udv|group

UDV MultiProtect

Комплексное решение для обеспечения
кибербезопасности среднего бизнеса

Информационная безопасность малого и среднего бизнеса*.

Ожидания

Рискуют только компании с объектами критической информационной

Хакерам небольшие компании неинтересны

Атакуют только в погоне за большими деньгами

Антивируса под нужды среднего бизнеса вполне достаточно

Эффективная защита – это дорого

Вероятность инцидентов крайне мала

Управлением ИБ занимаются только профильные специалисты

На небольшие компании не распространяются требования регуляторов ИБ

* компании с численностью сотрудников до 250 человек

Реальность
Вызовы ИБ для малого и среднего бизнеса

Более 30%

недостаточно защищены

«Ведомости», «Более 30% средних и малых компаний считают свою ИБ недостаточной» (16.01.2025)

20 млн ₽

средний ущерб от атаки, ликвидации последствий и простоя бизнеса

«Ведомости», «Чем больше бизнес зависит от цифры, тем выше приоритет кибербезопасности» (14.10.2024)

До 50%

случаев взлома в 2024 году связано с атаками через подрядчиков

«Как рынок ИБ пережил 2024 год и чего ждать от 2025: анализ и прогноз ГК «Солар» (26.12.2024)

45%

компаний МСБ сообщили о наличии инцидентов ИБ

Исследование защищенности от угроз ИБ малого и среднего бизнеса, Агентство стратегических инициатив, 2024 г.

Около 40%

утечек произошло у среднего и малого бизнеса

Исследование Центра противодействия киберугрозам Innostage CyberART

60%

компаний закрываются в течение 6 месяцев после инцидента ИБ

«Компьютерра», «Защита малого и среднего бизнеса от киберугроз в 2024 году»,

Актуальные угрозы по уровням зрелости ИБ

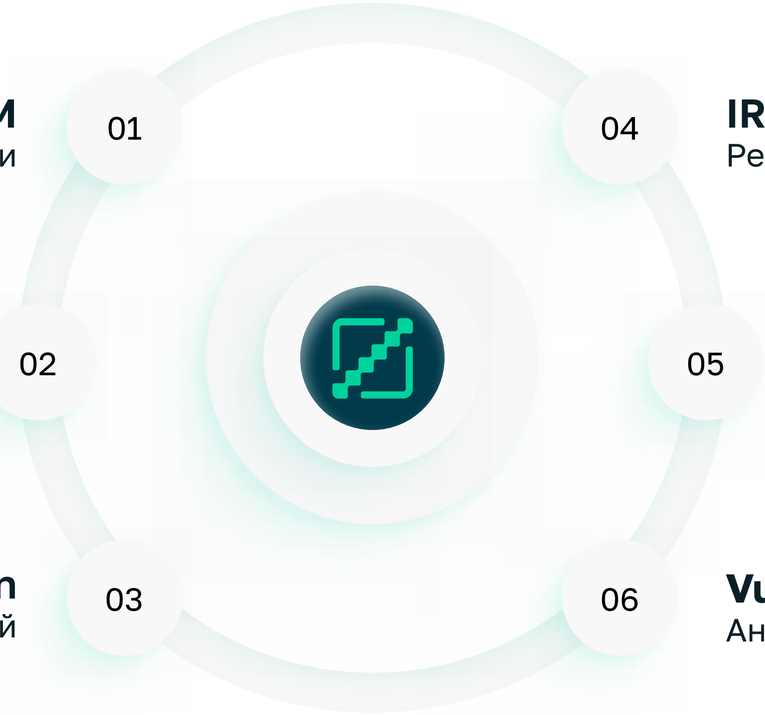
Продвинутый	Компрометация учётных записей	Целевые атаки
	Утечки информации	
Уверенный	Неконтролируемая инфраструктура	Неконтролируемый поток событий ИБ
	Уязвимости ПО	Некорректные настройки оборудования
Начальный	Сетевые атаки	Вредоносное ПО
	Потеря данных	Социальная инженерия

UDV MultiProtect

Комплексное решение для обеспечения
кибербезопасности среднего бизнеса

UDV MultiProtect – что это?

Решение позволяет быстро выстроить результативную защиту малого и среднего бизнеса за счет комбинации функциональности нескольких классов продуктов



01 **SIEM**
Управление событиями

02 **Configuration management**
Контроль конфигураций

03 **Intrusion Detection**
Обнаружение вторжений

04 **IRP**
Реагирование на инциденты

05 **Asset management**
Управление активами

06 **Vulnerability Management**
Анализ уязвимостей

udv|group

Актуальные угрозы по уровням зрелости ИБ, которые решает UDV MultiProtect

Продвинутый

- Компрометация учётных записей
- Целевые атаки
- Утечки информации

Уверенный

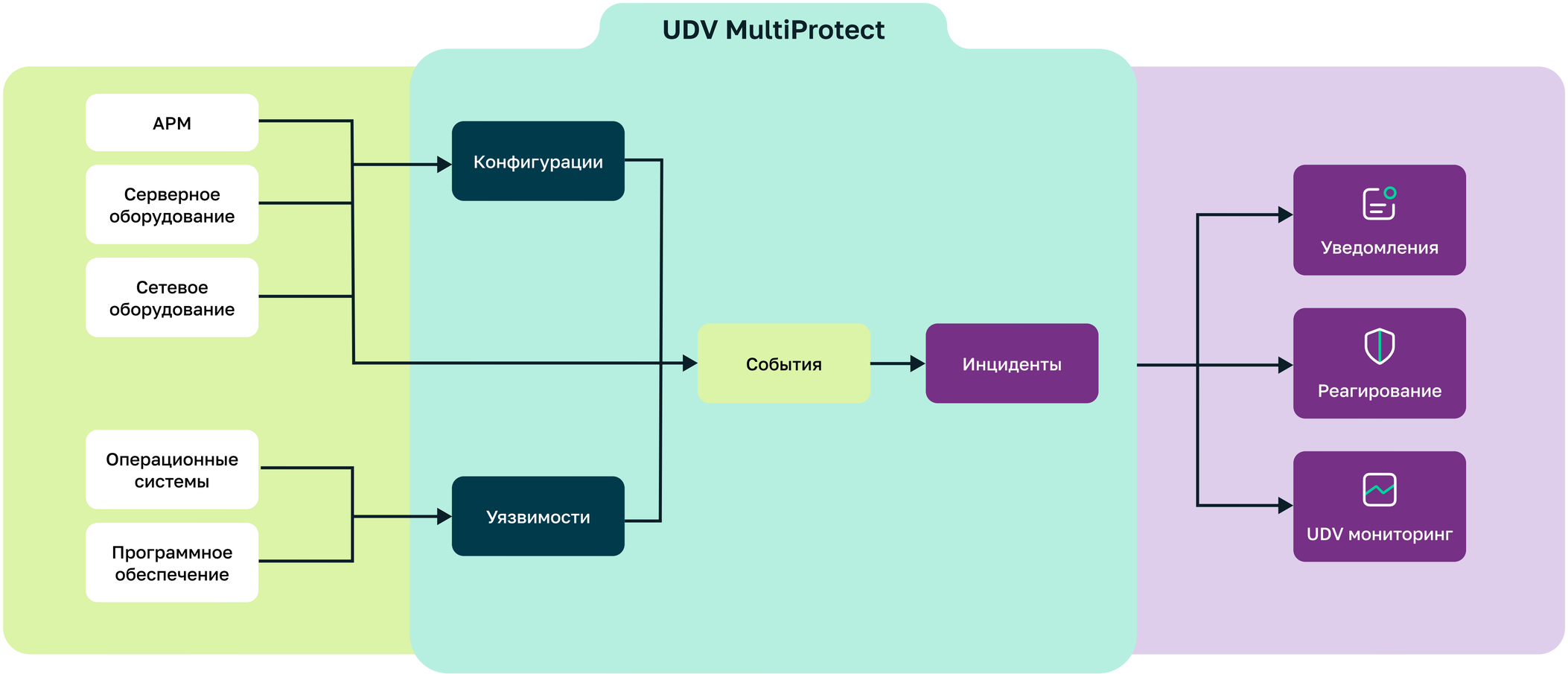
- Неконтролируемая инфраструктура
- Неконтролируемый поток событий ИБ
- Уязвимости ПО
- Некорректные настройки оборудования

Начальный

- Сетевые атаки
- Вредоносное ПО
- Потеря данных
- Социальная инженерия

udv|group

Схема функционирования UDV MultiProtect



udv|group

Возможности UDV MultiProtect

Asset Management
Управление активами

- Инвентаризация сети:
  — технических средств (АРМ, серверы и пр.)
  — программного обеспечения

- Классификация:
  — по типу
  — информационной системе
  — любым другим меткам

Пример:

Выявление новых устройств в сети, которые могут быть потенциальными злоумышленниками.

Configuration Manager
Управление конфигурациями

Контроль безопасности настроек и их неизменности, аудит изменений.

Пример:

На устройстве открыли несколько ранее закрытых портов – потенциальная угроза использования злоумышленником.

Есть возможность отследить эти изменения и при необходимости вернуться к эталонной конфигурации.

Возможности UDV MultiProtect

Intrusion Detection
Сканирование сетевого трафика и обнаружение вторжений

- Обнаружение несанкционированных сетевых потоков и соединений
- Выявление сетевых атак, «майнеров», удалённого администрирования
- Визуализация карты устройств в сети и сетевых соединений

Пример:

Обнаружение факта удалённого администрирования устройств в защищаемой сети.

Vulnerability Manager
Управление уязвимостями

- Поиск уязвимостей
- Проверка соответствия требованиям (Compliance)

Пример:

Проверка соответствия АРМ установленной в организации парольной политике.

Возможности UDV MultiProtect

External Event Manager (SIEM)
Управление внешними событиями

- Получение событий ИБ с различных источников
- Корреляция событий ИБ, выявление инцидентов из поступающих событий

Пример:

Обнаружение и корреляция в инцидент события установки программного обеспечения инструментов удаленного доступа (AnyDesk, RAdmin и пр.), которое может быть использовано злоумышленником.

Incident Response Platform (IRP)
Реагирование на инциденты

- Готовый пошаговый алгоритм обработки и расследования инцидентов
- Автоматизированное обогащение информации по инцидентам и реагирование
- Определение техник реализации инцидентов по известным методологиям (ТТУ ФСТЭК и MITRE ATT&CK)
- Оповещения на электронную почту о регистрируемых инцидентах

Пример:

- Получение информации о наличии в чёрном списке атакующего хоста.
- Автоматическая блокировка учетной записи пользователя, участвующей в атаке.

Преимущества UDV MultiProtect

Комплексная защита

1 продукт — 6 необходимых мер защиты в едином интерфейсе

Подтвержденная эффективность

Использование технологий, применяемых для защиты промышленных объектов КИИ, проверенных на 150+ проектах в сегменте корпораций

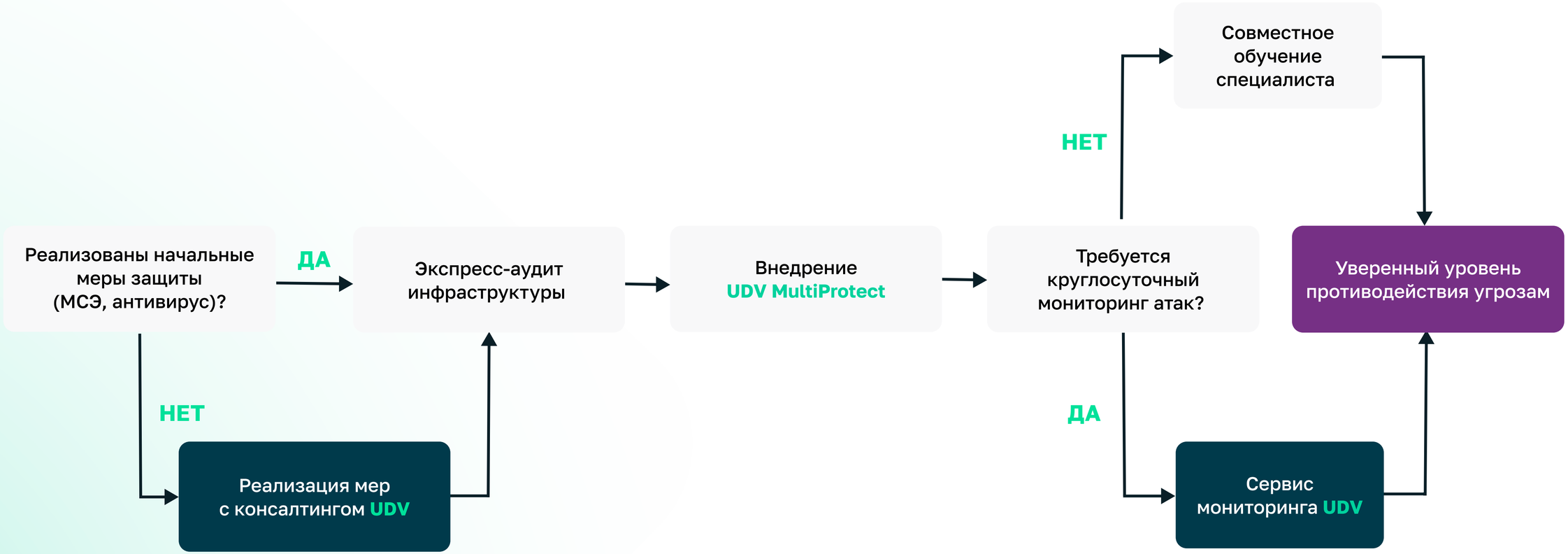
Экспертиза

Механизмы выявления инцидентов от коммерческого Центра мониторинга ИБ, техническая поддержка, консультации

Экономия ресурсов

Стоимость ниже, чем у сета моно-продуктов, автоматизация процессов

Что дальше?



UDV Group — ведущий разработчик в области кибербезопасности

UDV Group предоставляет единый портфель решений для защиты технологических сетей, корпоративного сегмента и автоматизации в области объектовой безопасности:

- защита АСУ ТП и объектов КИИ
- мониторинг инфраструктуры
- реагирование на инциденты ИБ
- автоматизация работы SOC
- выполнение требований регуляторов

200+

Разработчиков в штате

Распределённая команда
со штаб-квартирой в Екатеринбурге

1000+

Инсталляций

Проекты по защите АСУ ТП
и корпоративных сетей

10+

Патентов

Собственный исследовательский
центр в области кибербезопасности

10

Лет на рынке

Подтвержденный опыт интеграции
в крупных предприятиях
нефтегазовой отрасли, энергетики,
металлургии и других

udv|group

Спасибо!

Закажите пилотный проект или персональную демонстрацию наших решений

Контакты

commercial@udv.group
8-800-511-65-51

Адрес

620100, г. Екатеринбург,
ул. Сибирский тракт, 12,
строение 7, этаж 4

Сайт

udv.group

Telegram

@udv_group