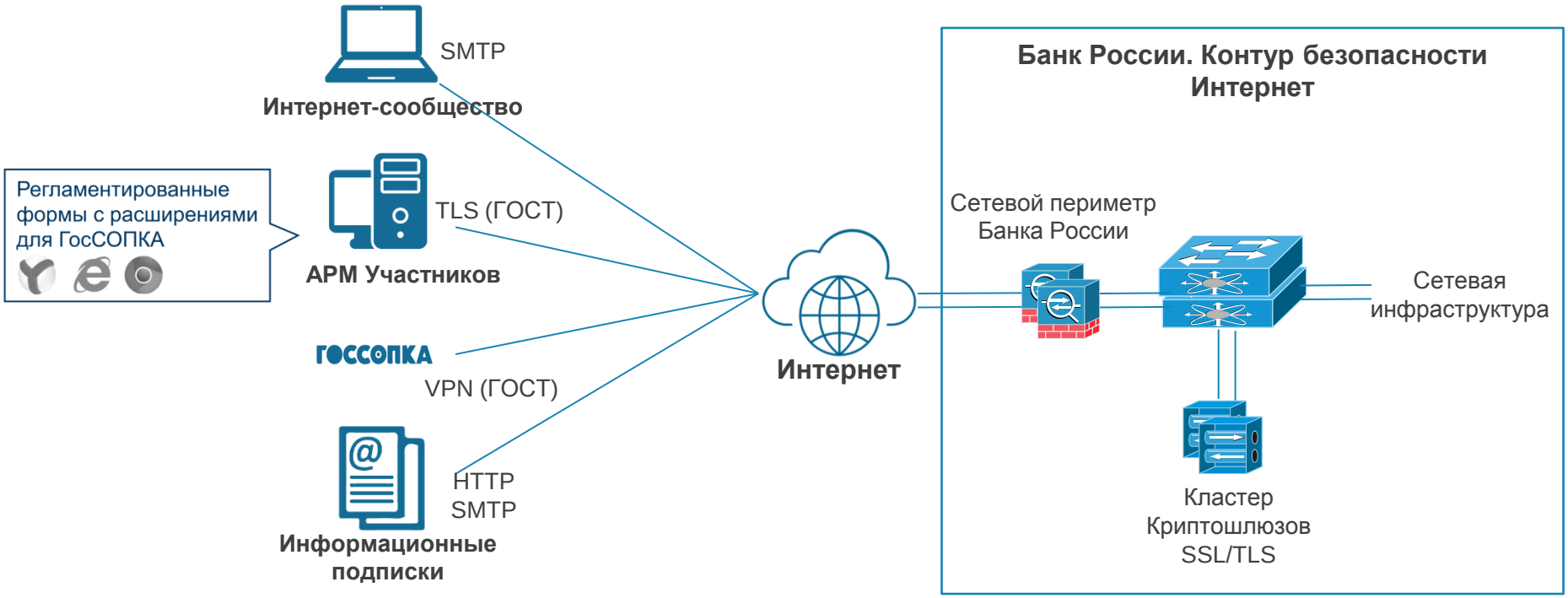
- PT Knowledge Base
  - ФСТЭК России (bdu.fstec.ru)
  - NIST (nvd.nist.gov)
  - OVAL (oval.cisecurity.org)

Электронные медиа

- «Крибрум»

Примечание* 1-я очередь

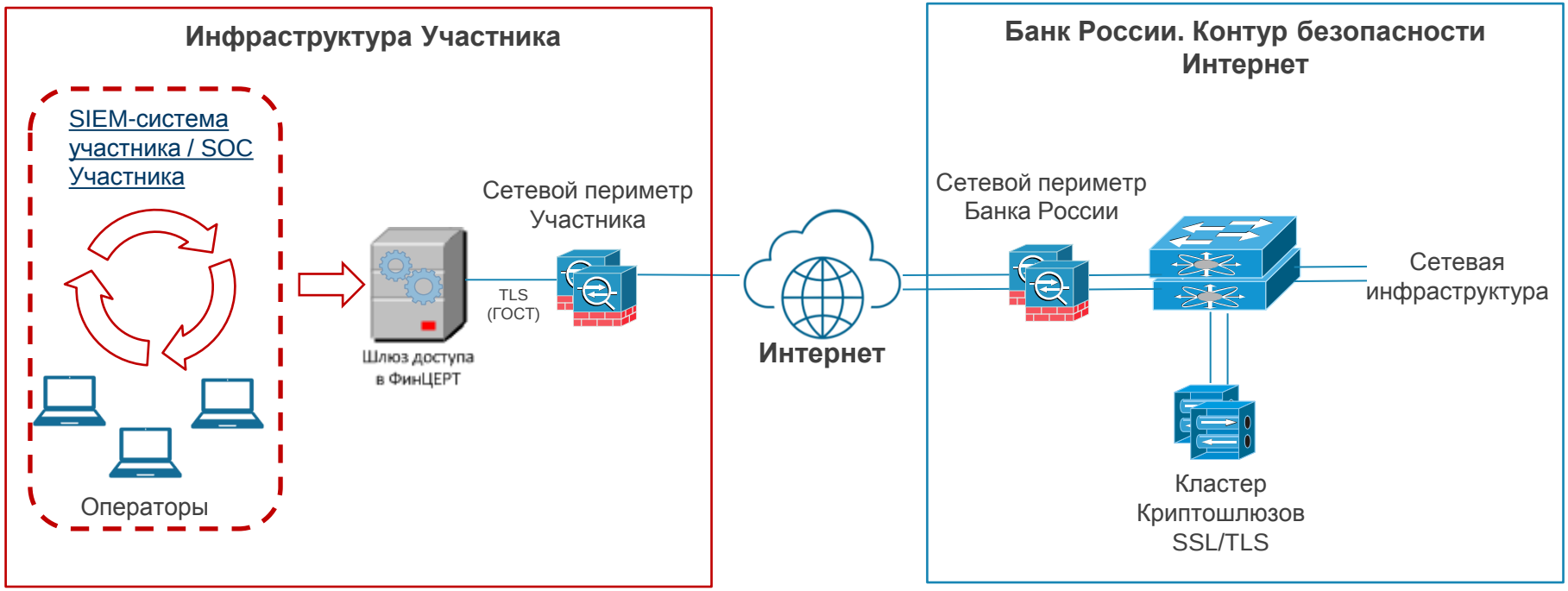
Организация подключения Участников и порядок взаимодействия (1-я очередь)



Регламентирующая документация

- http://www.cbr.ru/fincert/. Временный регламент передачи данных участников информационного обмена в Центр мониторинга и реагирования на компьютерные атаки в кредитно-финансовой сфере Банка России
- Регламент подключения участников информационного обмена к АСОИ ФинЦЕРТ
- Регламент работы с ключевой информацией
- Руководство Участника по работе с АСОИ ФинЦЕРТ

Расширение возможностей взаимодействия Участников (2-я очередь)



Канал автоматического межсистемного взаимодействия с Участниками

- Шлюз автоматической интеграции SIEM-систем / SOC Участника с АСОИ ФинЦЕРТ:
  - MaxPatrol SIEM (Positive Technologies)
  - ArcSight (MicroFocus)
  - QRadar (IBM)
- Автоматический прием инцидентов и дополнительной инф-ии, регистрация их в АСОИ ФинЦЕРТ и запуск процессов реагирования

Преимущества, получаемые при использовании АСОИ ФинЦЕРТ

- Безопасное и доверенное взаимодействие Участников с АСОИ ФинЦЕРТ
- Оперативность автоматизированного обмена информацией с большим количеством Участников
- Принятие решений экспертами ФинЦЕРТ на базе актуальной информации из национальных и международных источников, собираемой автоматически
- Возможность ретроспективного анализа компьютерных инцидентов в автоматизированном режиме на всей глубине хранения данных ФинЦЕРТ
- Формализация и автоматизация взаимодействия, как результат – повышение скорости и эффективности реагирования на инциденты и иную информацию
- Обеспечение централизованного взаимодействия Участников с ГосСОПКА через АСОИ ФинЦЕРТ – снижение сложности и стоимости взаимодействия для Участников
- Круглосуточный автоматический режим функционирования АСОИ ФинЦЕРТ

Спасибо за внимание!