PULKOVO

Airport

Особенности защиты информации в сетях АСУ ТП аэропортовой инфраструктуры

Март 2025

ТРЕБОВАНИЯ К БЕЗОПАСНОСТИ СЕТЕЙ АСУ ТП

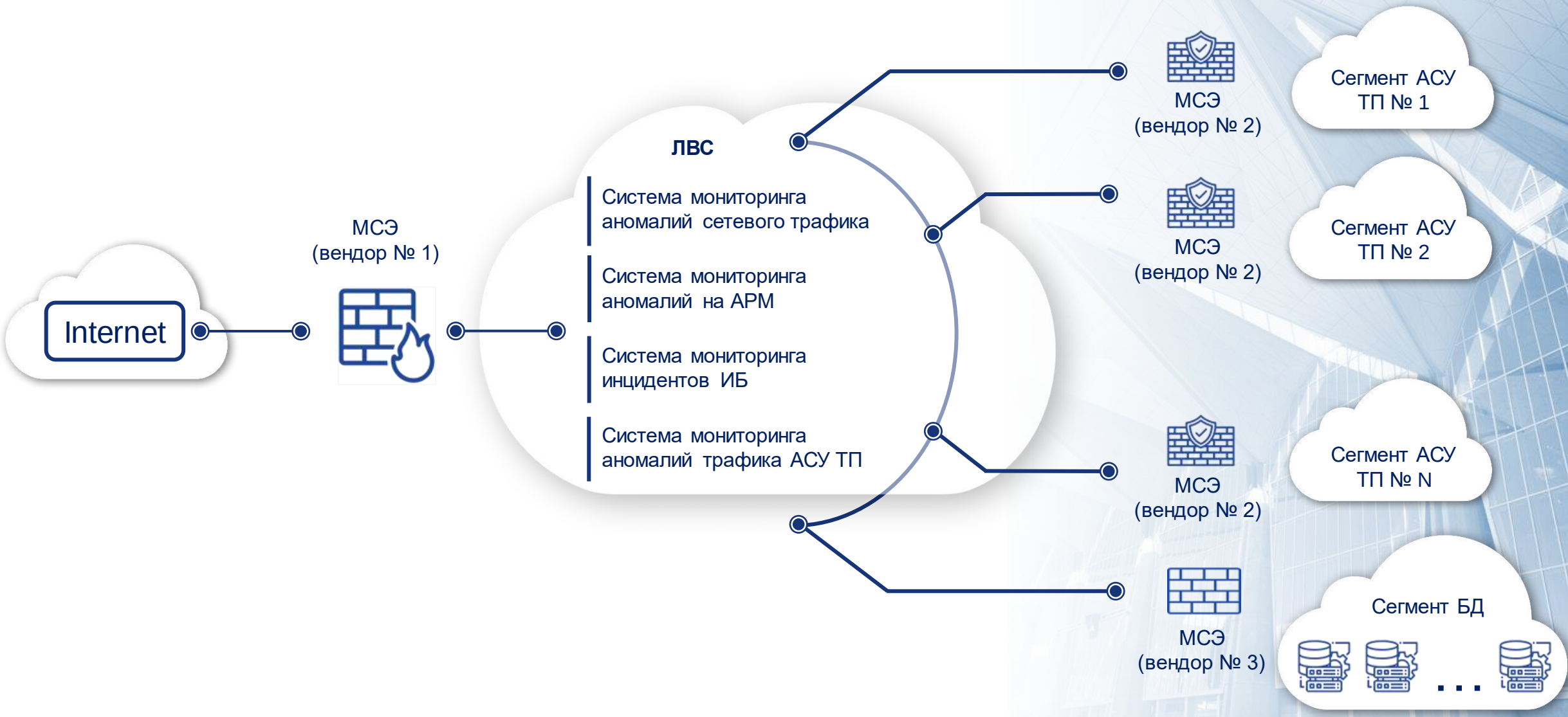
Приказ ФСТЭК России от 14.03.2014 г. № 31

«Об утверждении Требований к обеспечению защиты информации в автоматизированных системах управления производственными и технологическими процессами на критически важных объектах, потенциально опасных объектах, а также объектах, представляющих повышенную опасность для жизни и здоровья людей и для окружающей природной среды».

Приказ ФСТЭК России от 25.12.2017 г. № 239

«Об утверждении Требований по обеспечению безопасности значимых объектов критической информационной инфраструктуры Российской Федерации».

СХЕМА ПОСТРОЕНИЯ МНОГОВЕНДОРНОЙ ЗАЩИТЫ АЭРОПОРТА



ПЛЮСЫ И МИНУСЫ ПОСТРОЕНИЯ МНОГОВЕНДОРНОЙ ЗАЩИТЫ

- необходимость наличия в штате специалистов по всем системам и оборудованию;
- работа с различными командами технической поддержки;
- невозможность получения скидок за объем используемого ПО от одного вендора.

- при проведении кибератаки злоумышленникам приходится «ломать» не похожие системы от одного вендора, а разные по своей сути, от различных вендоров;
- специалисты, работающие с данными системами, становятся разносторонне подготовленными;
- время на реакцию со стороны специалистов ИБ в связи с многоэшелонированной системой защиты увеличивается, что позволяет вовремя среагировать на инциденты ИБ;
- в случае ухода с рынка одного из вендоров предприятие будет защищено оборудованием оставшихся вендоров.

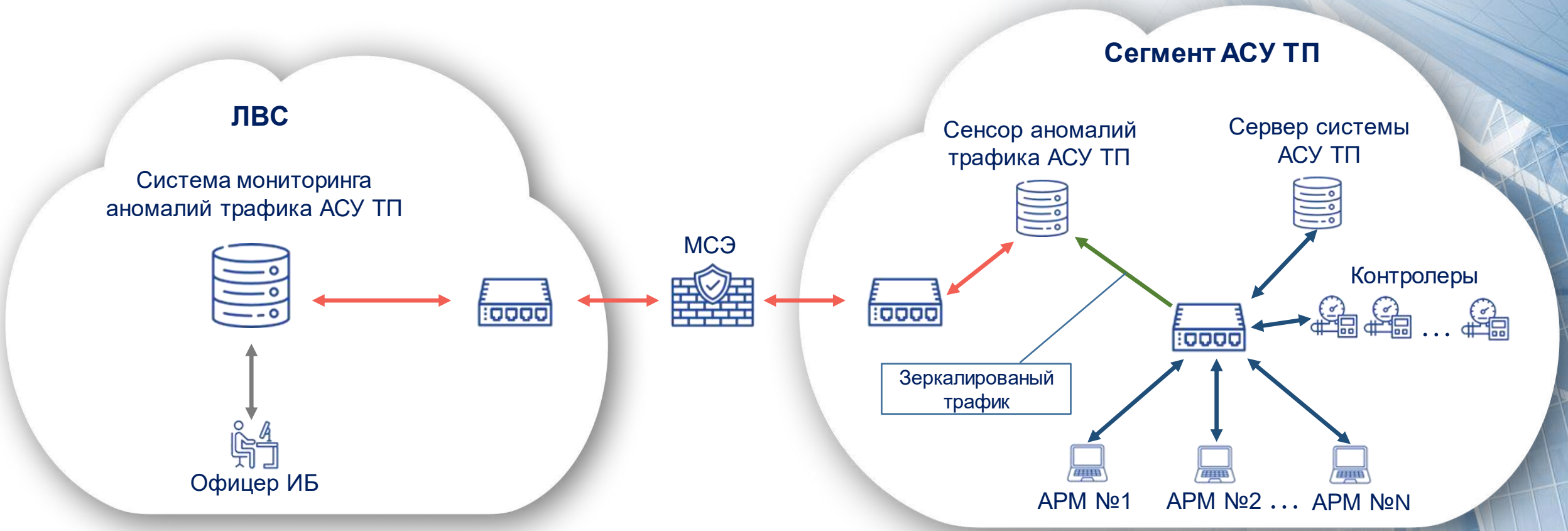
ОРГАНИЗАЦИЯ ЭКСТРЕННОГО УДАЛЕННОГО ДОСТУПА

ПЛЮСЫ И МИНУСЫ ОРГАНИЗАЦИИ ЭКСТРЕННОГО УДАЛЕННОГО ДОСТУПА

- продолжительное время на подключение к сервисам;
- в случае возникновения проблем при соединении поиск причин в большом количестве возможных точек отказа;
- предоставление данного вида доступа на временной основе;
- необходим фиксированный IP-адрес на подключаемой стороне для обеспечения максимальной безопасности;
- высокая стоимость систем.

- исключение неконтролируемого подключения к сервисам предприятия;
- контроль работы внешних специалистов на внутренних сервисах;
- логирование + видеозапись всех действий внешних пользователей;
- экстренное прерывание сессии в случае возникновения подозрительных действий со стороны внешних пользователей;
- контроль рабочего времени внешних пользователей на ресурсах предприятия.

ОРГАНИЗАЦИЯ КОНТРОЛЯ С ИСПОЛЬЗОВАНИЕМ СИСТЕМ МОНИТОРИНГА ТРАФИКА АСУ ТП



ПЛЮСЫ И МИНУСЫ КОНТРОЛЯ С ИСПОЛЬЗОВАНИЕМ СИСТЕМ МОНИТОРИНГА ТРАФИКА АСУ ТП

–

- установка в каждом сегменте АСУ ТП собственного сенсора для мониторинга аномалий в трафике АСУ ТП;
- работа сенсоров поддерживает анализ не всех проприетарных протоколов;
- недостаточное количество вендоров на рынке;
- малое количество специалистов на рынке труда, умеющих работать с данными системами.

+

- единая точка мониторинга аномалий на всех сегментах АСУ ТП;
- существование режима обучения перед вводом в режим постоянной работы;
- поддержка большого количества протоколов;
- построение топологической схемы взаимодействия сервисов в сегменте АСУ ТП.

ПУЛКОВО
Аэропорт Санкт-Петербурга

СПАСИБО ЗА ВНИМАНИЕ!

Начальник службы по обеспечению
информационной безопасности
ООО «Воздушные Ворота Северной Столицы»
Савченко Сергей Юрьевич
S.Savchenko@pulkovo-airport.com