SecretTechnologies

Создание системы защищенного обмена файлами между контурами информационной безопасности

на основе решения Secret Cloud Enterprise

Егор Изотов

Существующее положение

Сегментирование и поддержка нескольких контуров безопасности:

Внешний «открытый» контур безопасности

- Имеется доступ к ресурсам и сервисам в сети Интернет
- Разрешается регулируемая и контролируемая передача информации из открытого контура в закрытый

Внутренний «закрытый» контур безопасности

- Отсутствует доступ к расположенным вне закрытого контура информационным системам
- Передача конфиденциальной информации в открытый контур **не допускается**!
- Не конфиденциальная информация, может передаваться в открытый контур, или за его пределы

Как это делается обычно

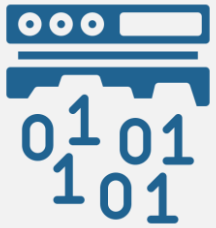
- Передача информации между контурами посредством USB-носителей
- Временный «проброс» сетевых соединений

Увеличенные риски и нагрузка на персонал, нестабильность процессов обмена данными

Утечки конфиденциальных данных

Неконтролируемое распространение данных

Проникновение вредоносного ПО

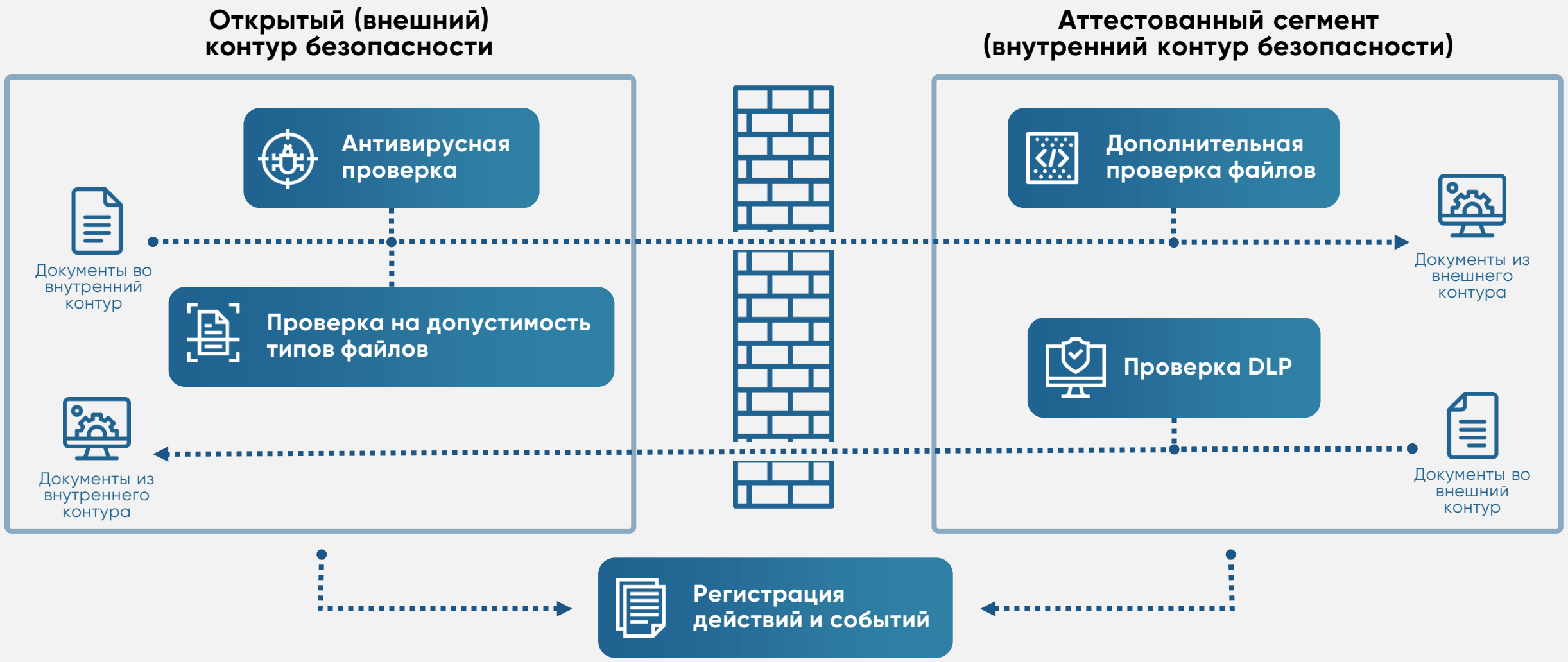


Потеря данных

Нарушение бизнес-процессов

Контролируемый безопасный обмен данными между контурами безопасности и внешними пользователями

Требования к процессу



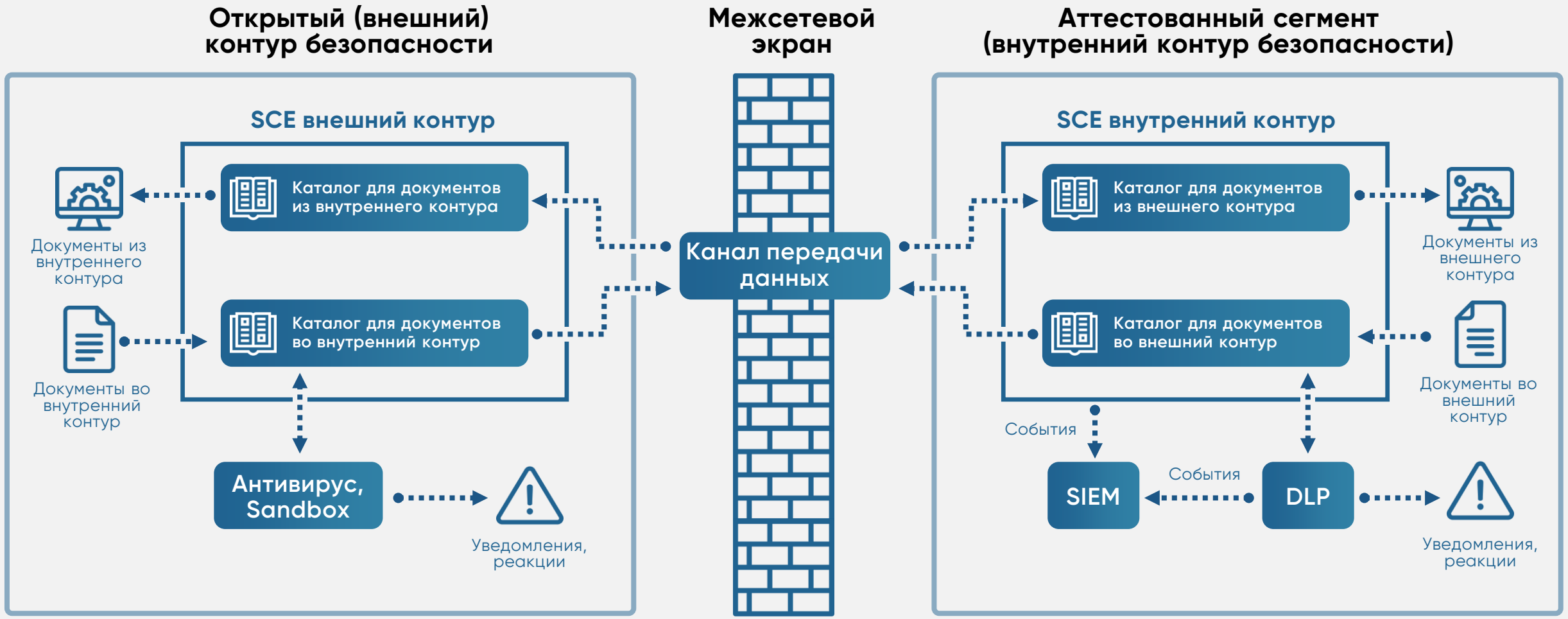
Решение

Построение системы защищенного обмена документами между различными контурами безопасности на основе защищенного облачного хранилища **Secret Cloud Enterprise**

Обеспечивается:

- Реализация процесса защищенного обмена информацией между различными контурами безопасности и внешними пользователями
- Соответствие требованиям к процессу межконтурного обмена информацией
- Сокращение неконтролируемого обращения носителей информации

Архитектура решения



Архитектура решения

Изолированные хранилища

Каждому контуру защиты информации сопоставляется свой, изолированный, экземпляр хранилища

Архитектура решения

Изолированные хранилища

Межсетевой экран

Внешний и внутренний контуры безопасности разделяются межсетевым экраном

Архитектура решения

Изолированные хранилища

Межсетевой экран

Защищённый протокол

Связь между хранилищами обеспечивается средствами API , по защищенному протоколу передачи данных

Архитектура решения

Изолированные хранилища

Межсетевой экран

Защищённый протокол

Антивирусная система

Каждый контур снабжен собственным экземпляром системы защиты от вредоносного ПО

Архитектура решения

Изолированные хранилища

Межсетевой экран

Защищённый протокол

Антивирусная система

DLP система

DLP обеспечивает минимизацию вероятности утечек информации

Архитектура решения

Изолированные хранилища

Межсетевой экран

Защищённый протокол

Антивирусная система

DLP система

SIEM система

Все системные события и события ИБ передаются в SIEM систему Предприятия

Почему Secret Cloud Enterprise

Полностью российская разработка,
в Едином реестре российского ПО
(Номер записи реестра: **10974**)

Решение сертифицировано **ФСТЭК РФ**
по **4 уровню доверия**

Может быть аттестовано
до ИСПДн У31/ГИС К1

Глубокая интеграция в системы
и бизнес-процессы Заказчика

Поддерживается распределенная
отказоустойчивая архитектура

Решение уже внедрено

Ростех

ОДК УМПО

АО «Центральная ППК»

РОСАТОМ

РусГидро

севернефтегазпром

Федеральная Налоговая Служба

ФКУ Налог Сервис ФНС России

Счётная палата Российской Федерации

SecretTechnologies

Ознакомиться с решением подробнее можно на нашем стенде

Москва, Волгоградский пр-т,
дом 43, корпус 3, офис 723,
БЦ «Авилон Плаза»

+7 (495) 109-29-50
info@secretgroup.ru
www.secretgroup.ru