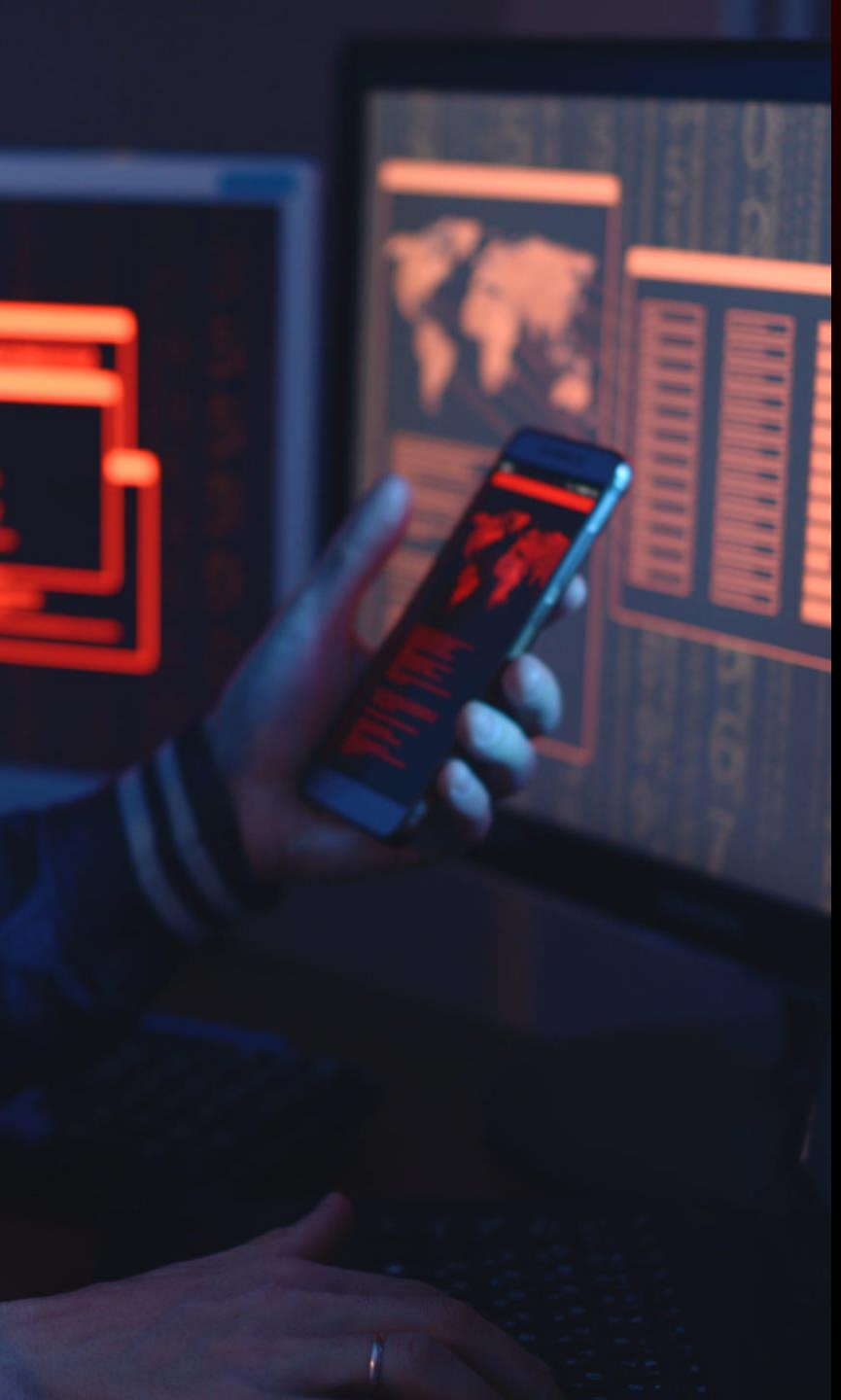
Игорь Тюкачев

Руководитель направления сетевой безопасности

+7 909 942 18 60

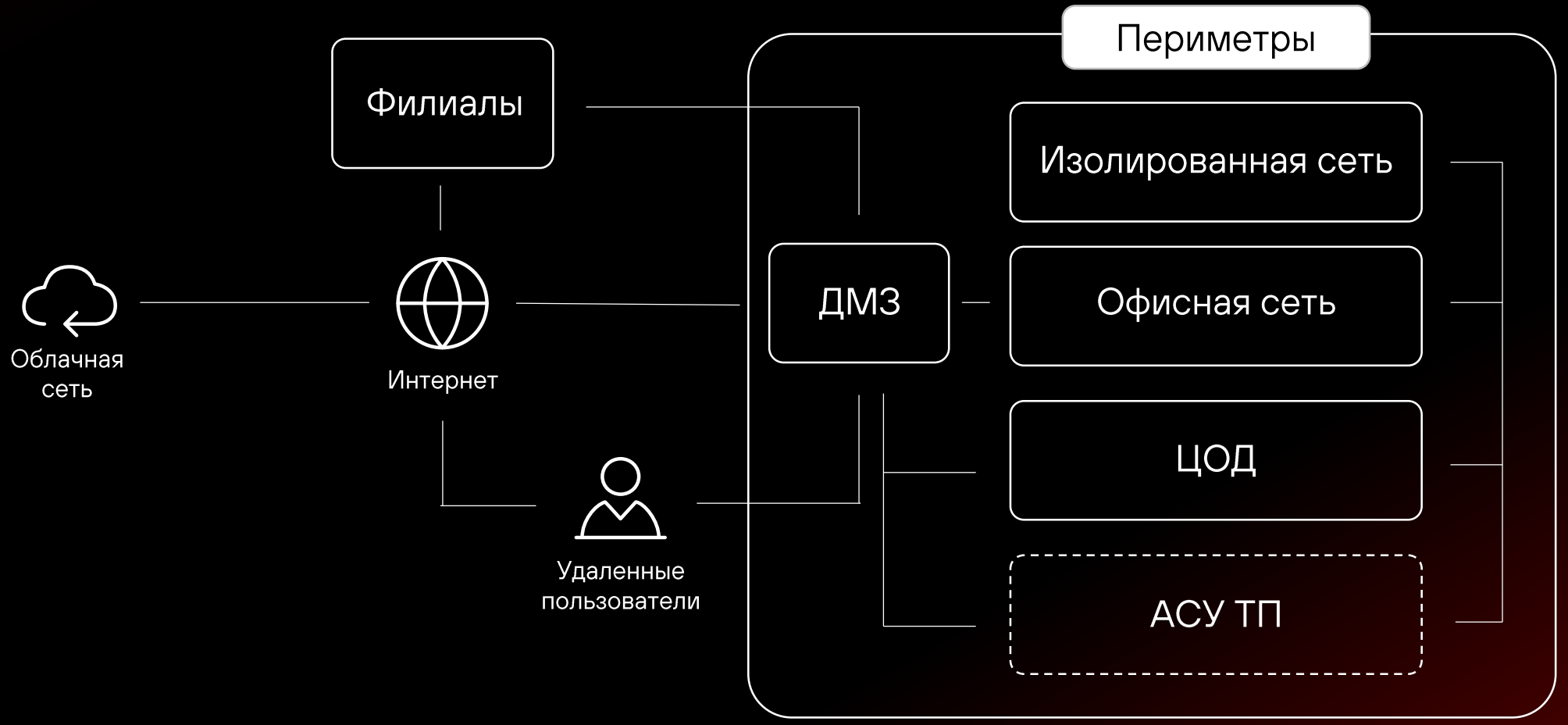
ityukachev@ptsecurity.com

Подходы к построению сетевой безопасности



Что у нас в 2024?

Классическая инфраструктура



Этапы атаки

1 Разведка

- Сбор данных о сотрудниках
- Сбор данных о компании
- OSINT
- Фишинг для сбора сведений

2 Подготовка

- Найм экспертов
- Ransomware as a service
- Собственная разработка
- Подготовка инфраструктуры

3 Первоначальный доступ

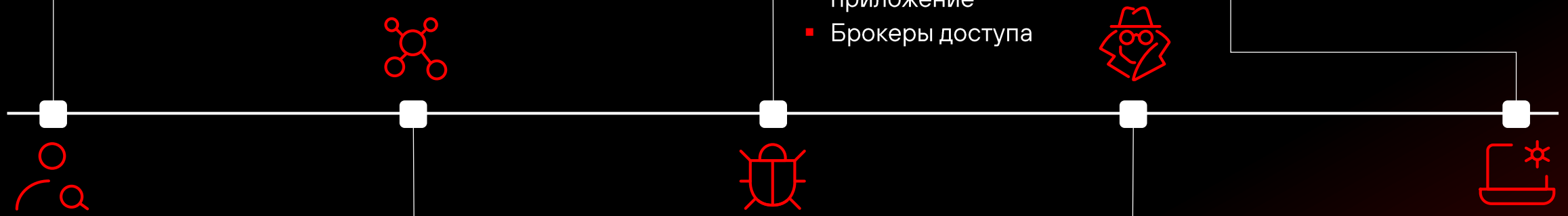
- Фишинг
- Уязвимости RDP и облачных хранилищ
- RCE / Уязвимости ПО
- Взломанное веб-приложение
- Брокеры доступа

4 Постэксплуатация

- Повышение привилегий
- Обеспечение резервного доступа
- Горизонтальное перемещение
- Кража данных

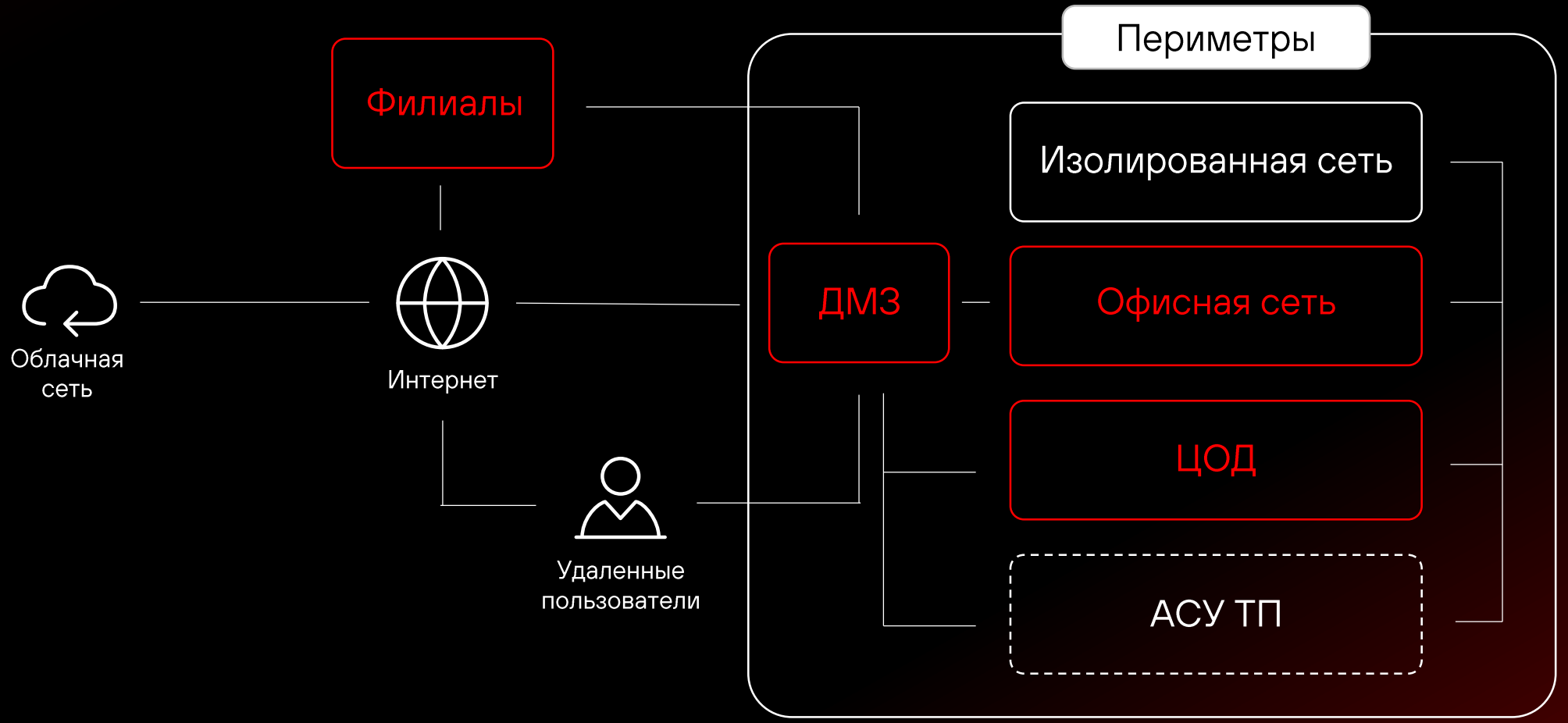
5 Нанесение ущерба

- Шифрование
- Остановка бизнес процесса
- Ущерб

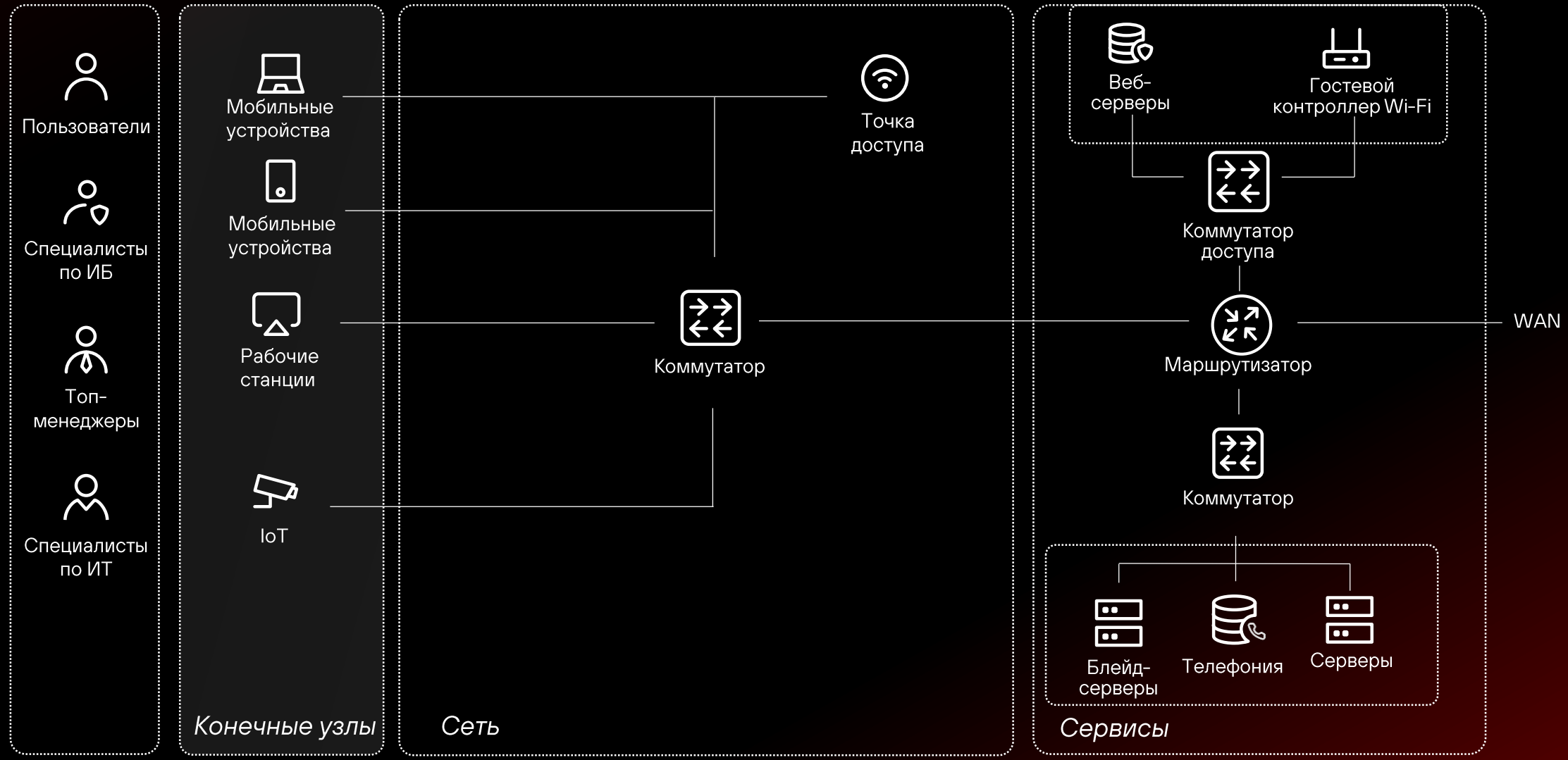


Это описание стандартных действий злоумышленников при атаке

Классическая инфраструктура



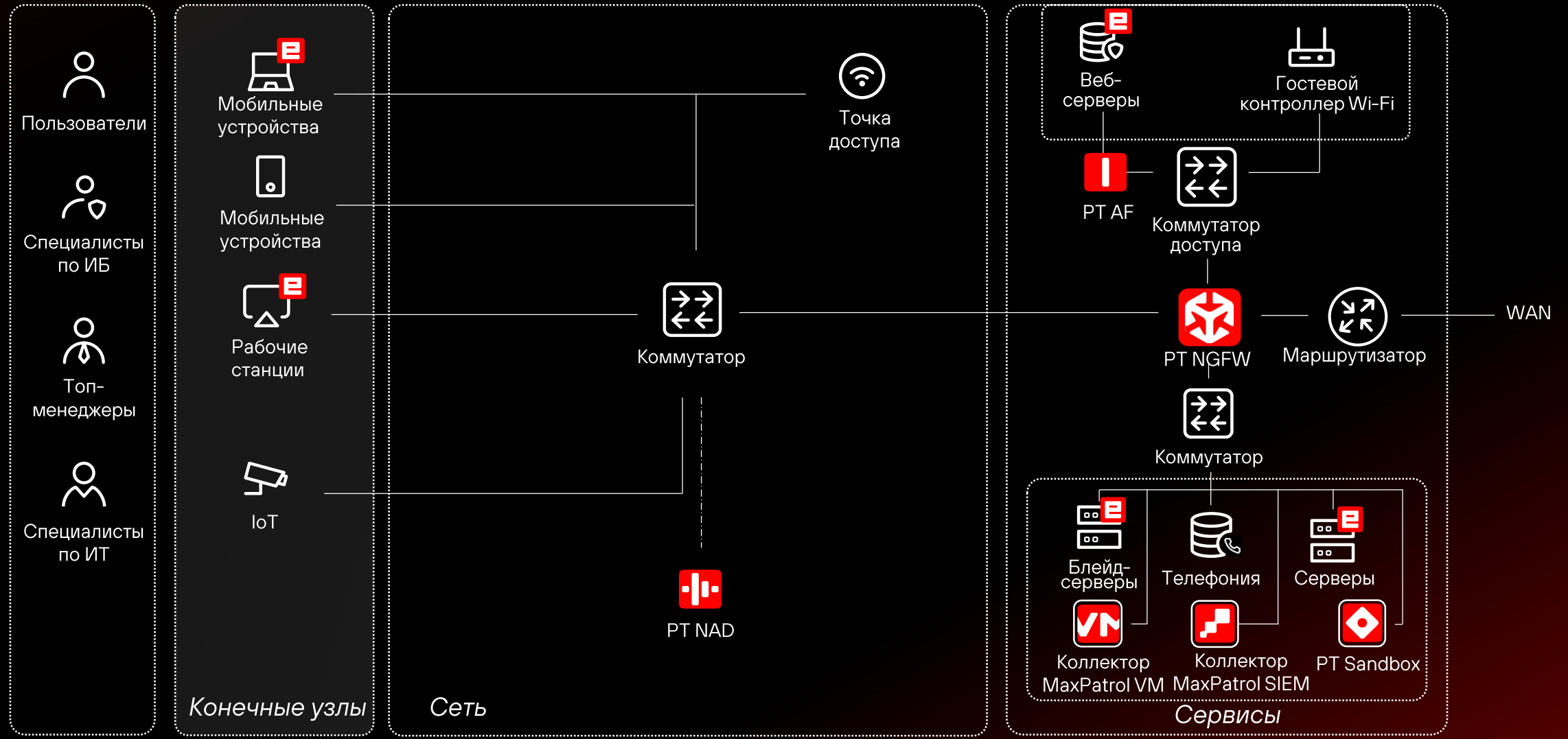
Офисная сеть



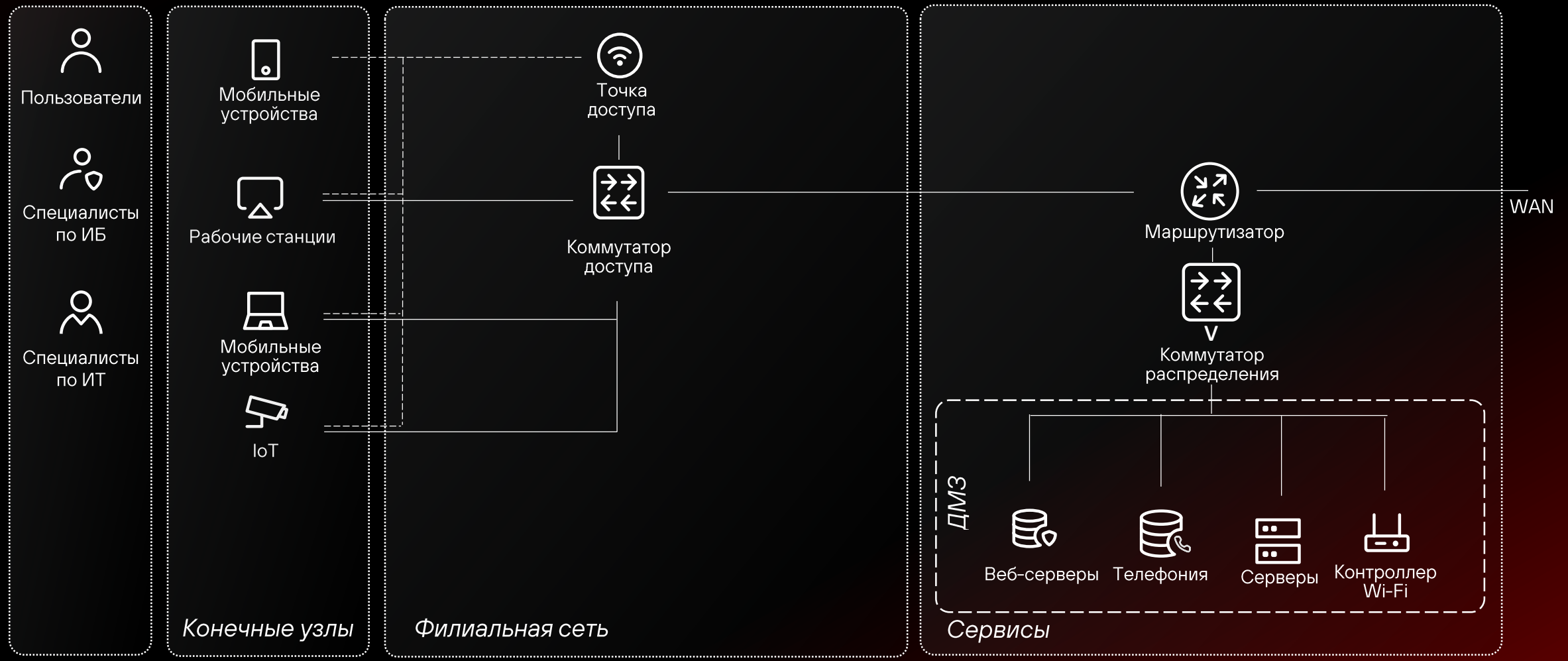
Особенности офисной сети

- Много зон безопасности
- Много рабочих станций
- Корпоративные мобильные устройства
- Личные устройства
- Личные мобильные устройства
- Доступ к интернету
- Гостевые пользователи
- Интернет вещей (управляемых и не очень)
- Служебные серверы
- Наличие квалифицированного персонала по ИТ и ИБ
- Руководство компании

Защита офисной сети



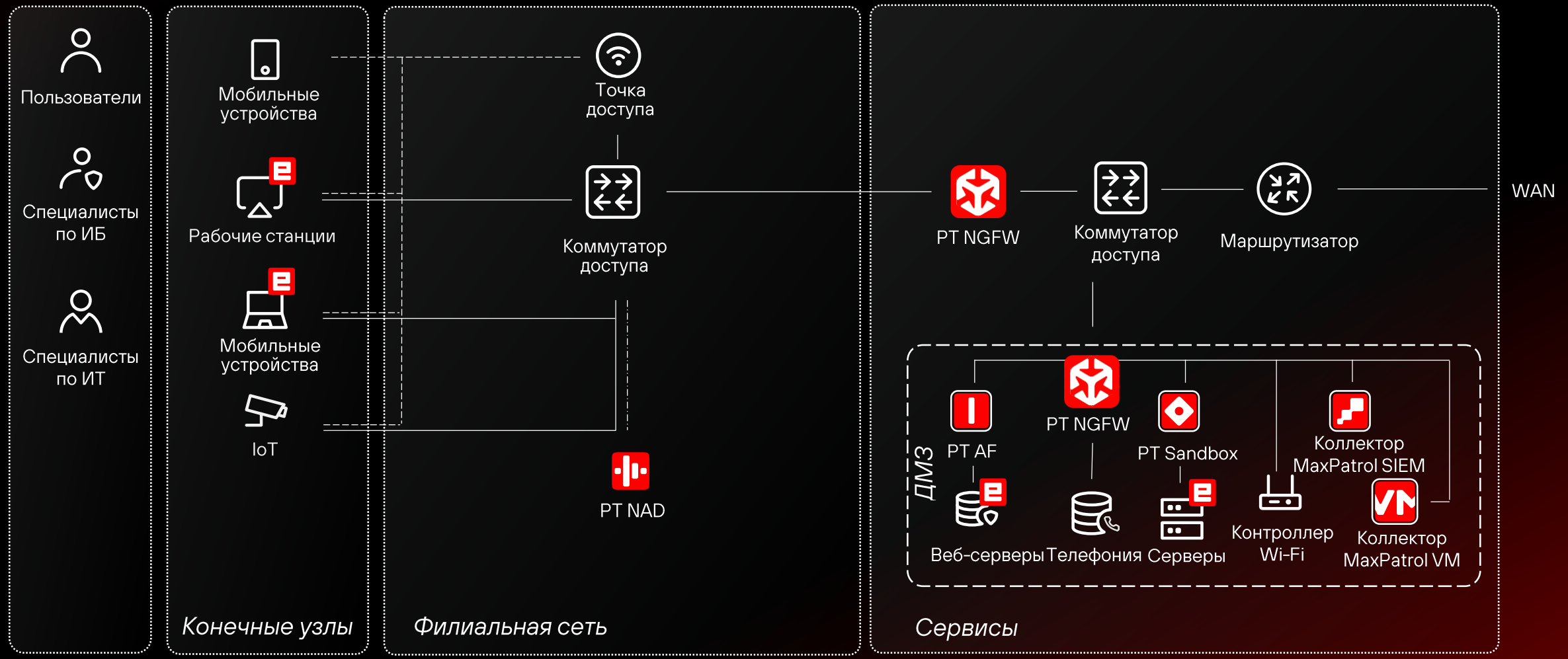
Сеть филиала



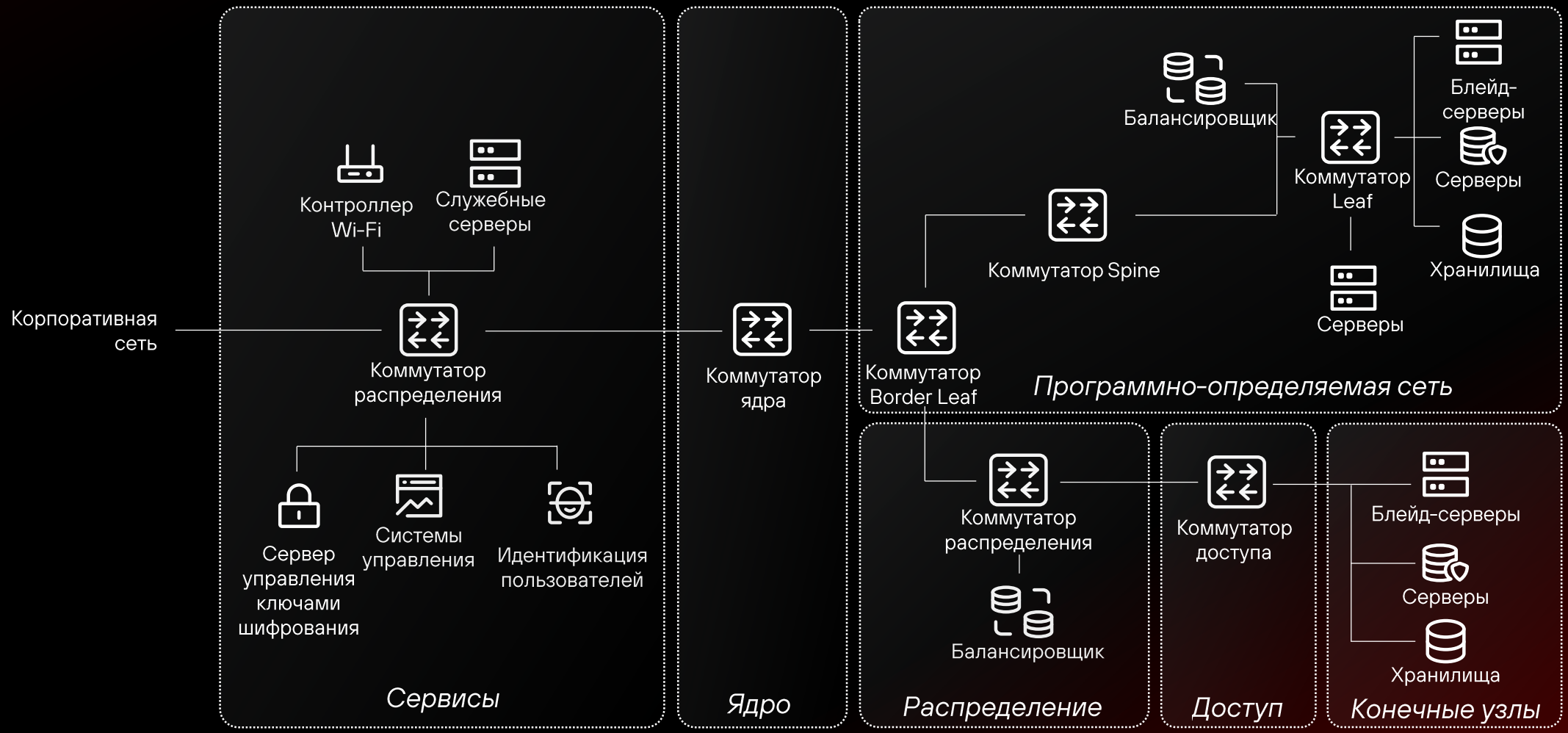
Особенности сети филиала

- Несколько зон безопасности
- Много рабочих станций
- Корпоративные мобильные устройства
- Личные устройства
- Личные мобильные устройства
- Может быть доступ к интернету
- Могут быть гостевые пользователи
- Квалифицированный персонал по ИТ
- Может отсутствовать квалифицированный персонал по ИБ
- Может быть руководство
- Служебные серверы
- Интернет вещей (управляемых и не очень)

Защита сети филиала



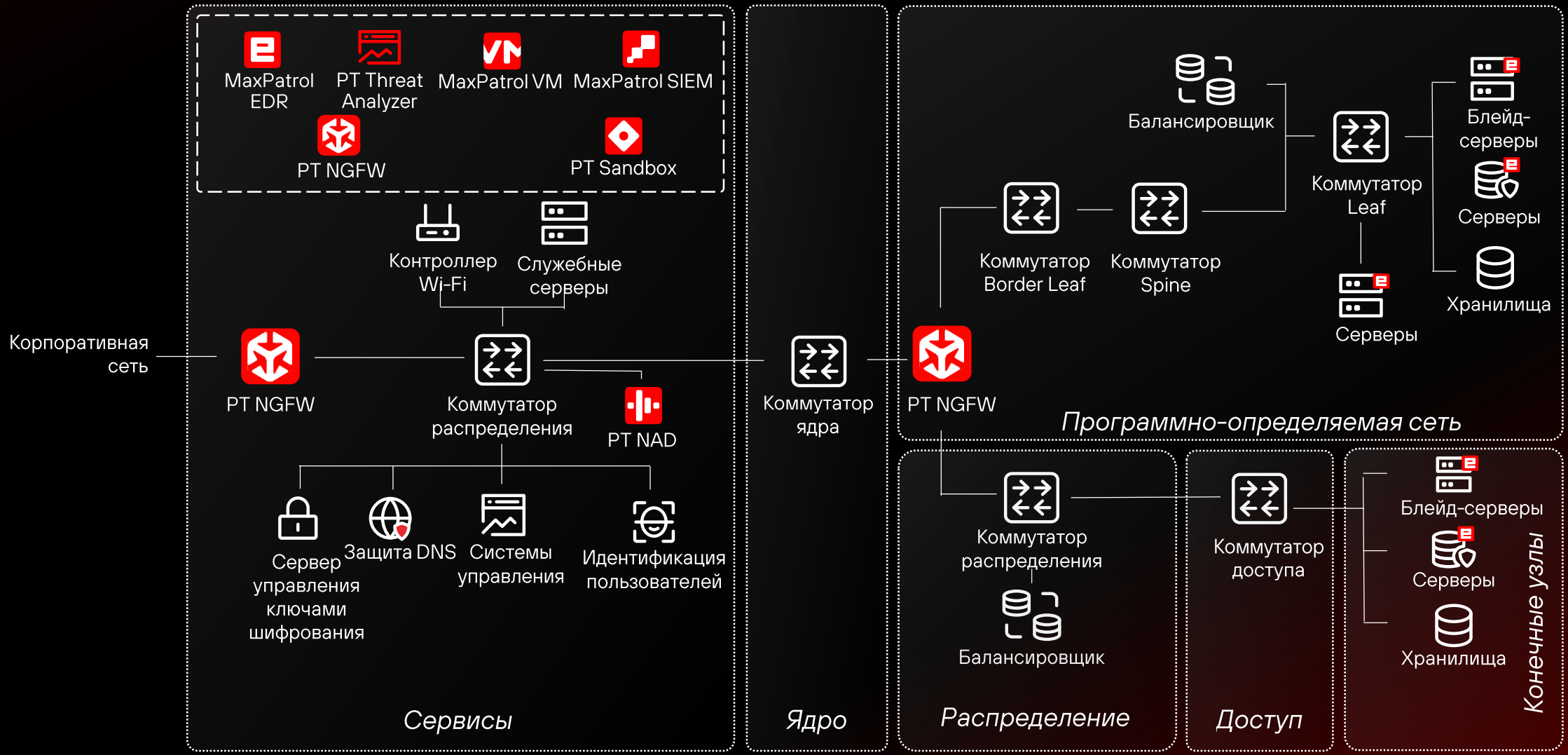
Сеть центра обработки данных



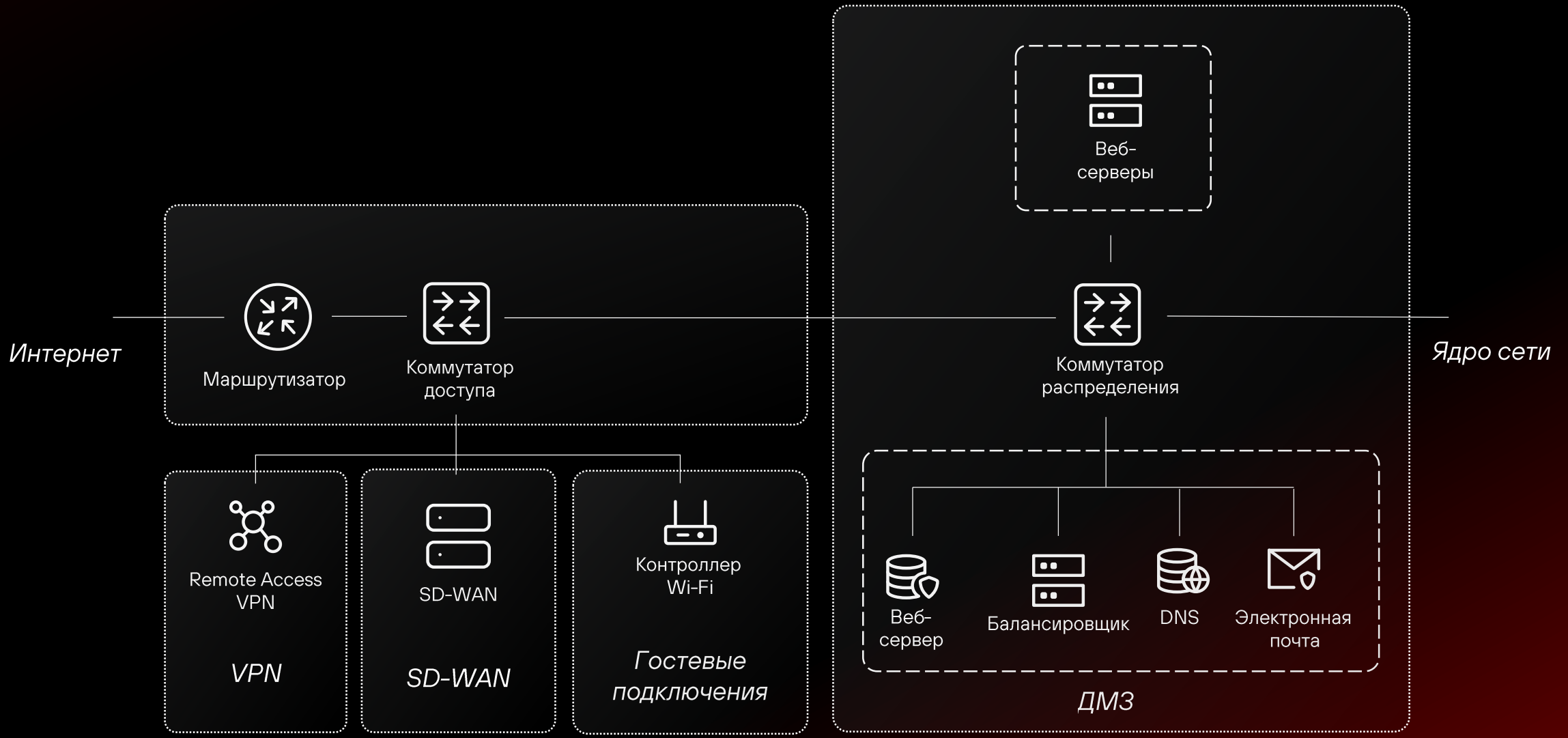
Особенности сети ЦОД

- Много зон безопасности
- Специализированные рабочие станции
- Корпоративные мобильные устройства
- Личные устройства
- Личные мобильные устройства
- Доступ из офисной сети
- Доступ из ДМЗ
- Подрядчики
- Необходимость поддержания всех компонентов и систем ЦОД в рабочем состоянии
- Высокая скорость обновления ПО
- Интернет вещей (управляемых)

Защита ЦОД


MaxPatrol EDR
PT Threat Analyzer
MaxPatrol VM
MaxPatrol SIEM
PT NGFW
PT Sandbox
Контроллер Wi-Fi
Служебные серверы
Корпоративная сеть
PT NGFW
Коммутатор распределения
PT NAD
Сервер управления ключами шифрования
Защита DNS
Системы управления
Идентификация пользователей
Сервисы
Коммутатор ядра
Ядро
PT NGFW
Балансировщик
Коммутатор Border Leaf
Коммутатор Spine
Коммутатор Leaf
Блейд-серверы
Серверы
Хранилища
Серверы
Программно-определяемая сеть
Коммутатор распределения
Балансировщик
Распределение
Коммутатор доступа
Доступ
Блейд-серверы
Серверы
Хранилища
Конечные узлы

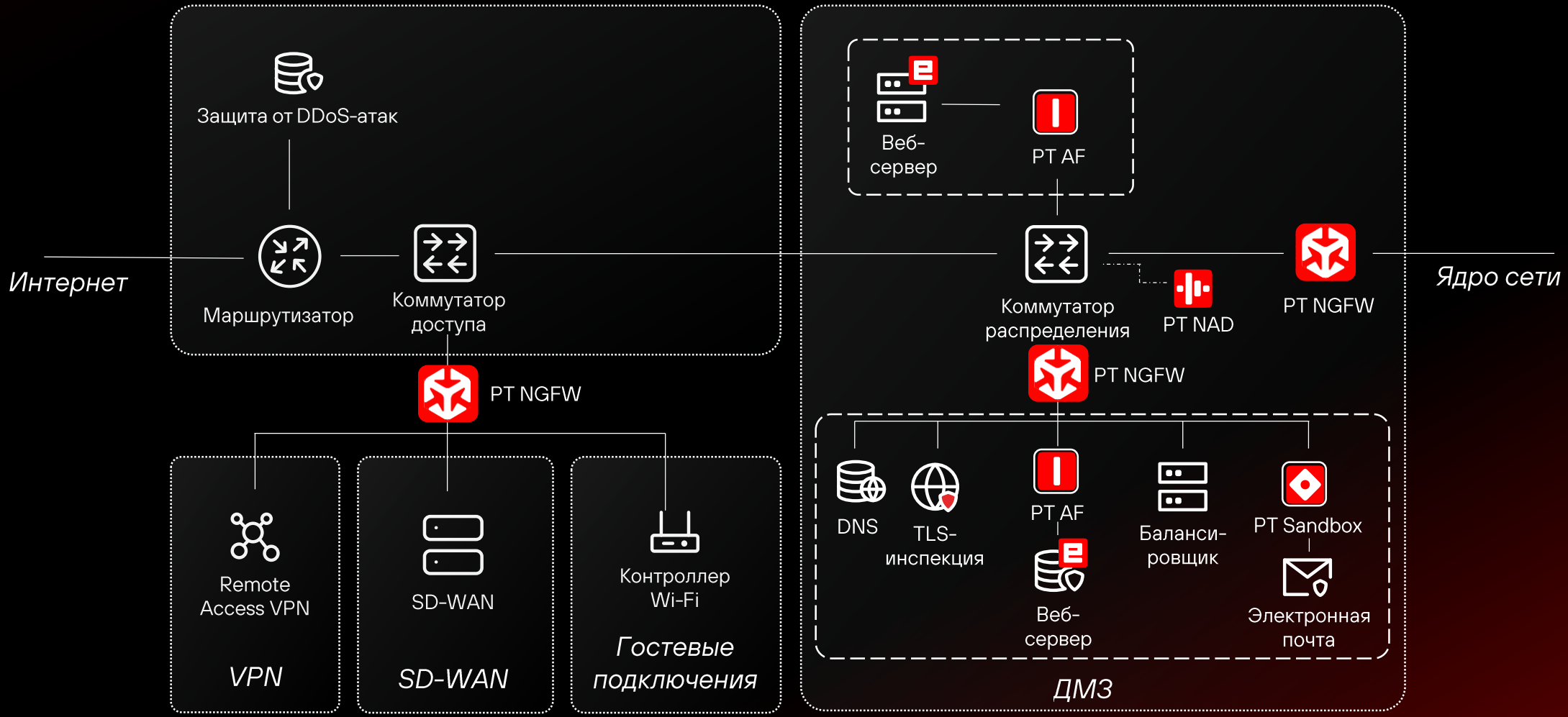
ДМЗ сети


Интернет
Маршрутизатор
Коммутатор доступа
Remote Access VPN
VPN
SD-WAN
SD-WAN
Контроллер Wi-Fi
Гостевые подключения
Веб-серверы
Коммутатор распределения
Ядро сети
Веб-сервер
Балансировщик
DNS
Электронная почта
ДМЗ

Особенности ДМЗ сети

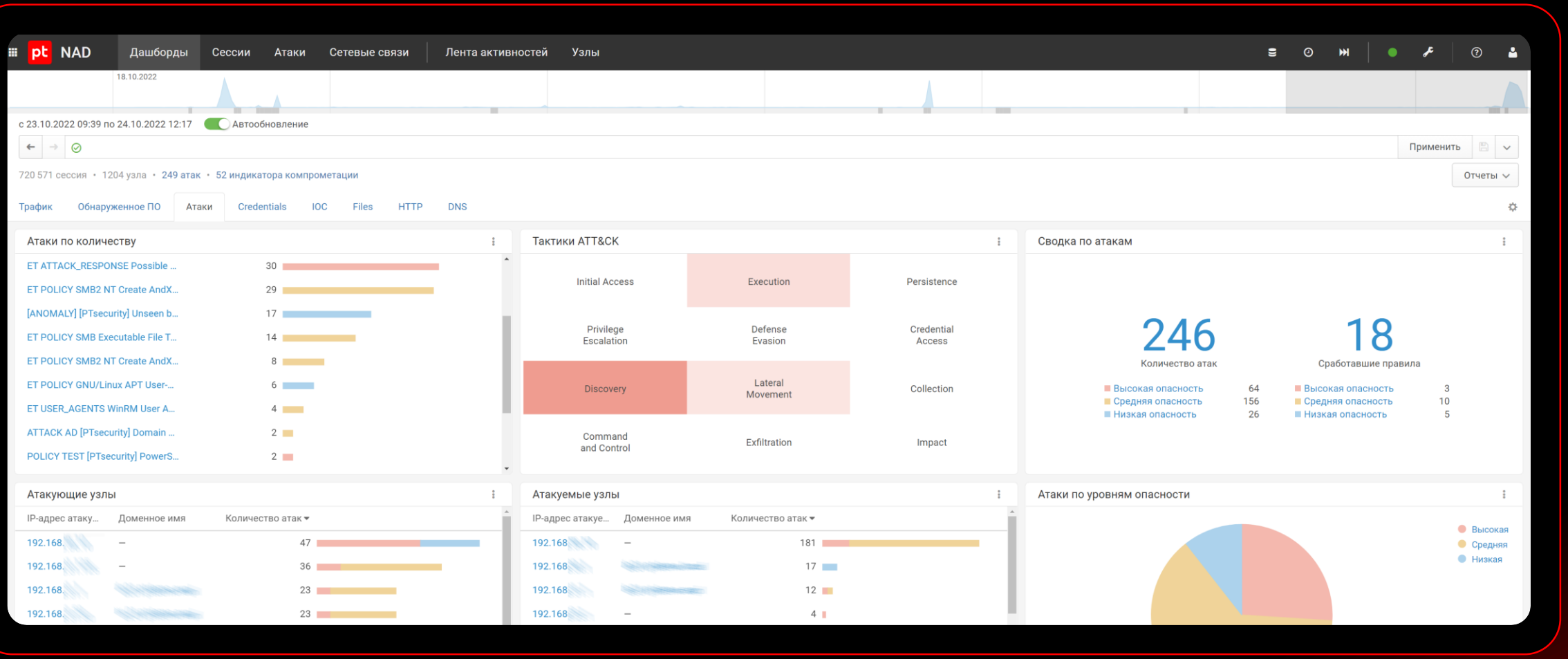
- Есть опубликованные сервисы
- Нет рабочих станций
- Доступ из интернета
- Подключение удаленных пользователей
- Подключение филиалов или отделений
- Доступ в ЦОД
- Доступ из офисной сети
- Гостевой доступ
- Сквозные служебные сервисы (например, веб, почта, DNS)

Защита ДМЗ сети



PT Network Attack Discovery

Система поведенческого анализа сетевого трафика для выявления атак на периметре и внутри сети



PT NAD

- Выявляет целевые атаки на периметре и внутри сети
- Обнаруживает скрытые угрозы
- Проверяет сетевую активность узлов

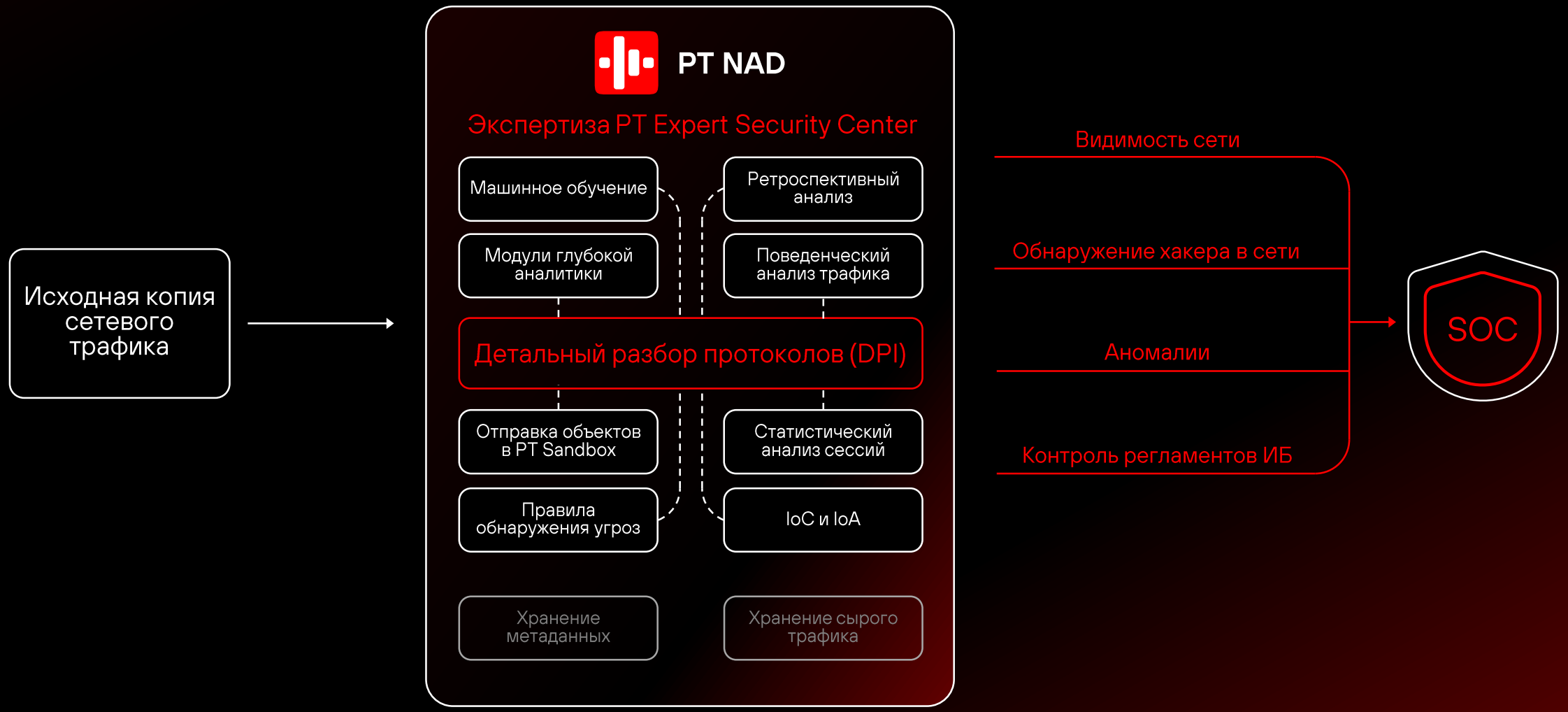
РЕЗУЛЬТАТ

Сокращает время присутствия злоумышленника в сети до считанных минут

Какие задачи решает PT NAD

- Обнаруживает нарушения регламентов ИБ
- Определяет новые устройства в сети
- Находит аномалии в трафике
- Профилирует сетевые узлы и определяет приложения
- Определяет угрозы в зашифрованном трафике
- Выявляет хакерские инструменты и перемещение атакующих внутри периметра

Как работает?



Что мониторить?

- Серверный сегмент
- Служебные сервисы (AD, DNS)
- DMZ
- WAN (исходящий трафик)
- Подключение удаленных пользователей
- Ключевые пользовательские сегменты

Полезные ссылки

Телеграм-чат о PT NAD

t.me/PTNADChat

Дополнительные материалы о PT NAD

clck.ru/33f7PP

Записаться на пилот

https://www.ptsecurity.com/ru-ru/products/network-attack-discovery/#nad-form

Спасибо!