КИБЕР
ПРОТЕКТ

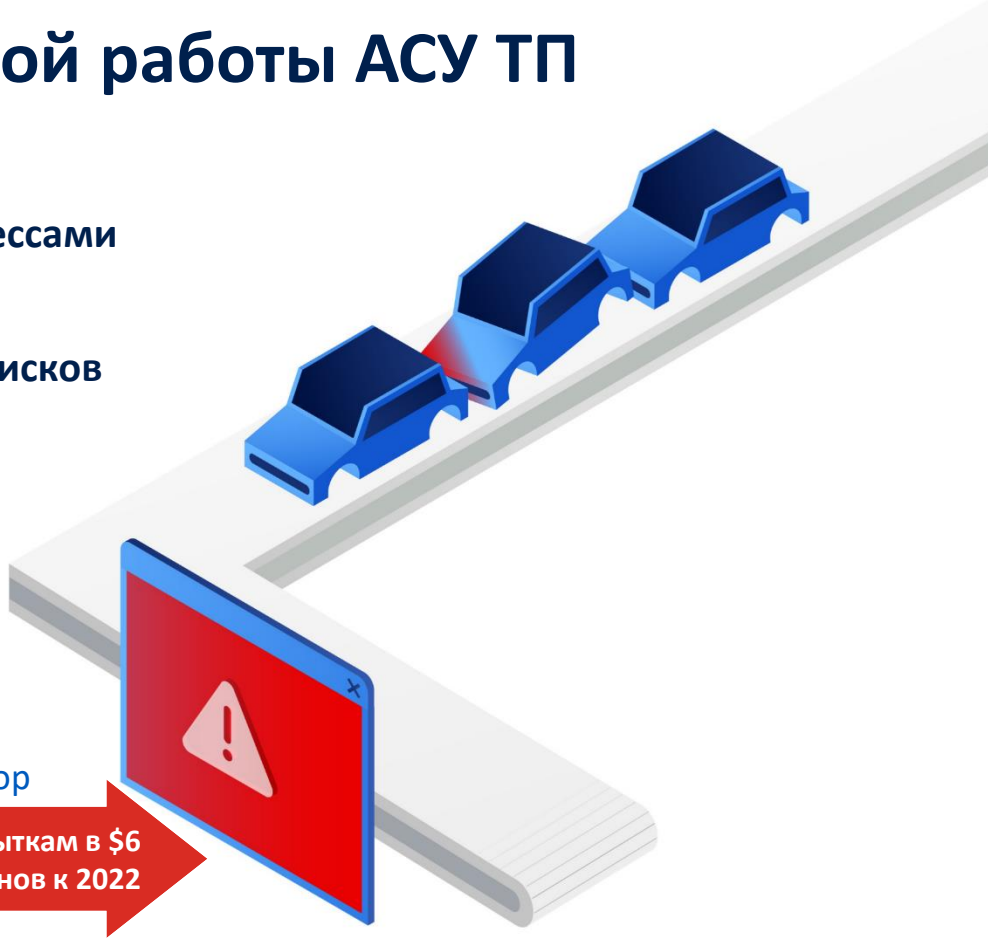
Применение продуктов Киберпротект для защиты АСУ ТП и инфраструктуры предприятий»

Александр Львов

Необходимость безотказной работы АСУ ТП

- **Высокая автоматизация управления процессами**
- **Усложняющиеся технологии**
- **Уязвимости инфраструктуры для разных рисков**
  - Сбои железа и ПО в АСУ ТП
  - Ошибки персонала и атаки злоумышленников
  - Внешние атаки:
    - Программы-вымогатели
    - Криптомайнеры
    - Специализированные атаки
  - Естественные катастрофы и человеческий фактор

Киберпреступность будет приводить к убыткам в $6 триллионов к 2022



Очень высокая стоимость простоя

потерянный доход + потерянная производительность + затраты на восстановление + нематериальные затраты

Средняя стоимость простоя
(в промышленности)

$4,333

в минуту!

Центры обработки данных
(незапланированное отключение)

$8,851

в минуту!

Автомобильная индустрия
(незапланированное отключение)

$22,000

в минуту!

Источник: Aberdeen Group report, “Maintaining Infrastructure Uptime in Today’s Transforming IT Infrastructure”

Как гарантировать сохранность Ваших данных

КИБЕР
Бэкап

- Корпоративная система резервного копирования для организаций любого размера
- Быстрое восстановление данных в случае необходимости
- Надежная защита от вирусов-шифровальщиков для данных и резервных копий
- Низкая стоимость внедрения и поддержки решения по защите данных

КИБЕР
Инфраструктура

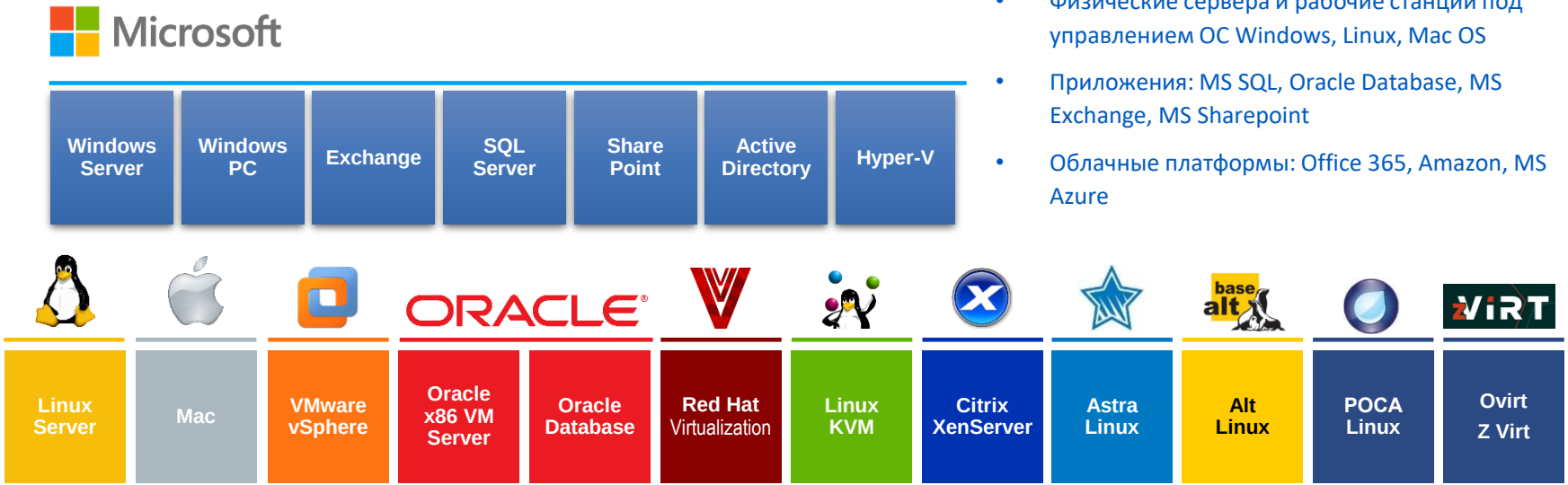
- Программно-определяемое решение, которое объединяет виртуализацию, хранилище и сеть
- Оптимальное решение для организации хранения больших объемов данных
- Высокая отказоустойчивость и производительность хранилища и виртуализации
- Высокая экономическая эффективность

Особенности инфраструктуры АСУ ТП

1. **Неоднородность** используемых программных и аппаратных платформ
2. Высокая распределенность сети и зависимость от уровня **компетенций** персонала
3. Наличие **устаревшего** оборудования и ОС
4. Сложности **миграции** на новое оборудование или среду виртуализации
5. Высокая нагрузка и требования к **доступности**
6. Частые **атаки** со стороны злоумышленников

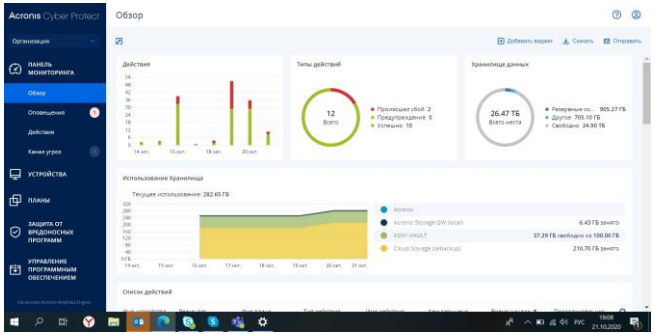
Неоднородность используемых программных и аппаратных платформ

- Платформы виртуализации: Vmware, Hyper-V, KVM, Redhat, Oracle VM, Citrix Xen, Nutanix, Proxmox
- Физические сервера и рабочие станции под управлением ОС Windows, Linux, Mac OS
- Приложения: MS SQL, Oracle Database, MS Exchange, MS Sharepoint
- Облачные платформы: Office 365, Amazon, MS Azure



Особенности инфраструктуры:

Высокая распределенность сети и зависимость от уровня компетенций персонала



- **Простой интерфейс**
  Интуитивно понятный веб-интерфейс позволяет работать с системой даже неподготовленному персоналу, что особенно актуально при географически распределенной филиальной сети

- **Удобство администрирования**
  Автоматическая установка, групповые операции

- **Одна система и один агент**
  Весь функционал доступен через единую систему управления и единый агент на конечных устройствах

Особенности инфраструктуры АСУ ТП:

Наличие устаревшего оборудования и ОС

- **Решение поддерживает устаревшие ОС:**
  Windows XP, Windows 7,8,10, которые еще могут использоваться в прошивках некоторых устройств

- **Универсальное восстановление**
  Технология универсального восстановления позволяет восстанавливать системы на любое оборудование, даже с отличающимися характеристиками

Особенности инфраструктуры:

Сложности миграции на новое оборудование или среду виртуализации

- **Миграция без ограничений P2V, V2P, P2P, V2V**
  Решение позволяет мигрировать системы между физическими и виртуальными средами как в процессе восстановления так и как инструмент переноса системы между разными средами

- **Восстановление на любое «голое» железо**
  Вне зависимости от того совпадают его аппаратные характеристики с исходным устройством или нет

- **Резервное копирование без сети**
  Применение загрузочного носителя

Особенности инфраструктуры:

Высокая нагрузка и требования к доступности

- «Мгновенное восстановление»:
  Технология Acronis Instant Restore позволяет снизить время восстановления физических и виртуальных серверов (RTO) до секунд за счет прямого запуска образа резервной копии в качестве виртуальной машины на платформах VMware или Hyper-V

- В 2 раза быстрее восстановление физических устройств
  За счет подготовки полного образа готового к развертыванию на «голом» железе

- Без влияния на производительность оборудования
  Минимизированное окно резервного копирования и выполнение части операций по резервному копированию за пределами защищаемого оборудования позволяют минимизировать влияние операций резервного копирования на производительность систем

Особенности инфраструктуры:

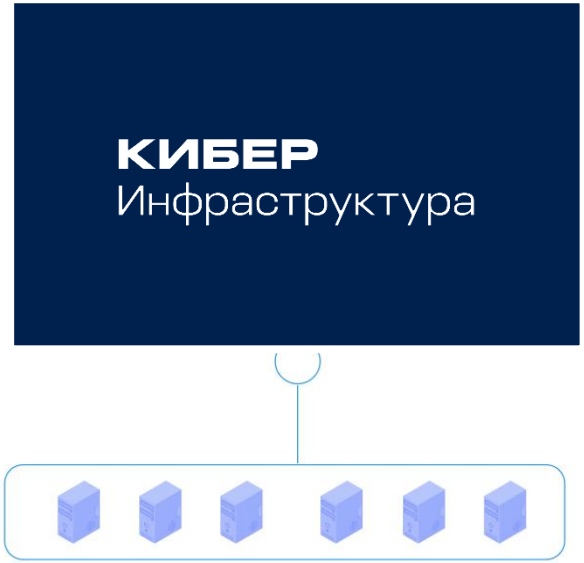
Частые атаки со стороны злоумышленников

- **Защита от атак нулевого дня**
  Встроенная технология активной защиты на основе алгоритмов машинного обучения блокирует действие вредоносного ПО (например вируса-шифровальщика) еще до того как его сигнатура попадет в базы антивирусов и автоматически восстановит поврежденные файлы
- **Защита всех подключенных устройств хранения**
  Технология защищает от воздействия вирусов-шифровальщиков как сами данные систем так и резервные копии
- **Оценка уязвимостей**
  Выявление уязвимостей до того, как злоумышленники их найдут. Определение уровня риска в системах
-

AV TEST APPROVED BACKUP & DATA SECURITY SOFTWARE av-test.org

Gold Self-Protection Award

Где хранить резервные копии?



Программно-опредеделяемое хранилище

- Возможность использования недорогих традиционных серверов в качестве узлов хранения
- Гибкое масштабирование за счет добавления дополнительных узлов хранения
- Интуитивно понятный интерфейс управления позволяет сократить расходы на поддержку решения

Кейсы внедрения на предприятиях в России

Решения «Акронис Инфозащиты» помогли создать комплексную систему резервирования данных для АСУ ТП ПАО «Северсталь»

ГАЗПРОМ

ЕВРАЗ

Северсталь

Сетевая Компания

Киберпротект

Работает

Удобно

Выгодно

Рядом

КИБЕРПРОТЕКТ

Благодарим за внимание