udv|group

Безопасность МСБ

- Актуальные требования регуляторов
- Типичные риски ИБ в МСБ
- Защита с использованием UDV MultiProtect

Ольга Луценко
Консультант ИБ
UDV Group

Иван Бурмистров
Пресейл-инженер
UDV Group

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

1500+
инсталляций

Проекты по защите АСУ ТП и корпоративных сетей

10+
патентов

Собственный исследовательский центр в области кибербезопасности

12
лет на рынке

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

udvgroup

О спикере

- Консультант по информационной безопасности UDV Group
- Ведущий аудитор в области ИБ, специалист по внедрению стандарта ISO 27001:2022 в области ИБ
- Ключевые компетенции: аудит ИБ, категорирование ОКИИ, комплексное решение задач ИБ для компаний малого и среднего бизнеса

udv|group

Реальность.
Вызовы ИБ для малого и среднего бизнеса

Собственная безопасность

45%
компаний МСБ сообщили о наличии инцидентов ИБ

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

62%
Предпринимателей больше всего опасаются спам-атак, DDoS, вирусов и шпионского ПО

Исследование «Кибердома», 2025 г.

ТОП-3 угроз:

34%
Фишинги

25%
Бот-атаки

22%
Вирусы

Исследование «Солар», 2025 г.

Безопасность в цепочке поставок

udvlgroup

Реальность.
Вызовы ИБ для малого и среднего бизнеса

Собственная безопасность

Безопасность в цепочке поставок

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)

В ТОП-6

самых распространенных способов проникновения в инфраструктуру входят атаки через подрядчиков-МСБ. Количество инцидентов возросло в 3 раза

Исследование Red Security SOC по итогу 2024 г.

На 80%

Увеличилось количество кибератак через поставщиков в Q1 2025 по сравнению с Q1 2024

По данным «Информзащиты»

Почему сейчас это особенно актуально?

1

Ужесточение ответственности за нарушение законодательства в области ПДн

- Оборотные штрафы
- Усиленный контроль за информацией об утечках

2

Ужесточение законодательства в области КИИ

Отмена запрета на внеплановые проверки -> повышенное внимание регулятора к новостям о компьютерных инцидентах -> **возможное признание субъектности**

3

Ужесточение законодательства в части ГИС

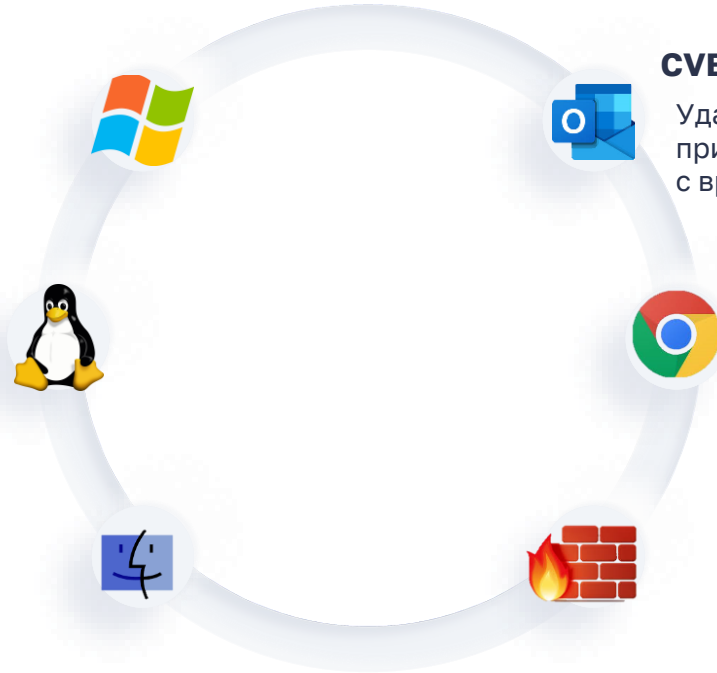
- Не только ГИС, а **все ИС госорганов**
- Регулярная оценка защищенности и зрелости
- Расширенный набор требований ИБ

Типовые риски ИБ в МСБ

1. Эксплуатация актуальных уязвимостей компонентов
2. Небезопасные настройки оборудования
3. Неконтролируемая инфраструктура
4. Отсутствие мониторинга событий

Типовые риски ИБ в МСБ

1. **Эксплуатация актуальных уязвимостей компонентов**
2. Небезопасные настройки оборудования
3. Неконтролируемая инфраструктура
4. Отсутствие мониторинга событий



CVE-2024-21413

Удаленное выполнение кода при открытии писем с вредоносными ссылками

CVE-2025-2783

Заражение компьютера под управлением Windows при переходе по вредоносной ссылке

Типовые риски ИБ в МСБ

1. **Эксплуатация актуальных уязвимостей компонентов**
2. Небезопасные настройки оборудования
3. Неконтролируемая инфраструктура
4. Отсутствие мониторинга событий

udvlgroup

Типовые риски ИБ в МСБ

1. Эксплуатация актуальных уязвимостей компонентов
2. **Небезопасные настройки оборудования**
3. Неконтролируемая инфраструктура
4. Отсутствие мониторинга событий

Эталонная конфигурация

IVANOV: Пользователь	Администраторы: DomainAdmin	Брандмауэр: включен
Гость: Отключен	Минимальная длина пароля: 12 символов	

Типовые риски ИБ в МСБ

1. Эксплуатация актуальных уязвимостей компонентов
2. **Небезопасные настройки оборудования**
3. Неконтролируемая инфраструктура
4. Отсутствие мониторинга событий

Эталонная конфигурация

IVANOV: Пользователь	Администраторы: DomainAdmin	Брандмауэр: включен
Гость: Отключен	Минимальная длина пароля: 12 символов	

Измененная конфигурация

IVANOV: Администратор	Администраторы: DomainAdmin, IVANOV	Брандмауэр: включен
Гость: Включен	Минимальная длина пароля: 12 символов	

Типовые риски ИБ в МСБ

1. Эксплуатация актуальных уязвимостей компонентов
2. **Небезопасные настройки оборудования**
3. Неконтролируемая инфраструктура
4. Отсутствие мониторинга событий

Эталонная конфигурация

IVANOV: Пользователь	Администраторы: DomainAdmin	Брандмауэр: включен
Гость: Отключен	Минимальная длина пароля: 12 символов	

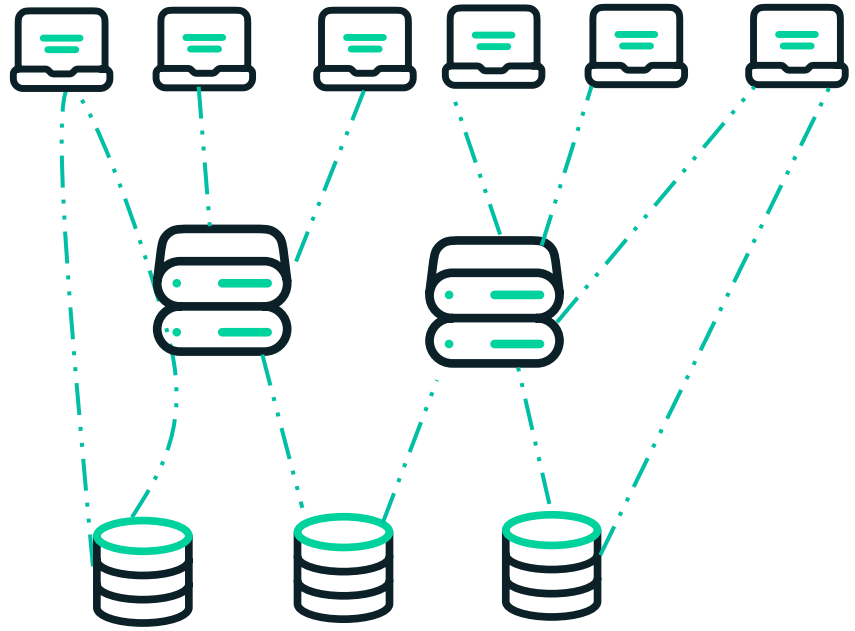
Configuration Manager

Измененная конфигурация

IVANOV: Администратор	Администраторы: DomainAdmin, IVANOV	Брандмауэр: включен
Гость: Включен	Минимальная длина пароля: 12 символов	

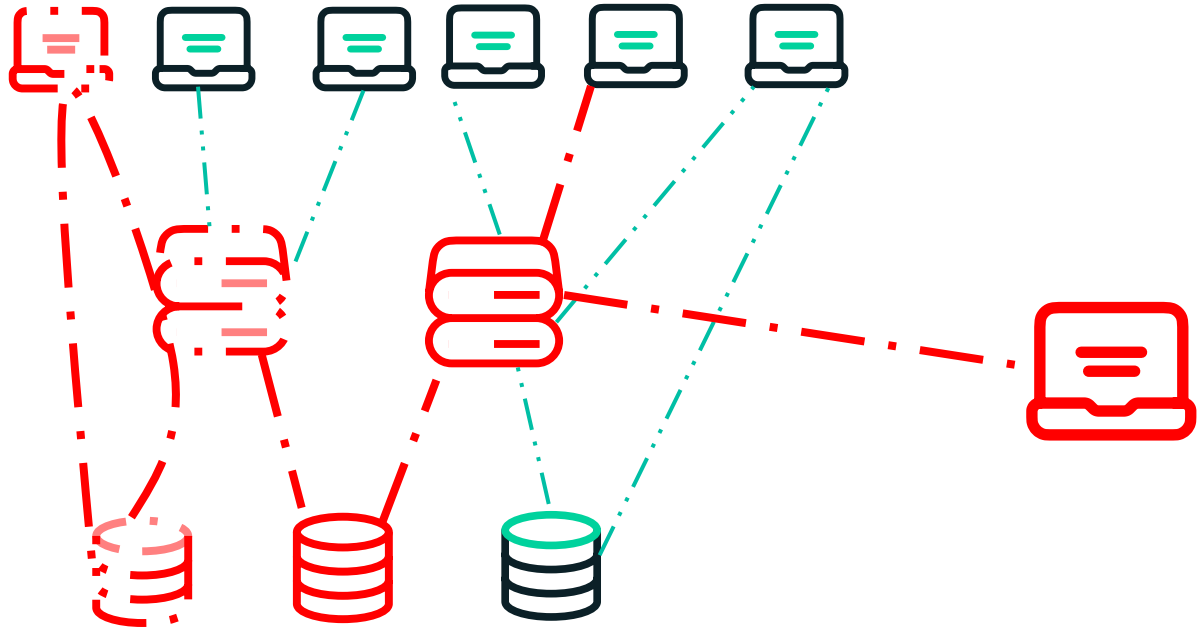
Типовые риски ИБ в МСБ

1. Эксплуатация актуальных уязвимостей компонентов
2. Небезопасные настройки оборудования
3. **Неконтролируемая инфраструктура**
4. Отсутствие мониторинга событий



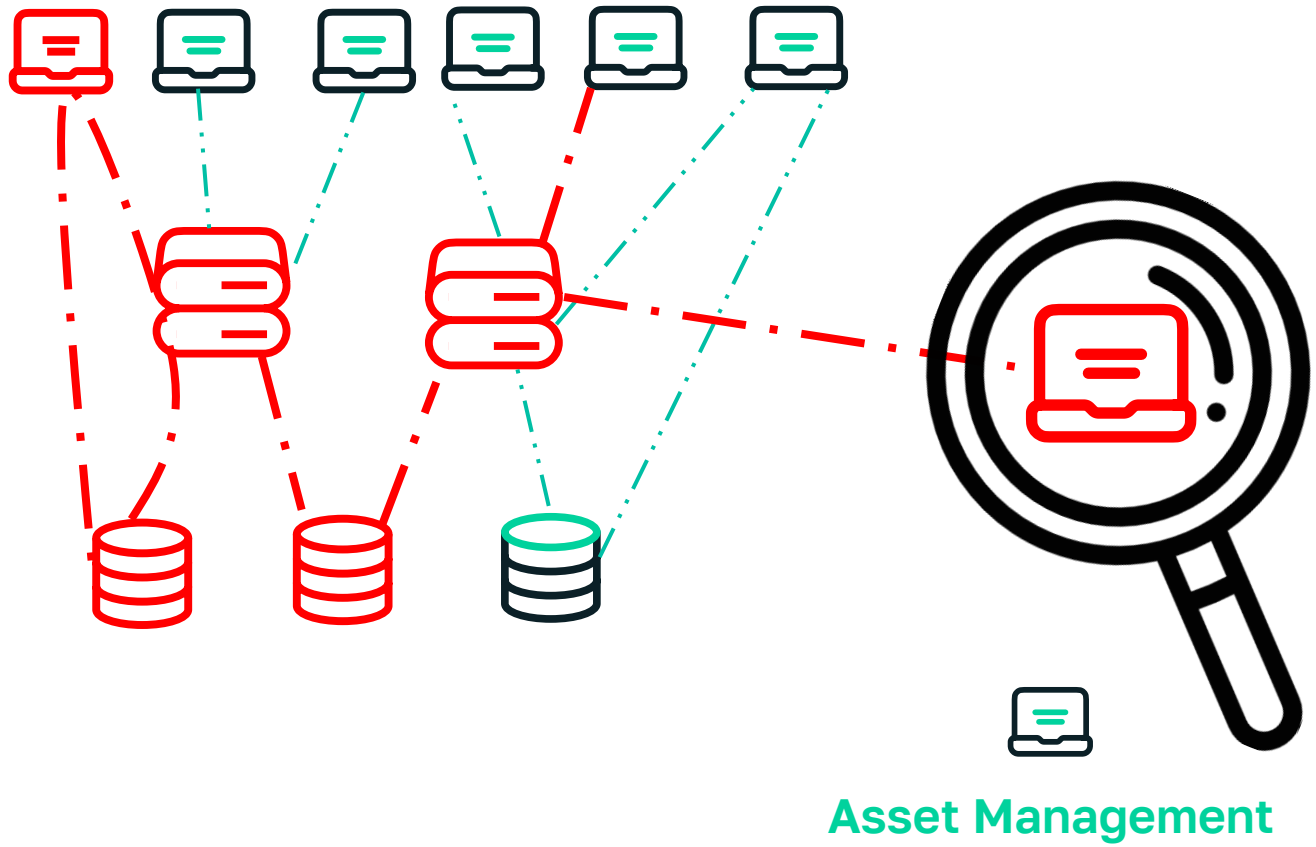
Типовые риски ИБ в МСБ

1. Эксплуатация актуальных уязвимостей компонентов
2. Небезопасные настройки оборудования
3. **Неконтролируемая инфраструктура**
4. Отсутствие мониторинга событий



Типовые риски ИБ в МСБ

1. Эксплуатация актуальных уязвимостей компонентов
2. Небезопасные настройки оборудования
3. **Неконтролируемая инфраструктура**
4. Отсутствие мониторинга событий



Типовые риски ИБ в МСБ

1. Эксплуатация актуальных уязвимостей компонентов
2. Небезопасные настройки оборудования
3. Неконтролируемая инфраструктура
4. **Отсутствие мониторинга событий**

Установка ПО удаленного доступа

Выполнение задач по расписанию

Неудачная попытка входа в систему

Смена пароля

Новое сетевое взаимодействие

Обнаружение нового устройства

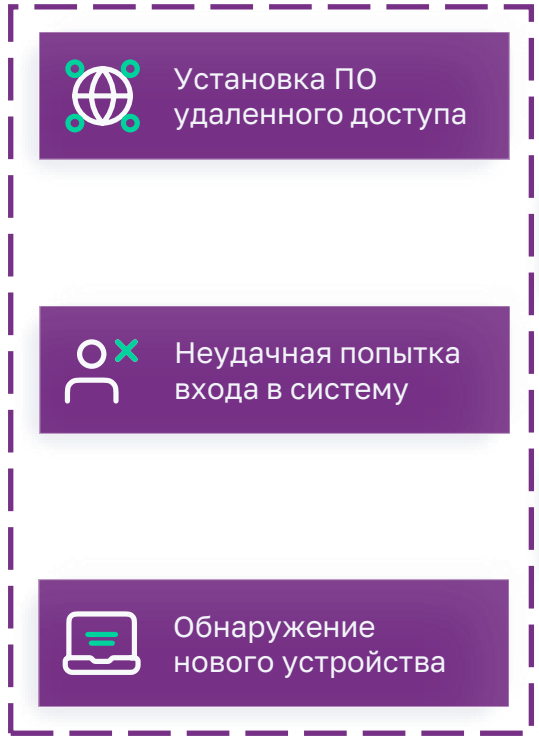
Изменение привилегий

Изменение конфигурации

Запущено сканирование

Типовые риски ИБ в МСБ

1. Эксплуатация актуальных уязвимостей компонентов
2. Небезопасные настройки оборудования
3. Неконтролируемая инфраструктура
4. **Отсутствие мониторинга событий**



- Выполнение задач по расписанию
- Смена пароля
- Новое сетевое взаимодействие
- Изменение привилегий
- Изменение конфигурации
- Запущено сканирование

Security Information and Event Manager (SIEM)

01

SIEM
Управление событиями

02

Configuration management
Контроль конфигураций

03

IRP
Реагирование на инциденты

04

Asset management
Управление активами

05

Vulnerability management
Анализ уязвимостей

udv|group

UDV MultiProtect

Комплексное решение для обеспечения кибербезопасности среднего бизнеса

udv|group

UDV MultiProtect — что это?

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

SIEM
Управление событиями

01

Configuration management
Контроль конфигураций

02

Intrusion Detection
Обнаружение вторжений

03

IRP
Реагирование на инциденты

04

Asset management
Управление активами

05

Vulnerability management
Анализ уязвимостей

06

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.

udvgroup

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.

udvgroup

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.

udvgroup

Преимущества UDV MultiProtect

Комплексная защита

1 продукт - 6 необходимых мер защиты в едином интерфейсе

Экономия ресурсов

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

Экспертиза

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

Подтвержденная эффективность

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

udv|group

Демонстрация обработки инцидентов ИБ

на примере UDV MultiProtect

udv|group

софтлайн РЕШЕНИЯ

Спасибо!

Закажите пилотный проект или персональную демонстрацию наших решений

Контакты

Анастасия Зырянова,
пресейл-менеджер по сетевой безопасности

Email

anastasiya.zyryanova@softline.com