

Аутсорсинг IT-инфраструктуры.
Единый подход к обеспечению
надёжности, безопасности и
конфиденциальности

Маринов Дмитрий
dm@h1host.ru



ООО «H1»
<http://h1host.ru>

Аутсорсинг IT-инфраструктуры

Необходимость увеличения конкурентных преимуществ



Необходимость в надёжной и эффективной IT-инфраструктуре



Развитие и усложнение технологий повышает требования к наличию множества высокоспециализированных компетенций



Привлечение необходимых компетенций у аутсорсера экономически целесообразнее содержания большого штата высокооплачиваемых специалистов



Необходимость использования дорогих вычислительных комплексов и программного обеспечения, а также инженерной инфраструктуры



Использование аппаратных, программных и инженерных ресурсов аутсорсера



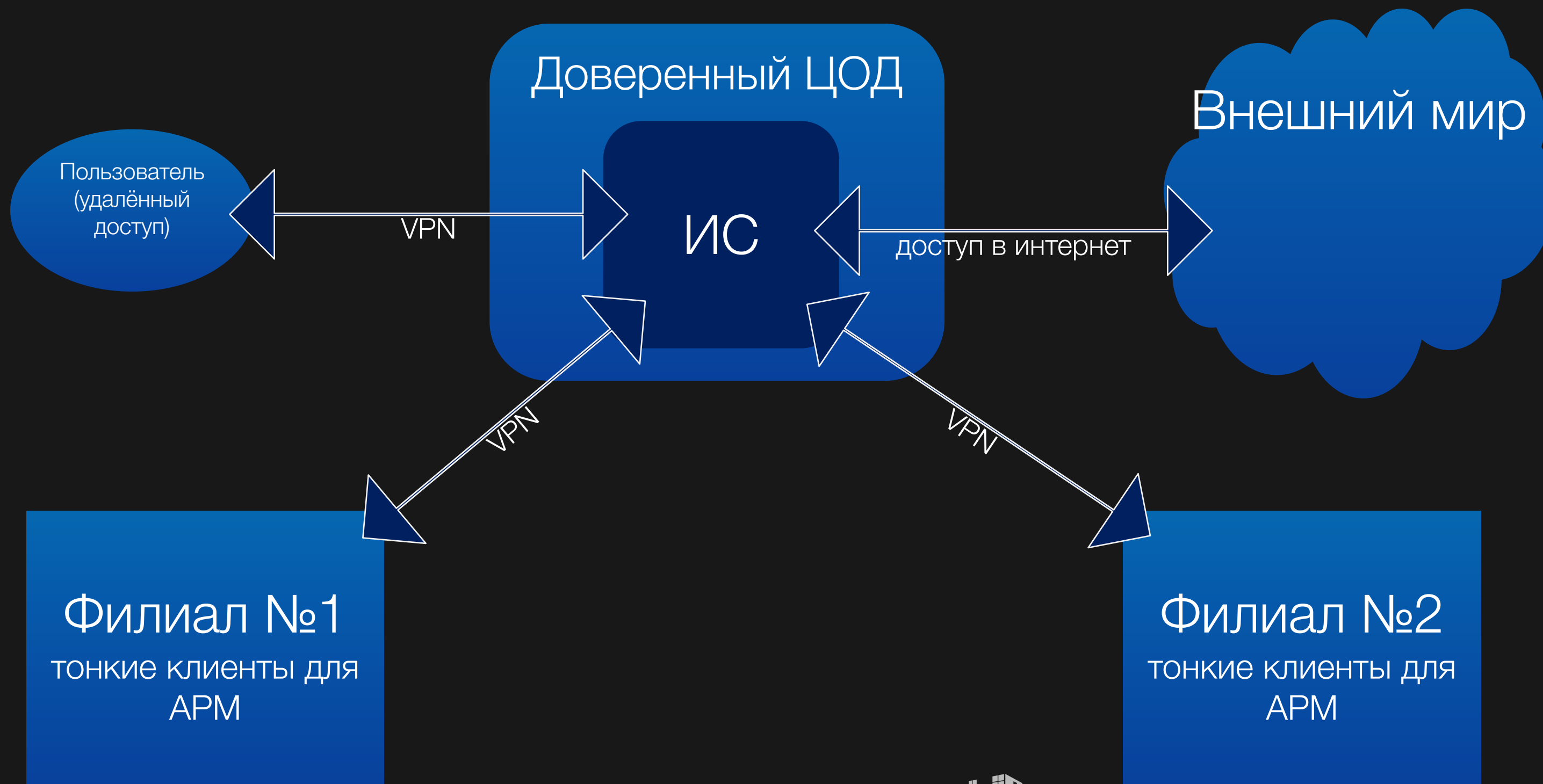
Факторы принятия решения использования аутсорсинга IT-инфраструктуры



- ▶ Капитальные вложения
- ▶ Операционные расходы
- ▶ Надёжность
- ▶ Безопасность
 - внешние угрозы
 - внутренние угрозы
- ▶ Доступность
- ▶ Телекоммуникации
- ▶ Защита персональных данных в соответствии с ФЗ-152



Структурная схема типового решения для аутсорсинга IT-инфраструктуры (SMB сегмент)



Влияние применяемого типового решения на различные факторы

Безопасность (от внешних угроз)

- доверенная изолированная сетевая среда
- межсетевые экраны (в том числе сертифицированные в РФ)
- системы защиты от DDoS, системы IPS (предотвращение хакерских атак)
- использование VPN-соединений для доступа в доверенную среду (в том числе сертифицированные в РФ)
- сильная авторизация пользователей (в том числе с использованием сертифицированных в РФ средств)
- централизованная система антивирусной защиты
- физическая безопасность обеспечена вооруженной охраной здания ЦОД

Безопасность (от внутренних угроз)

- фильтрация исходящего во внешний мир трафика с использованием DLP-решений
- централизованный контроль сетевых принтеров
- централизованный контроль USB-портов тонких клиентов
- комплексный мониторинг действий пользователей



Влияние применяемого типового решения на различные факторы

2

Конфиденциальность

- использование программно-аппаратных средств шифрования носителей информации в комплексе со средствами сильной аутентификации и средствами безопасности, применяемые в соответствии с регламентами безопасности, исключают физическую возможность случайного или преднамеренного доступа к конфиденциальной информации
- использование тонких клиентов в качестве АРМ - исключена возможность взлома и доступа к файлам и журналам
- использование для удалённого доступа к ИС средства Remoter

Надежность

- физическое расположение информационной системы в ЦОД с надёжностью инженерной инфраструктуры Tier3+
- применение вычислительных систем для размещения ИС заказчика Enterprise – уровня
- регулярное резервирование критичной информации или дублирование информации
- централизованный мониторинг работоспособности всех компонентов информационной инфраструктуры

Доступность

- централизованное управление всей информационной инфраструктурой
- доступ из любой точки земного шара
- резервированные каналы общей пропускной способностью более 10Gbps
- объединение географически распределённых офисов в единое информационное пространство



Влияние применяемого типового решения на различные факторы

3

Соответствие законодательству

- построение архитектуры, соответствующей необходимому классу защиты в соответствии с ФЗ-152 «О персональных данных»

Снижение издержек

- отсутствие необходимости содержания большого числа администраторов в штате
- отсутствие необходимости покупать дорогостоящее программное и аппаратное обеспечение
- отсутствие необходимости модернизировать имеющийся парк компьютеров
- гибкая возможность масштабирования системы (увеличение рабочих мест)
- быстрота подключения новых офисов
- максимальная утилизация имеющихся ресурсов с применением средств виртуализации



Кому и почему нужен аутсорсинг информационной инфраструктуры?

Техническому директору:

- если он заинтересован в развитии
- если он заинтересован в большем арсенале имеющихся в его распоряжении ресурсов

Топ менеджерам компании:

- если они заинтересованы в надёжном функционировании бизнес-процессов, работающих с применением IT
- если они заинтересованы в технологичности и эффективности бизнеса
- если они понимают финансовые и репутационные угрозы, связанные с некомпетентным построением IT
- если они понимают личную ответственность, связанную с потерей конфиденциальной информации
- если они понимают личную ответственность, связанную с несоответствием законодательству

Владельцам компании:

- если они заинтересованы в прозрачности бизнеса
- если они хотят фокусироваться на достижении стратегических целей
- если они хотят снизить издержки и повысить эффективность бизнеса
- если они хотят быть привлекательными для инвесторов



Догмы, риски, страхи и мифы аутсорсинга

Доверие к собственному персоналу выше, чем к сторонней компании

- аутсорсер, в отличие от персонала, несёт финансовую и репутационную ответственность за сохранность данных

Данные «под боком» хранить надёжнее, чем где-то там

- безопасность данных обеспечивается высоконадёжным оборудованием, комплексными средствами защиты от внешних и внутренних угроз, криптографическими методами шифрования информации, резервированием или дублированием критичной информации, круглосуточным мониторингом инфраструктуры, регламентами физического и удалённого доступа к системе в соответствии с политиками безопасности

Конфиденциальные данные могут быть прочитаны сотрудниками аутсорсера

- в соответствии с заключаемым договором, аутсорсинговая компания получает доступ только к тем данным, к которым её уполномочил владелец данных
- шифрование физических носителей данных, техническая невозможность прочтения без авторизации



Спасибо за ваше внимание.



ООО «H1»
<http://h1host.ru>