Построение систем реагирования на кибератаки для организации критической инфраструктуры

Александр Оводов

директор департамента информационной безопасности

uniteller GOZNAK

Международный конгресс ИТМ,
Москва, 12-13 октября 2023

ИНФОРМАЦИОННЫЕ ТЕХНОЛОГИИ В МЕДИЦИНЕ
ITM
www.itmcongress.ru

Объекты современной медицины

- Медицинские информационные системы
- Телемедицинские системы и сервисы
- Экспертные и рекомендательные системы
- Диагностические и лабораторные системы
- Робототехника

Требования по реагированию на компьютерные атаки и инциденты

- 187-ФЗ О безопасности критической информационной инфраструктуры РФ
- 152-ФЗ О персональных данных (в части нарушений в отношении персональных данных)
- Подзаконные акты

2 большие задачи в инфобезе

1 Создание преград на пути злоумышленника

2 Обнаружение злоумышленника

ЗА ЛЮБЫХ ВРЕДОНОСОМ СТОИТ
ЗЛОУМЫШЛЕННИК

Несколько шагов:

ПЕРВЫЙ ШАГ

ИНВЕНТАРИЗАЦИЯ
(С КАКИХ СИСТЕМ, ПО КАКИМ ПРОТОКОЛАМ МОЖНО СОБИРАТЬ СОБЫТИЯ)

ВТОРОЙ ШАГ

ОПРЕДЕЛЕНИЕ ТОЧЕК СНЯТИЯ КОПИИ ТРАФФИКА

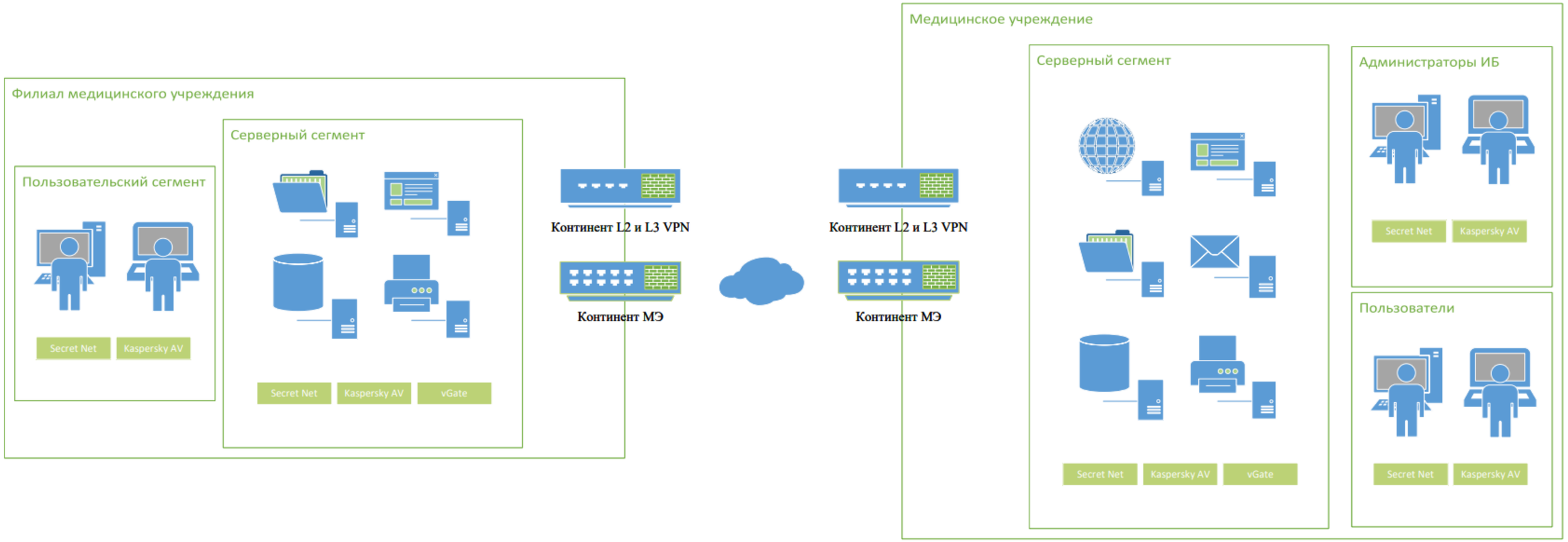
ТРЕТИЙ ШАГ

ВЫБОР АРХИТЕКТУРЫ И ПРОЕКТИРОВАНИЕ СИСТЕМЫ С УЧЕТОМ ТРУДОВЫХ РЕСУРСОВ

ЧЕТВЕРТЫЙ ШАГ

ВНЕДРЕНИЕ

Первый уровень



Второй уровень

но не дает полной картины происходящего это связка от компании

INFOTECS – ОБЪЕДИНЯЮЩАЯ СРЕДСТВА ОБНАРУЖЕНИЯ ВТОРЖЕНИЙ VIPNET IDS NS, IDS HS И СРЕДСТВО АВТОМАТИЧЕСКОГО ВЫЯВЛЕНИЯ ПРИЗНАКОВ КОМПЬЮТЕРНЫХ АТАК TIAS.

ПЛЮСЫ невысокая стоимость, простота эксплуатации.

МИНУСЫ требует установки агентов на все АРМ и сервера, работает только с событиями безопасности. Отсутствие возможности заблокировать подозрительную активность.

Третий уровень

КОММЕРЧЕСКАЯ ОТЕЧЕСТВЕННАЯ
NTA СИСТЕМА + EDR + MDR

ПЛЮСЫ

- отечественное
- максимизация сбора событий
- большое количество правил из коробки
- рускоязычная документация и поддержка
- сертификация.

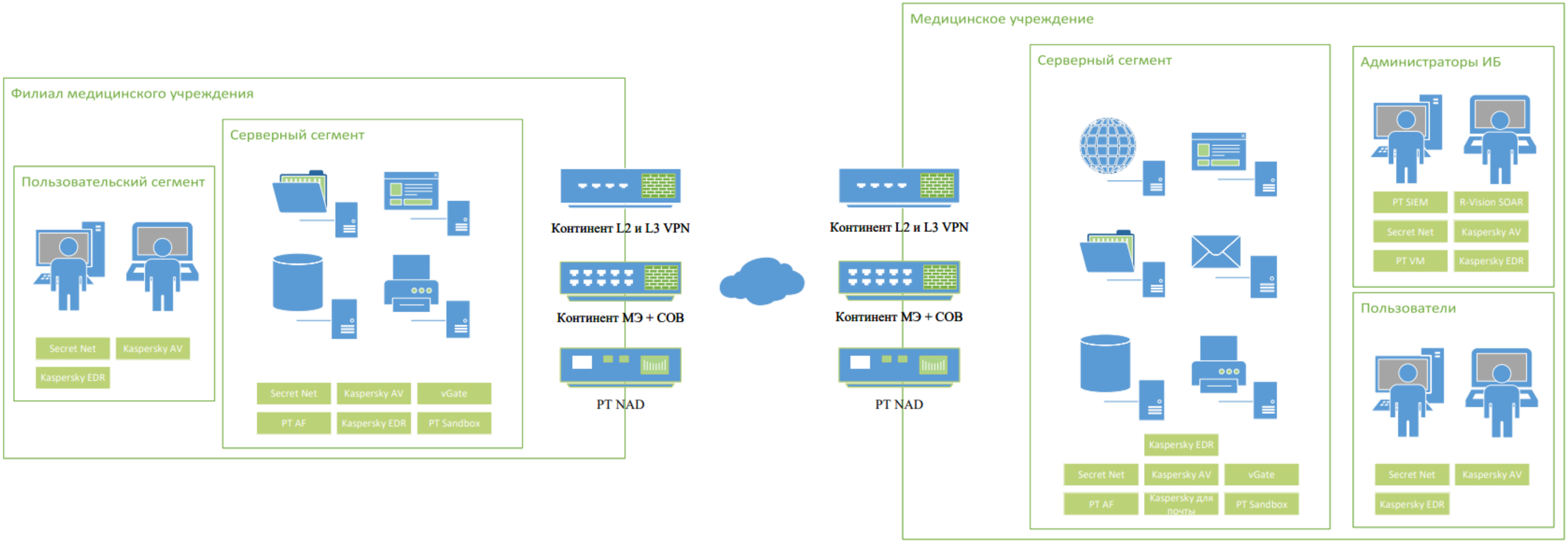
Четвертый уровень

SIEM + NTA + ERD

Источниками для SIEM систем являются:

- NGFW
- IDS/IPS
- Межсетевой экраней
- EDR
- NTA/NDR
- А также то что есть в вашей инфраструктуре

Четвертый уровень



Медицинская техника

Проблемы:

Удаленный доступ и мониторинг работы со стороны поставщиков

Обслуживание сторонними подрядчиками

Пропиетарное ПО, в том числе невозможность смены ОС, БД на подключенных АРМ и серверах

Невозможность или высокие риски установки обновлений

Взаимодействие с МИС, ЛИС, PACS и т.д.

Решения:

1. Договорные отношения с обязательным требования к АРМ по соблюдению ваших политик
2. Допуск подрядчиков со своим оборудование только после проверки на соответствие политикам
3. Защищенный СКЗИ канал связи
4. Доступ не напрямую, а через NGFW и АРМ/сервер медорганизации с установленным ПО для записи действий или через PAM
5. Выделение каждый тип и единицу оборудование в vlan через NGFW
6. Траффик через NTA
7. Мониторинг аномального поведения оборудования через ISIM или аналоги

СТЕНД Е7

Компания

uniteller

Обеспечиваем
вашу информационную
безопасность

ib@uniteller.ru

+7 (800) 100-19-60, доб.4
- инфобезопасность

uniteller.ru