CONEWS FORUM

Информационная безопасность предприятий – глухой забор или выстраивание киберустойчивого периметра

«Если ты откроешь эту дверь, ты не сможешь контролировать то, что в нее войдет…»

Ганнибал Лектер

Раньше было так…
или «Добро пожаловать»

- неограниченный доступ к Wi-Fi в корпоративной сети

- неограниченные доступы к USB-портам

- неограниченный удаленный доступ к ресурсам предприятия

- неограниченный доступ в сеть Интернет из корпоративной сети

Предпосылки к усилению требований в области ИБ

Иллюзия выбора

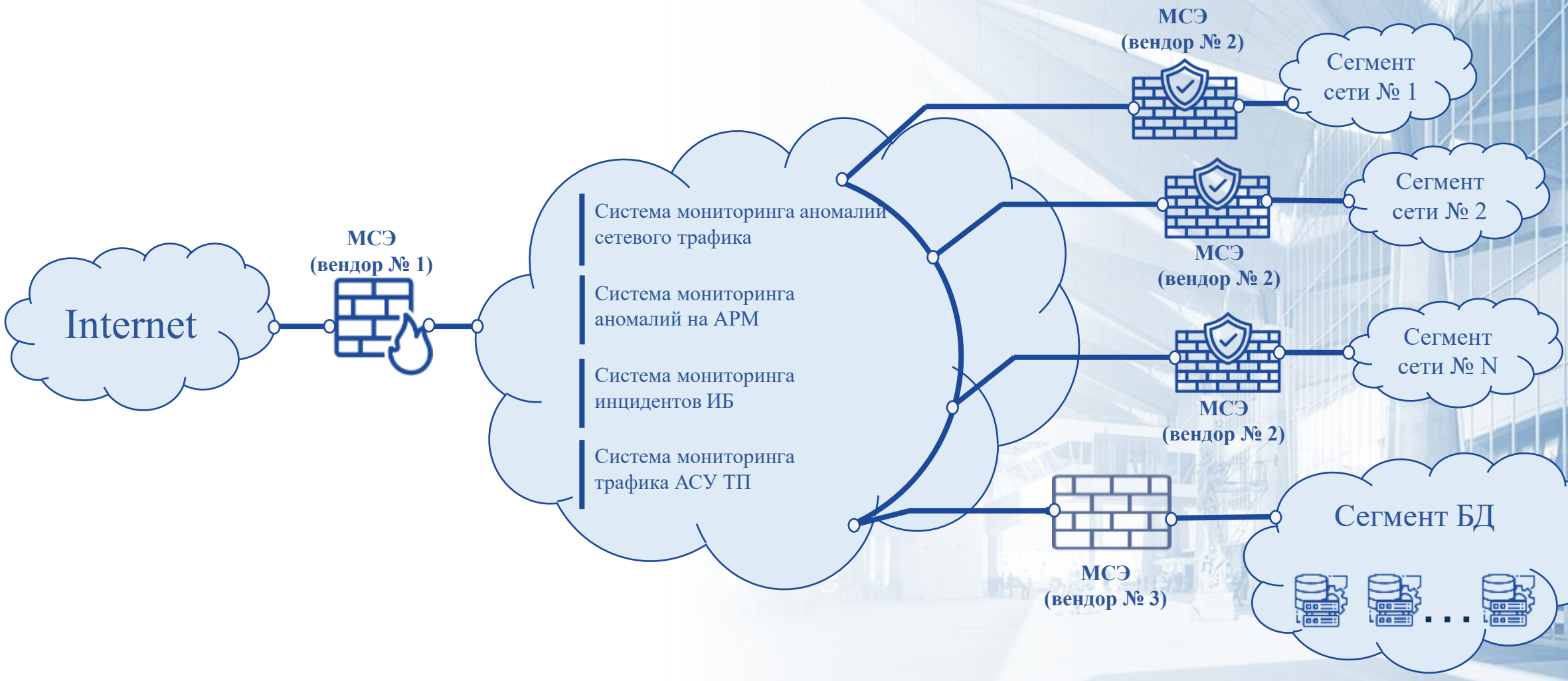
«глухой» забор по периметру
(новые требования)

или

свободный доступ в периметр
(старые желания)

Главный вопрос

Схема построения многоэшелонированной защиты



Плюсы и минусы многоэшелонированной защиты

Минусы

- 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.

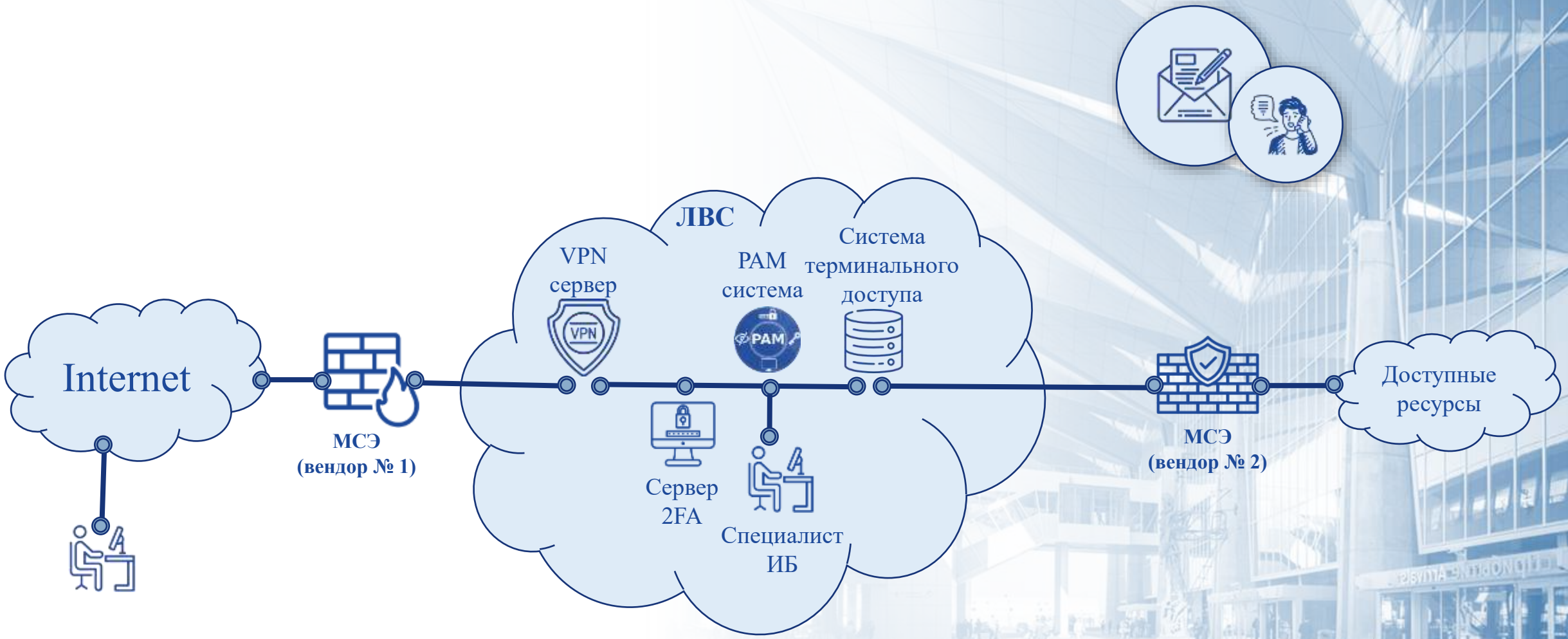
Плюсы

- 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.

Отраженные атаки

А дальше что?...

Организация защищенного удаленного доступа



Плюсы и минусы экстренного удаленного доступа

Минусы

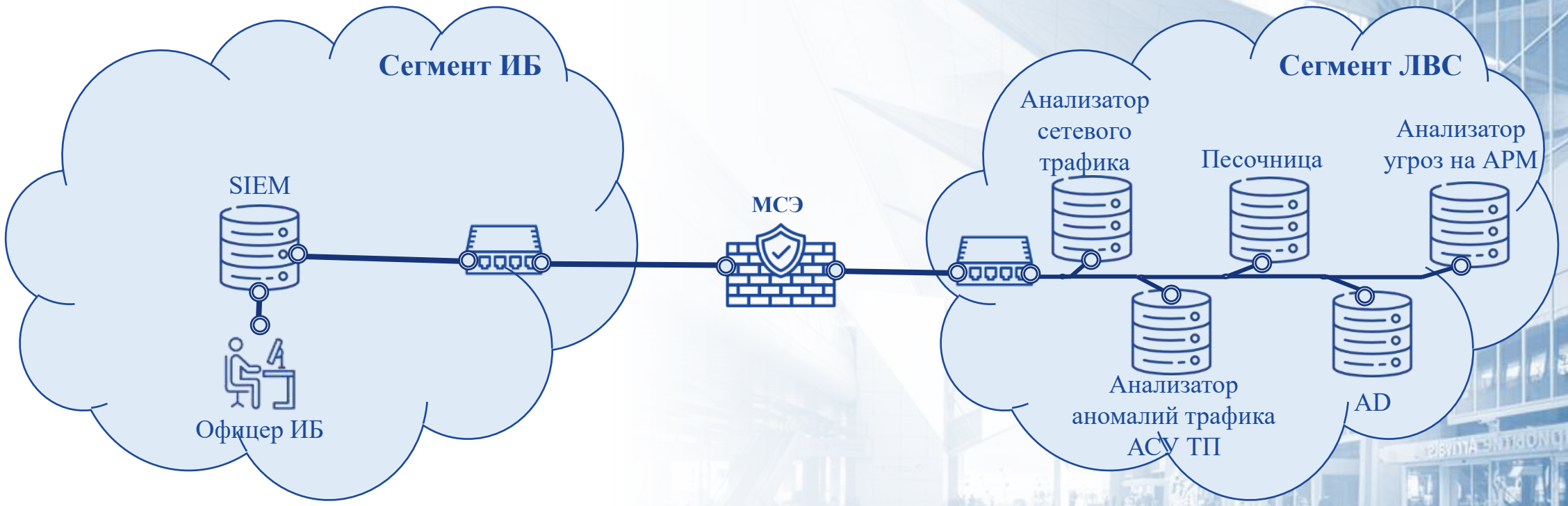
- продолжительное время на подключение к сервисам;
- в случае возникновения проблем при соединении поиск причин в большом количестве возможных точек отказа;
- предоставление данного вида доступа на временной основе (экстренный доступ);
- необходим фиксированный («белый») IP-адрес на подключаемой стороне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

Плюсы

- 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.

А как всё это контролировать?

Организация мониторинга и контроля со стороны ИБ



Плюсы и минусы мониторинга и контроля со стороны ИБ

Минусы

- большое количество событий, которые необходимо обработать, особенно в пиковые нагрузки;
- организационно-штатная проблема – людей всегда не хватает;
- подготовленных специалистов на рынке труда, готовых сразу работать на системах мониторинга и контроля, на данный момент минимальное;
- необходимость обучения персонала ИБ для работы с системами от разных производителей.

Плюсы

- возможность мониторинга и контроля из единой точки;
- возможность более оперативного реагирования на события и инциденты, имея все данные в едином интерфейсе;
- удобное получение данных из единой точки при проведении расследований инцидентов ИБ;
- специалисты, работающие с данными системами, прокачивают собственные скилы по различным производителям.

Дальнейшие пути развития

Постоянное увеличение количества событий и инцидентов ИБ, а также растущий спрос на специалистов ИБ и их нехватка на рынке труда подводит нас к необходимости использования высокоуровневых систем мониторинга ИБ с использованием ИИ.

Выводы

1. Требования регуляторов ужесточаются с каждым годом и необходимо строить максимально защищенные периметры предприятий и системы ИБ, особенно для субъектов КИИ.
2. В случае необходимости, существует возможность взаимодействия с внешними пользователями по схемам, согласованным с регуляторами. Но данные схемы требуют значительных как финансовых, так и человеческих затрат, что может являться стоп-фактором для большинства предприятий.
3. Одна из самых значительных проблем, на данный момент, является нехватка персонала, поэтому приходится рассматривать системы ИБ с использованием ИИ. Но на данный момент это не является панацеей и в ближайшее будущее такие системы будут использоваться при непосредственном участии человека. Данные системы также требуют значительных финансовых затрат и времени специалистов на их настройку.

ПУЛКОВО
Аэропорт Санкт-Петербурга

СПАСИБО ЗА ВНИМАНИЕ!

Начальник службы по обеспечению информационной безопасности
ООО «Воздушные Ворота Северной Столицы»
Савченко Сергей Юрьевич