КИБЕР ПРОТЕКТ

info@cyberprotect.ru

Резервное копирование как последний шанс сохранить данные

Александр Львов

alvov@cyberprotect.ru

ПОТЕРИ ДАННЫХ ПРОИСХОДЯТ ПОСТОЯННО

90%

Потерь данных происходит по четырем причинам

Случайное удаление

49% потерь данных в результате ошибок

Поломка железа

560,000 жестких дисков выходят из строя в месяц

Зловредное ПО

365% – рост атак вирусов-вымогателей, основная угроза для данных в последние 3 года

Кража/потеря

70 миллионов компьютеров теряют/крадут в год

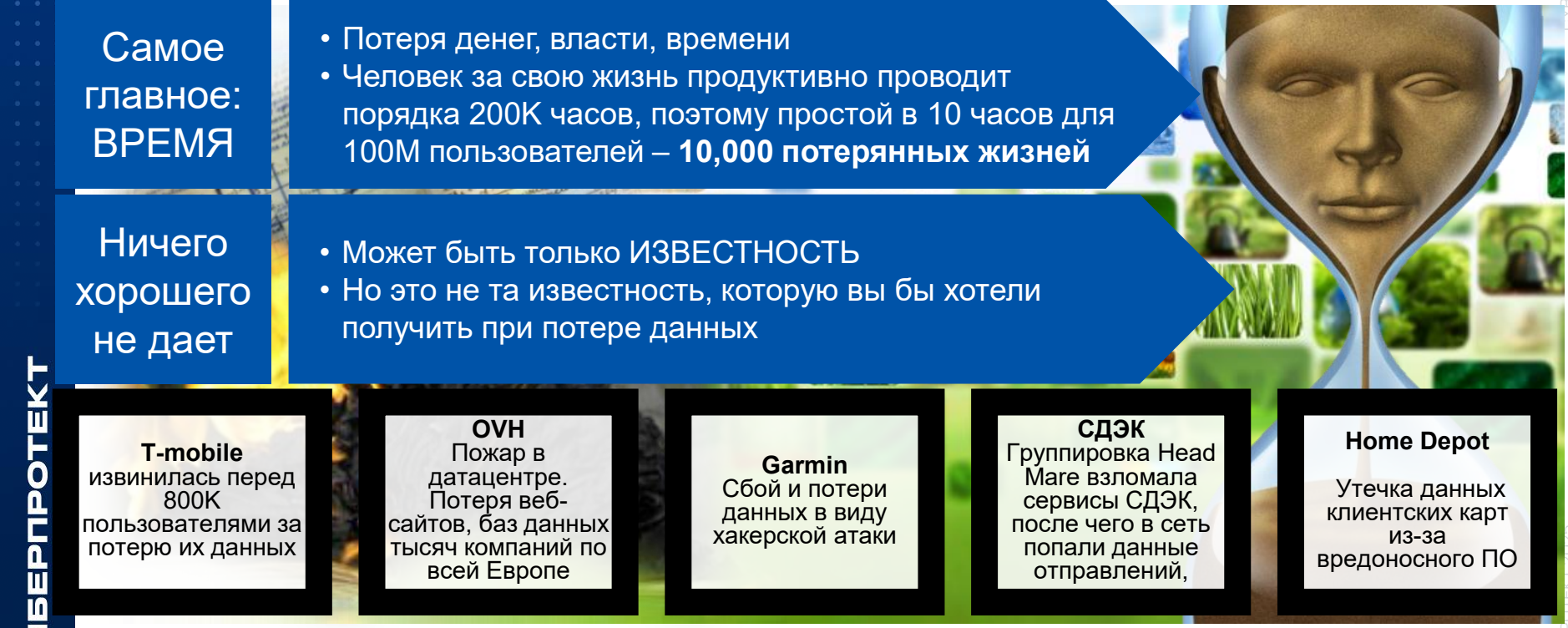
РЕЗУЛЬТАТЫ ПОТЕРЬ ДАННЫХ

Самое главное: ВРЕМЯ

- Потеря денег, власти, времени
- Человек за свою жизнь продуктивно проводит порядка 200K часов, поэтому простой в 10 часов для 100M пользователей – **10,000 потерянных жизней**

Ничего хорошего не дает

- Может быть только ИЗВЕСТНОСТЬ
- Но это не та известность, которую вы бы хотели получить при потере данных



T-mobile
извинилась перед 800K пользователями за потерю их данных

OVH
Пожар в датацентре. Потеря веб-сайтов, баз данных тысяч компаний по всей Европе

Garmin
Сбой и потери данных в виду хакерской атаки

СДЭК
Группировка Head Mare взломала сервисы СДЭК, после чего в сеть попали данные отправлений,

Home Depot
Утечка данных клиентских карт из-за вредоносного ПО

ДАННЫЕ СПАСЕНЫ ИЗ РЕЗЕРВНЫХ КОПИЙ

TARGET

Утечка данных из-за атаки. Бэкапы помогли восстановить работоспособность основных систем

X5 Group

Сбой в системе инвентаризации
Благодаря ежедневным бэкапам данные были восстановлены за 3 часа

МАГНОЛИЯ

Удаление данных по ошибке сотрудника
Аварийный план сработал — система восстановлена из резервной копии

ДЕЙСТВИЯ ДЛЯ СНИЖЕНИЯ РИСКОВ ПРОСТОЕВ И ЗАЩИТЫ ДАННЫХ

Даже при самых продуманных мерах защиты сбои неизбежны. Важнее не то, удастся ли их полностью избежать, а то, насколько быстро компания сможет восстановить работу и минимизировать последствия.

Анализа рисков и их воздействия на бизнес

- Какие системы критически важны для бизнеса, как быстро они должны быть восстановлены и какой объем данных компания готова потерять без ущерба для операционной деятельности.

Мониторинг и предиктивная аналитика снижают риски простоев

- Отслеживать не только технические сбои, но и поведение приложений, нагрузку на сеть и аномалии в пользовательской активности.

Регулярные обновления ПО и микрокодов компонентов оборудования

- Системы с неподдерживаемыми производителем оборудованием или версиями ПО часто становятся причиной инцидентов. Устаревшие версии одного из компонентов сложной архитектуры тянут за собой невозможность обновления других компонентов.

Защита от человеческого фактора

- Человеческий фактор чаще всего становится «слабым звеном». Подготовка сотрудников так же важна , как к защите оборудования и ПО

Ограничение доступа к продуктивному контуру

- Принцип «минимально необходимого». Распространение политик ИБ в полной мере на подрядчиков. .

КИБЕРПРОТЕКТ

ДЕЙСТВИЯ ДЛЯ СНИЖЕНИЯ РИСКОВ ПРОСТОЕВ И ЗАЩИТЫ ДАННЫХ

Регулярное обучение по информационной безопасности

- Специализированные программы помогают сотрудникам распознавать атаки, понимать угрозы социальной инженерии и правильно действовать при обнаружении подозрительных ситуаций.

Реальные сценарии реагирования

- Симуляции фишинговых атак и тесты на устойчивость к социальной инженерии.

Тренировки и сценарное тестирование

- Планы восстановления необходимо регулярно отрабатывать в реальных условиях. Такие упражнения позволяют не только проверить технические процессы «на прочность», но и выявить «узкие места» в коммуникациях между подразделениями.

Резервное копирование как основа непрерывности

- Резервное копирование остается фундаментом стратегии непрерывности бизнеса. Без регулярных копий компания теряет доступ к данным

Диверсификация рисков, связанных с хранением данных и их резервных копий

- Хранение резервной копии на отделяемом от основных данных оборудовании, а также гарантировать возможность восстановления на резервной площадке в случае полной недоступности основной.

ДЕЙСТВИЯ ПРИ ИНЦИДЕНТЕ

- ✓ **Запустить аварийный план**
  Первый шаг – активация заранее утвержденного сценария реагирования. Это позволяет исключить хаотичные действия и сэкономить драгоценное время.

- ✓ **Определить приоритеты восстановления**
  Решить, какие сервисы и данные критически важны и должны быть восстановлены в первую очередь. Это позволяет сосредоточить ресурсы там, где простой наиболее опасен для бизнеса.

- ✓ **Активировать резервные площадки или облачные сервисы**
  Если основная инфраструктура недоступна, задействуются резервные дата-центры или облачные решения для поддержания критических операций.

- ✓ **Восстановить критические сервисы и проверить их работоспособность**
  Недостаточно просто перезапустить систему – необходимо убедиться, что сервисы функционируют корректно и доступны пользователям.

- ✓ **Оценить ущерб**
  Важно проанализировать последствия инцидента не только в денежном выражении, но и в разрезе репутационных и операционных рисков.

- ✓ **Коммуникация с клиентами и партнерами**
  Прозрачность – ключ к сохранению доверия. Компании необходимо сообщить о сбое, обозначить ожидаемое время восстановления и держать клиентов в курсе.

- ✓ **Постинцидентный анализ**
  После устранения сбоя необходимо провести разбор ситуации: что сработало хорошо, а где есть слабые места. На основе этого обновляются BCP и DRP, чтобы исключить повторение проблемы.

ТРЕБОВАНИЯ К СОВРЕМЕННЫМ СРК

Масштабирование

- Поддержка различных типов данных и платформ
- Гибкие политики резервного копирования

Надежность и целостность данных

- Использование нескольких уровней защиты данных
- Автоматическая проверка целостности
- Тестирование восстановления

Автоматизация и централизованное управление

- Единая панель управления для мониторинга, настройки
- Автоматическое оповещение
- Интеграция с другими системами управления

Мониторинг и отчетность

- Мониторинг в реальном времени
- Генерация настраиваемых отчетов

Сохранность копий

- Шифрование данных при передаче и хранении
- Защита от ransomware
- Соответствие нормативным требованиям

Оптимизация и эффективность

- Удаление повторяющихся блоков данных
- Компрессия данных
- Быстрое восстановление

ПОРТРЕТ ПУБЛИЧНОГО КЕЙСА

Вертикаль

Реальный сектор (без ТЭК) 23%

Госуправление 17%

Медицина 14%

Образование и культура 14%

Ретейл 12%

ТЭК 12%

3%

Финансы 3%

Другая 2%

Государство и бизнес

Особенности внедрения

Организация резервного копирования до внедрения

Зарубежные СРК | Отсутствие СРК

22 рабочих дня

Реализация пилотного проекта / внедрение, [медиана]

Исполнитель

160 ТБ

Средний объём защищаемых данных

Частые отзывы

01 Простота развертывания и управления

02 Скорость резервного копирования и восстановления

03 Широкие функциональные возможности

04 Качество технической поддержки

05 Масштабируемость

РИВ ГОШ

В тройке
Ведущих бьюти-ритейлеров России

>250 магазинов
В десятках регионов страны

30
Серверов

800
Рабочих мест

1 000
Виртуальных машин

Географически распределённая инфраструктура

Различные информационные системы
1С, базы данных, файловые серверы, аналитические, учётные решения, системы отчётности, др.

~9 месяцев
Заняло поэтапное внедрение собственными силами

Система поддерживает все наши инфраструктурные технологии: хранилища SAN, платформу VMware, ленточные библиотеки, ОС, и отлично встроилась во все процессы. Работает стабильно, бесперебойно восстанавливая данные в любой нештатной ситуации.

“Киберпротект” выстраивает с заказчиком отличные рабочие коммуникации, все вопросы решаются оперативно. Мы вывели защиту данных на качественно новый уровень.

Дмитрий Смирнов
Руководитель группы администрирования серверов

Было
Зарубежные СРК Veeam Backup & Replication, Veritas NetBackup

Стало
Единая отечественная система резервного копирования

Объём защищаемых данных **~800 ТБ**

ДОМ МОДЫ HENDERSON

61 город России

География присутствия

160

Магазинов в торговых центрах

30

Рабочих станций и серверов под защитой

Задача

Минимизировать время простоев рабочих станций и серверов, вызванных инцидентами в ИТ-инфраструктуре

30

Дней пилотирования

1 день

Заняло внедрение собственными силами

> Дружелюбный интерфейс всегда является важным обстоятельством и для пользователей, и для ИТ-администраторов. Но для нас ключевым фактором выбора стала скорость восстановления данных. Здесь КИБЕР Бэкап показывает превосходные результаты.
>
> Заметно повысился внутренний KPI команды Service Desk.

Вячеслав Закариев

Руководитель отдела системных администраторов

Было

Отсутствие резервного копирования на рабочих станциях

Стало

Единая система резервного копирования серверов и рабочих станций

Объём резервных копий

~30 ТБ

КИБЕРПРОТЕКТ

Спасибо

Александр Львов
alvov@cyberprotect.ru