



UDV MultiProtect

Комплексное решение для обеспечения
кибербезопасности среднего бизнеса



Информационная безопасность малого и среднего бизнеса

Ожидания



Эффективная защита –
это дорого



Хакерам небольшие
компании неинтересны



Рискуют только компании с объектами
критической информационной инфраструктуры



Атакуют только в погоне
за большими деньгами



Антивируса под нужды среднего
бизнеса вполне достаточно



Вероятность
инцидентов крайне мала



Управлением ИБ занимаются
только профильные специалисты



На небольшие компании не распространяются
требования регуляторов ИБ

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)

45%

компаний МСБ сообщили о наличии инцидентов ИБ

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

20 млн ₽

ущерб от атаки, ликвидации последствий и простоя для среднего бизнеса

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

Около 40%

утечек произошло у среднего и малого бизнеса

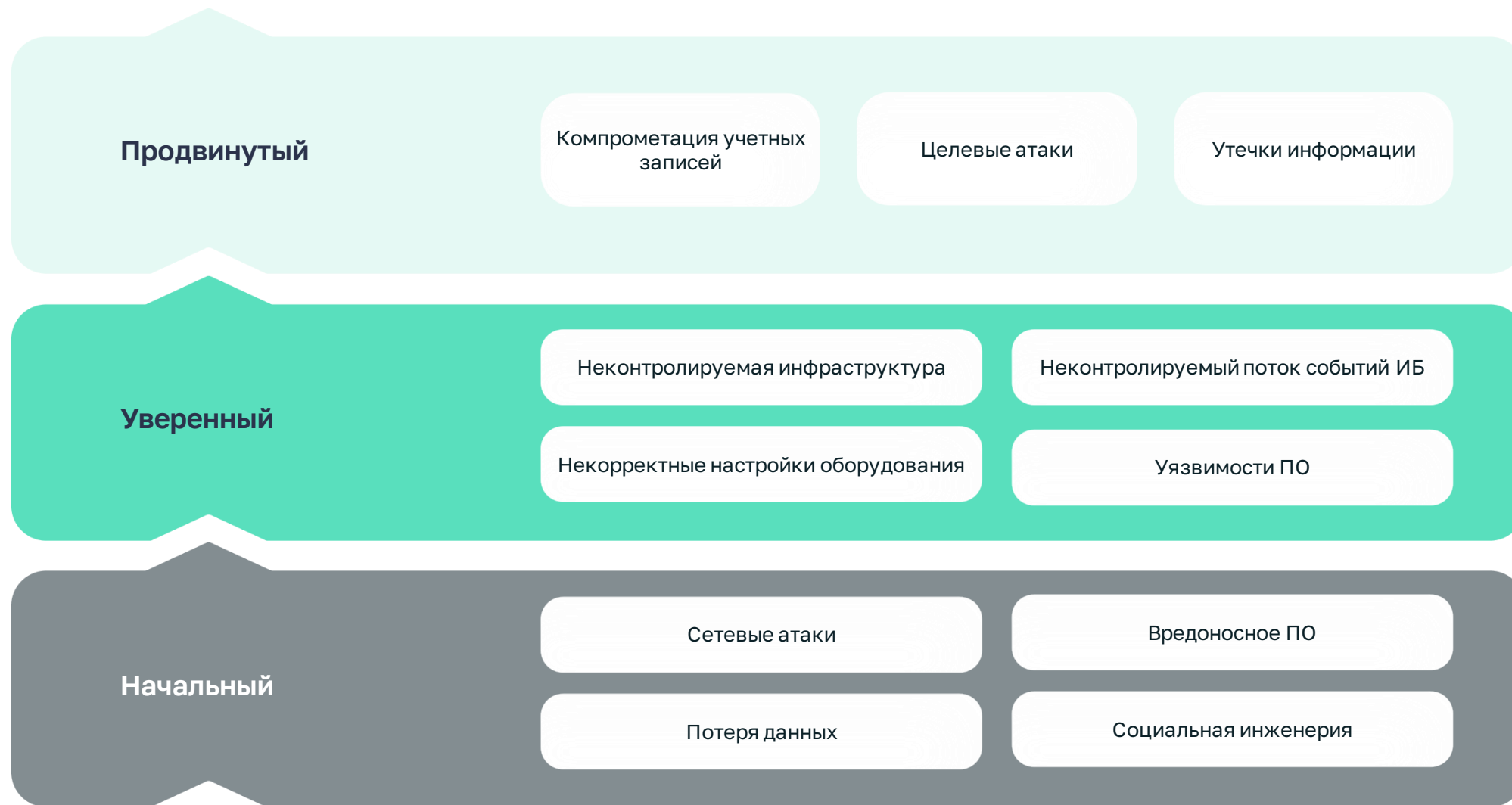
Исследование Центра противодействия киберугрозам Innostage CyberART

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)

Актуальные угрозы по уровням зрелости ИБ





UDV MultiProtect

Комплексное решение для обеспечения
кибербезопасности среднего бизнеса

UDV MultiProtect — что это?

Решение позволяет быстро и эффективно повысить уровень защищенности за счет комбинации функциональности нескольких классов продуктов



Актуальные угрозы по уровням зрелости ИБ, которые решает UDV MultiProtect

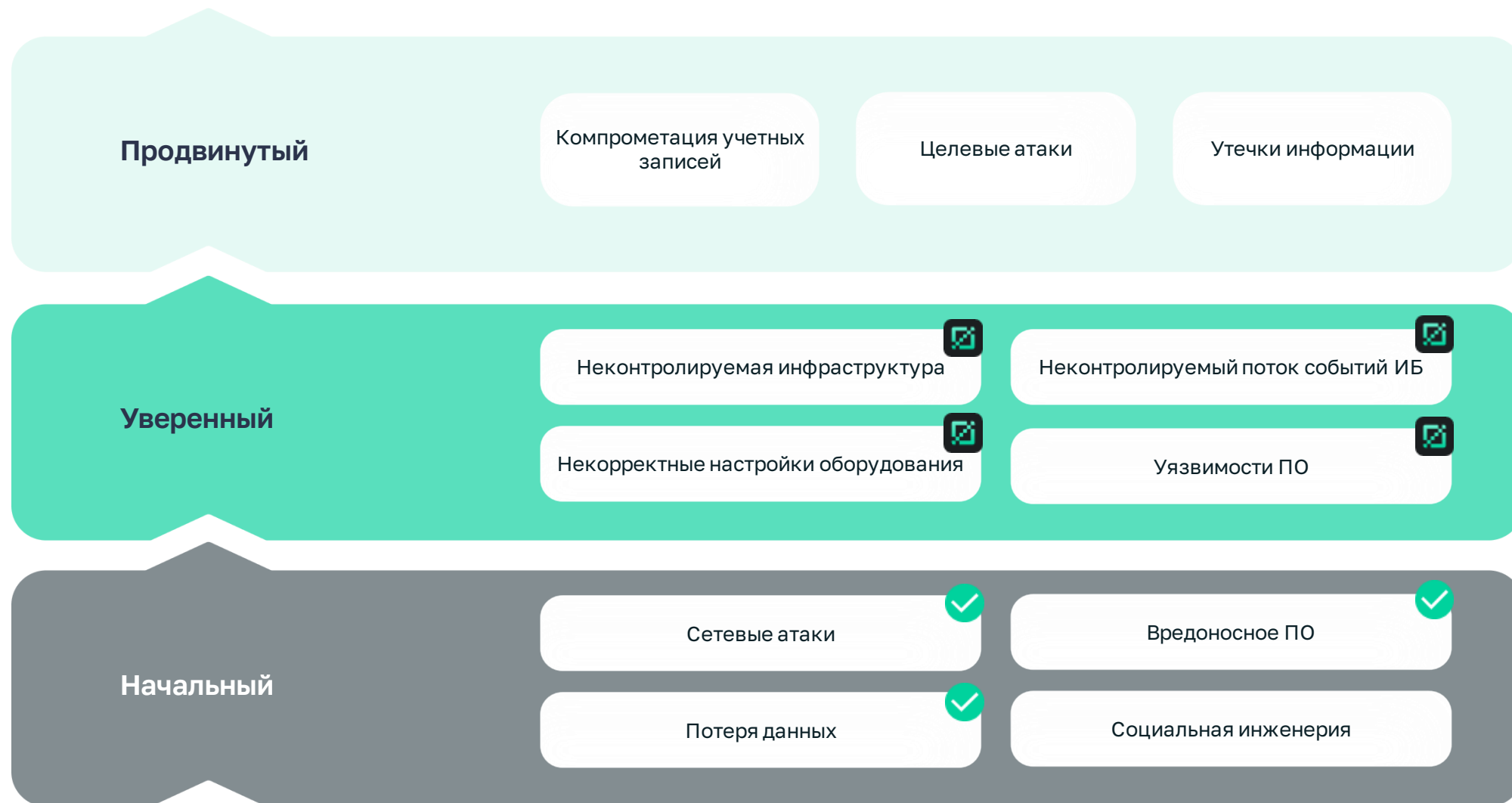
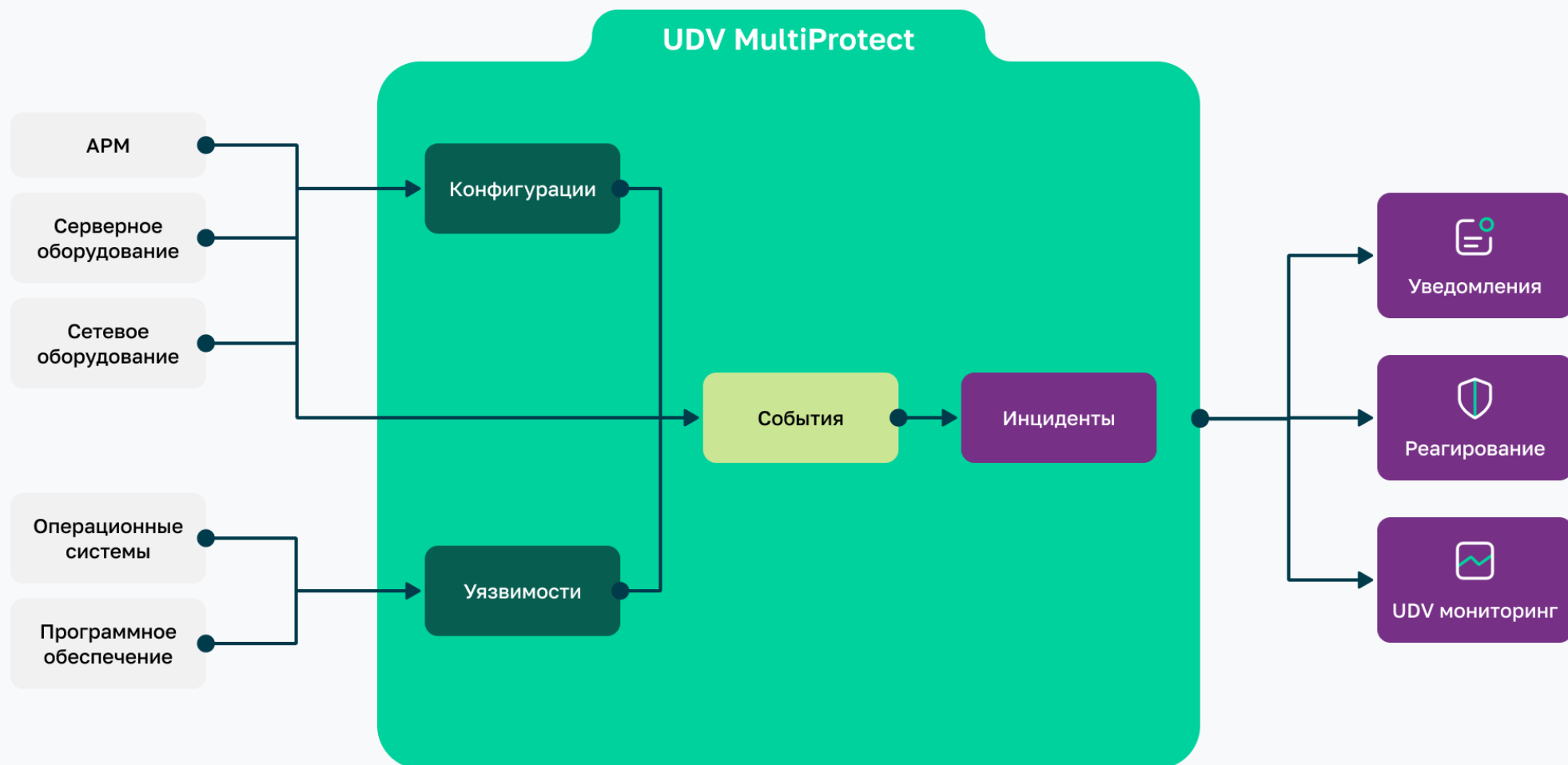


Схема функционирования UDV MultiProtect



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

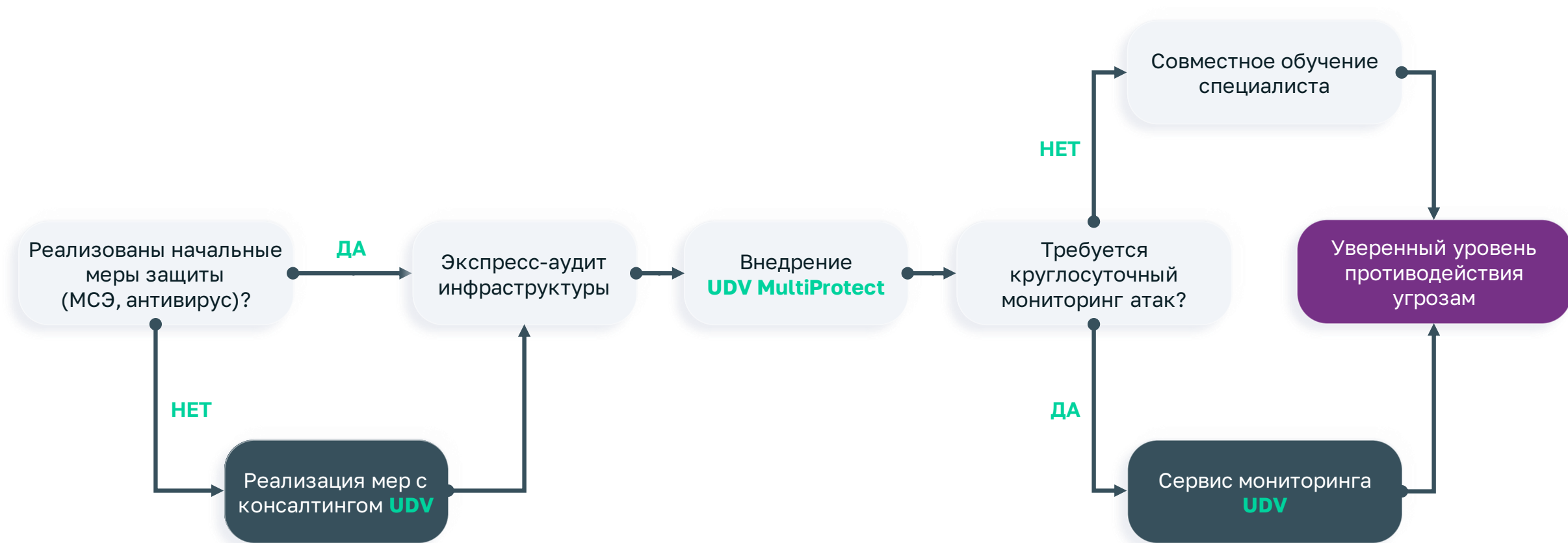
Пример:

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

Преимущества UDV MultiProtect



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



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

