



Business  
Ecosystems

# Информационная безопасность

Каталог решений

# Содержание

<b>Модернизация сетевой инфраструктуры</b>	3
Фундамент сервисов безопасности	
<b>Управление доступом к информационным активам</b>	6
Единая платформа управления доступом к ресурсам корпоративной сети и защиты корпоративных данных на личных устройствах сотрудников	
<b>Сегментирование и межсетевое экранирование сетей</b>	9
Основа в разграничении доступа к информационным активам в компании	
<b>Обеспечение безопасности сети за счет интегрированных функций</b>	11
Самые эффективные инвестиции в защиту бизнеса	
<b>Решение по организации безопасного доступа в Интернет</b>	13
Комплексное решение защиты ваших сотрудников от угроз сети Интернет	
<b>Решение по организации удаленного доступа</b>	15
Возможность расширить границы бизнеса и снизить затраты на каждого сотрудника на 500 000 рублей ежегодно	
<b>Обнаружение и предотвращение вторжений в информационные системы предприятия</b>	19
Подход, обеспечивающий предупреждение инцидентов информационной безопасности	
<b>Система сбора и анализа событий безопасности</b>	21
Основа центра обеспечения информационной безопасности	
<b>Корпоративное облако</b>	22
Повышение масштабируемости, гибкости и безопасности вашего бизнеса	

# Модернизация сетевой инфраструктуры

## Фундамент сервисов безопасности

Сетевая инфраструктура является транспортом между всеми компонентами информационных систем – серверы и приложения, системы хранения данных, а также мобильные устройства и компьютеры пользователей. Надежность и безопасность такой среды определяет непрерывность и безопасность бизнеса.



### Предпосылки к применению

- Обеспечение непрерывного доступа к приложениям и данным.
- Создание платформы для доставки приложений и данных для каждого сотрудника, партнера и клиента.
- Обеспечение широких возможностей по оптимизации бизнес-процессов.
- Снижение эксплуатационных расходов.

### Проводная сеть

- Обеспечение единой транспортной сети для передачи голоса, видео и данных, без необходимости прокладывать и поддерживать отдельные сети.
- Обеспечение высокой масштабируемости сети по мере роста бизнеса.
- Обеспечение высокой производительности сети, позволяющей внедрять любые бизнес-приложения.
- Обеспечение непрерывной работа сети.

### Беспроводная сеть

- Возможность безопасно пользоваться любыми приложениями и Интернет, в любом месте с любых устройств без необходимости дорогостоящей прокладки кабелей.
- Повышение скорости бизнес-процессов.
- Непрерывный доступ к важнейшей информации.
- Мобильность сотрудников.
- Определение и анализ местоположения беспроводных клиентов, формирование исторических тенденций местоположений.
- Привлечение клиентов за счет доставки на их мобильные устройства данных (например, промо-акции в торговых залах) с учетом контекста в реальном времени.

### Корпоративная сеть

- Объединение всех офисов, филиалов, партнеров и клиентов в единое информационное пространство.



## Описание решения

### Проводная сеть

- Коммутаторы **Cisco Catalyst**.

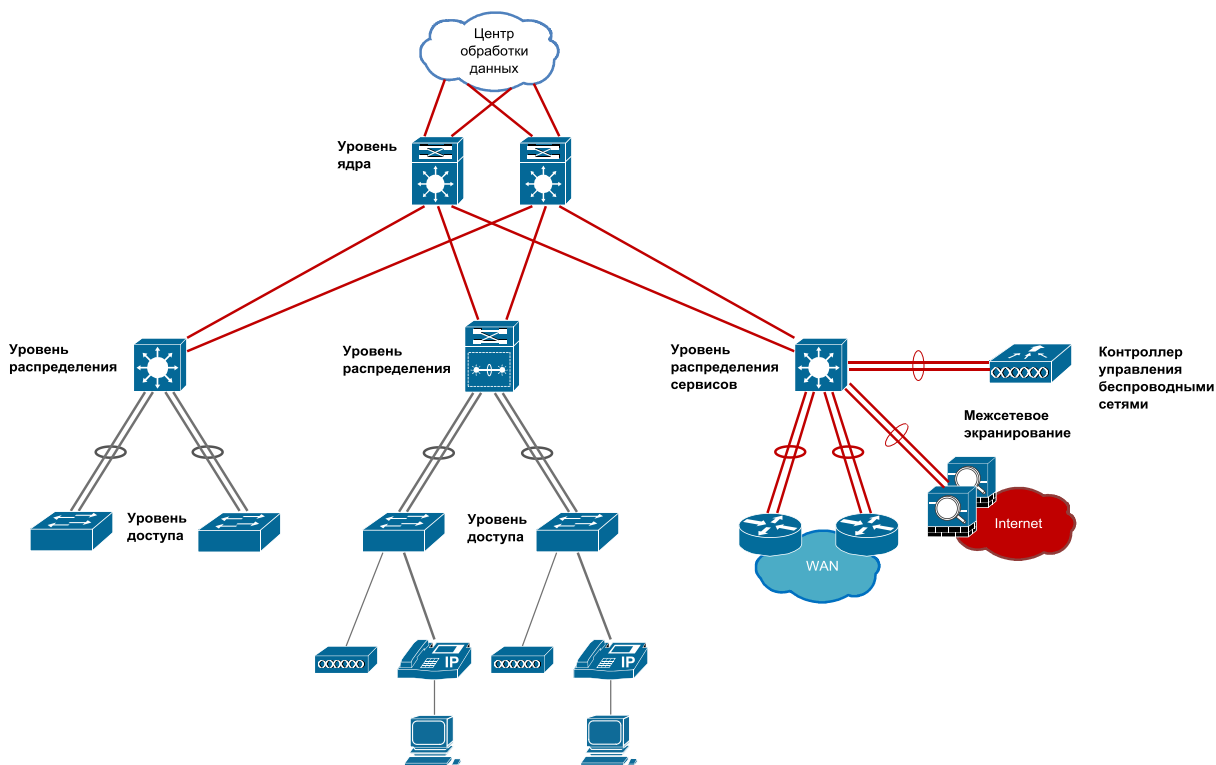
### Беспроводная сеть

- Контроллеры **Cisco Wireless LAN Controller**
- Система мониторинга **Cisco Prime**.
- Средство безопасности беспроводных сетей **Cisco Mobility Services Engine**.

- Сервисы определения местоположения.
- Внутренние и наружные точки доступа **Cisco Aironet**.

### Корпоративная сеть

- Маршрутизаторы **Cisco Integrated Service Router** и **Cisco ASR**.



Локальная сеть офиса или филиала

## Преимущества

### Преимущества пользователей

- Доступ в реальном времени к корпоративным приложениям и сетевым ресурсам.
- Широкие возможности для коммуникации с людьми без привязки к рабочему месту: отправка сообщений, телефонные звонки, видеоконференции.
- Единые настройки при перемещении между рабочими местами и между офисами.
- Возможность информационного обмена между партнерами и клиентами.

### Преимущества для администраторов безопасности

- Единое управление проводной, беспроводной и корпоративной сетью.

- Улучшение защиты беспроводных сетей за счет применения сервисов адаптивной защиты беспроводных сетей от вторжений.
- Обнаружение и отслеживание неавторизованных устройств, источников помех, клиентов Wi-Fi, смартфонов и меток радиочастотной идентификации (RFID) с помощью сервисов определения местоположения.
- Широкие возможности по масштабированию сетей за счет гибкой модели развертывания, включая новые возможности виртуализации.

### Преимущества для руководителей

- Широкие возможности по оптимизации бизнес-процессов.
- Единое информационное пространство для всей компании.
- Снижение эксплуатационных расходов.

- Непрерывная работа проводной, беспроводной и корпоративной сети.
- Адаптация сети к меняющимся бизнес-требованиям и оптимизация развертывания новых приложений.
- Быстрое масштабирование с ростом компании.
- Архитектурный подход, который дает представление о том какие затраты и мероприятия по модернизации необходимы для масштабирования компании и запуска новых бизнес-процессов.

# Управление доступом к информационным активам

Единая платформа управления доступом к ресурсам корпоративной сети и защиты корпоративных данных на личных устройствах сотрудников

Сотрудники все чаще запрашивают доступ к корпоративным ресурсам для работы на своих личных устройствах – ноутбуках, смартфонах, планшетах, как в офисе, так и за его пределами. Мобильность сотрудников сегодня повышает продуктивность труда и является конкурентным преимуществом для любого бизнеса. При этом существует угроза утечки данных. В то же время, ИТ-специалистам приходится поддерживать инициативы мобильности сотрудников при небольших бюджетах и ограниченности трудовых ресурсов для проводного, беспроводного и удаленного доступа в рамках всей компании.



## Предпосылки к применению

- Предоставить возможность сотрудникам работать с корпоративными приложениями и данными на собственных устройствах, обеспечивая безопасность корпоративных данных.
- Обеспечить управление и контроль доступа в корпоративную сеть. Построение политики доступа, основанной на критериях: кто подключается, откуда, каким способом, в какое время, с какого устройства и соответствует ли устройство требованиям безопасности и если не соответствует, то предоставить возможность для его автоматического приведения к соответствию политике безопасности. Основываясь на перечисленных выше и других критериях для каждого конечного устройства и пользователей предоставить доступ к заданным информационным активам в сети компании.
- Обеспечить быструю организацию гостевого проводного и беспроводного доступа в Интернет для гостей компании.

## Экономические показатели

## Затраты на поддержку мобильности сотрудников

Метрика	Значение
Часы, затрачиваемые на настройку, обеспечение безопасности мобильных устройств пользователей до внедрения предлагаемого решения в год	1 920 ч.
Процент времени, сэкономленного после внедрения данного решения	75 %
Ставка ИТ-администратора в час	750 р.
<b>Затраты в год</b>	<b>1 080 000 р.</b>

## Стоимость поддержания гостевого доступа

Метрика	Значение
Количество запросов на создание гостевых учетных записей в день	25
Время, затрачиваемое на создание учетной записи гостя в день	8 мин.
Процент времени, сэкономленного после внедрения предлагаемого решения	75 %
Ставка ИТ-администратора в час	750 р.
<b>Затраты в год</b>	<b>625 000 р.</b>

## Затраты на звонки в Help Desk из-за сложности установки повсеместных корпоративных политик

Метрика	Значение
Количество звонков в Help Desk, связанных с сетевым доступом и обновлением устройств без предлагаемого решения (для сотрудников) в год	12 000
Процент снижения звонков в Help Desk, связанных с сетевым доступом и обновлением устройств после внедрения предлагаемого решения	75%
Среднее время звонка	5 мин.
Средняя ставка специалиста Help Desk в час	1 200 р.
<b>Затраты в год</b>	<b>900 000 р.</b>

## Описание решения

## Состав решения

- Инфраструктура открытых ключей **Microsoft Public Key Infrastructure (PKI)**.

- Система **Cisco Identity Service Engine (ISE)**, представляющую собой платформу управления политиками безопасности.
- Система управления и обеспечения безопасности мобильных устройств **Good For Enterprise**, позволяющая защитить данные на личных мобильных устройствах сотрудников.
- Система разграничения доступа **Cisco Access Control Server (ACS)**.
- Коммутаторы **Cisco Catalyst**, точки беспроводного доступа **Cisco Aironet**, **Cisco Wireless LAN Controller (WLC)** (см. раздел , стр. ).
- **Сапликант 802.1X** (встроенный в операционную систему или **Cisco AnyConnect**).
- Сервис каталогов **Microsoft Active Directory**.



## Преимущества

## По управлению доступом к информационным ресурсам

## Преимущества пользователей

- Надежный и безопасный проводной, беспроводной и удаленный доступ в любом месте, в любое время и с любого устройства к бизнес-приложениям и сервисам, необходимых для работы.
- Снижено время предоставления доступа за счет повышения операционной эффективности управления доступом для ИТ-службы и службы поддержки.
- Оперативное получение проводного или беспроводного доступа к сети Интернет гостями компании.

## Преимущества для администраторов безопасности

- Точная идентификация любого устройства и пользователя.
- Простота применения единой корпоративной политики доступа на всех устройствах в сети.
- Централизованная консоль управления политиками доступа с учетом контекста: кто, откуда и с какого устройства подключается.

- Непревзойдённая прозрачность в сети с широкими возможностями профилирования для точной оценки всех пользователей и устройств, подключенных к сети.
- Исключительно надежный механизм для разграничения доступа в сети в соответствии с корпоративной политикой безопасности.
- Обширное и последовательное применение политик безопасности через средства управления сетевым доступом, систему управления безопасностью мобильных устройств и систему сбора, анализа и корреляции событий для выявления угроз безопасности и исключения возможностей для распространения атак в сети.

#### Преимущества для руководителей

- Корпоративные данные защищены от утечки через мобильные устройства сотрудников.
- В случае потери устройства или увольнения сотрудника, все корпоративные данные на этом устройстве уничтожаются.
- Прозрачность сети. Все устройства в сети точно идентифицируются, это позволяет создать для всех типов устройств, пользователей и типов доступа (проводной, беспроводной, удаленный) политику доступа.
- Задействованы интегрированные функции сетевой инфраструктуры, поэтому не требуются затраты на принципиальную модернизацию.
- Снижена нагрузка на специалистов ИТ.
- Единая политика доступа, действующая во всей инфраструктуре на всех видах доступа: проводной, беспроводной и удаленный.



#### По управлению безопасностью мобильных устройств

##### Преимущества для пользователей

- Интеграция почты, календаря, контактов и файлового менеджера.
- Защита бизнес данных при использовании сторонних приложений.

- Защищенный доступ к корпоративной сети через безопасный веб-браузер.
- Портал самообслуживания.
- Специальный репозиторий для хранения бизнес-данных на мобильном устройстве.

##### Преимущества для администраторов безопасности

- Возможность разделить личные и корпоративные данные на мобильных устройствах сотрудников.
- Обеспечить безопасность данных на мобильных устройствах средствами шифрования.
- Удаленное затирание данных на утерянных устройствах, с возможностью сохранять пользовательские данные.
- Блокировка различных функций мобильных устройств: камера, инфракрасный порт, Wi-Fi или Bluetooth.
- Управление доступом к приложениям на мобильных устройствах.
- Управление парольной политикой и контролем доступа.
- Возможность распространять и управлять приложениями через корпоративный AppStore.
- Обеспечение мобильных устройств наложенными средствами защиты при отсутствии встроженных.
- Легкость поддержки политик.
- Возможность управления большим парком мобильных устройств на основе ролевой модели доступа администраторов через веб-интерфейс консоли.
- Возможность ограничения функций «копирования» и «вставки» между различными приложениями.
- Поддерживаемы платформы: iOS, Android, Windows Phone.

##### Преимущества для руководителей

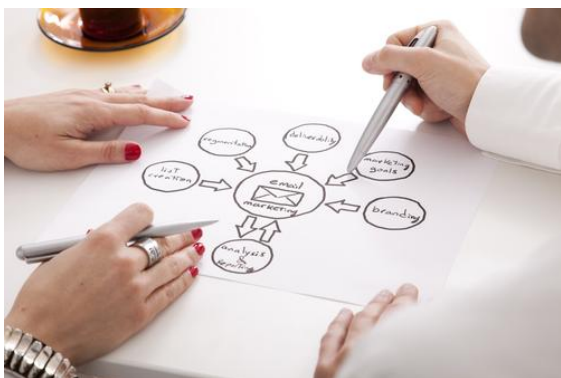
- Расширенные возможности взаимодействия пользователей.
- Высокий уровень безопасности бизнеса, несмотря на широкие возможности использования личных устройств сотрудников для работы.
- Повышения продуктивности работы пользователей за счет возможности работать в любом месте в любое время на свое привычном устройстве.
- Использование пользователями своих личных устройств избавляет от необходимости приобретать корпоративные устройства.



# Сегментирование и межсетевое экранирование сетей

Основа в разграничении доступа к информационным активам в компании

Ваши сотрудники, партнеры и клиенты должны иметь доступ только к тем бизнес-приложениям, которые необходимы для выполнения их бизнес-функций. Нарушение данного принципа может привести к утечке конфиденциальной информации, ущербу со стороны уволенных сотрудников, инсайдеров, рейдеров, мошенников, хакеров и вредоносного кода. В то же время, Интернет стал источником различных угроз, в том числе вирусов, шпионских программ, фишинга и других угроз. Сегментирование и межсетевое экранирование корпоративной сети позволяет существенно снизить описанные риски.



## Предпосылки к применению

- Существенное снижение рисков информационной безопасности.
- Обеспечение защищенности корпоративной сети от угроз сети Интернет.
- Обеспечение безопасности внутренней сети.
- Организация доступа пользователям сети Интернет к публичным информационным ресурсам Компании, исключая риски нарушения безопасности внутренних активов компании.

## Описание решения

### Сегментирование сетей

Позволяет выделить уровни доступа к ресурсам сети. Выполняется интегрированными средствами виртуализации сетей Virtual Routing and Forwarding Lite (VRF-Lite) и технологией Security Group Tagging (SGT). Эти механизмы встроены в оборудование Cisco Catalyst, лежащего в основе современной сетевой инфраструктуры (см. раздел «Модернизация сетевой инфраструктуры», стр. 3).

### Межсетевое экранирование

Позволяет реализовать политику доступа к ресурсам сети на основе выделенных сегментов

доступа. Выполняется с использованием следующих продуктов:

- Межсетевые экраны **Cisco Adaptive Security Appliance**, являющиеся самой доверенной и наиболее часто внедряемой платформой в отрасли уже более 15 лет.



- Система управления межсетевыми экранами **Cisco Prime Security Manager**, позволяющая централизованно управлять любым количеством межсетевых экранов, сохраняя высокий уровень безопасности и операционной эффективности администраторов безопасности.
- Система управления сетевым доступом **Tufin Orchestration Suite** в состав которой входят три подсистемы: **SecureTrack** для управления и аудита политик межсетевого экранирования; **SecureChange** для обеспечения процессов изменения политик доступа; **SecureApp** для управления доступом к приложениям в сети.

## Преимущества

### Преимущества для администраторов безопасности

- Высокая безопасность сети за счет применения политик доступа.
- Исключительная масштабируемость, отвечающая широкому набору бизнес-требований. За счет набора форм-факторов, производительности и сервисов безопасности, решение масштабируется для защиты от небольших филиалов до огромных офисов из нескольких зданий.
- Прозрачность сетевых потоков в компании и соотнесение их с пользователями, приложениями, устройствами и другими контекстными данными.
- Эффективное использование сетевых ресурсов за счет исключения не относящегося к бизнесу трафика и контента.
- Резкое сокращение ручных, повторяющихся и подверженных человеческому фактору задач связанных с конфигурированием политик доступа.

### Преимущества для руководителей

- Высокие показатели непрерывности бизнеса за счет предотвращения угроз информационной безопасности и защиты от нарушения работы критически важных бизнес-приложений и сервисов.
- Экономия затрат за счет снижения времени и ресурсов для удаления шпионских программ, вирусов и другого вредоносного кода.
- Защита информационных активов компании от хакеров, конкурентов и недобросовестных сотрудников.
- Увеличение производительности труда сотрудников за счет уменьшения времени на борьбу с вредоносным кодом.
- Низкая операционные затраты по поддержке политик доступа.
- Соответствие отраслевым и регуляторным требованиям в области информационной безопасности.
- Защита инвестиций. Данное решение имеет расширяемый функционал по безопасности доступный в виде отдельных модулей, которые могут использоваться в дальнейшем при дополнительных малых вложениях.

# Обеспечение безопасности сети за счет интегрированных функций

## Самые эффективные инвестиции в защиту бизнеса

Безопасность прикладных систем высокая на столько, на сколько высока безопасность инфраструктуры. Использование встроенных механизмов безопасности сетевой инфраструктуры позволяет исключить многие угрозы в локальных сетях вашей компании.

### Предпосылки к применению

- Исключение возможностей для реализации существующих угроз в локальной сети без применения дополнительных средств защиты.

**C** – конфиденциальность

**I** – целостность

**A** – доступность

- Глобальное применение интегрированных функций безопасности, исключающих угрозы, как для существующих, так и для новых информационных систем.

### Описание решения

- Коммутаторы **Cisco Catalyst**

В «Таблица 1» приведены существующие угрозы нарушения конфиденциальности, целостности и доступности информации в локальных сетях и перечень интегрированных функций, позволяющих их исключить.

Таблица 1. Защита от угроз нарушения конфиденциальности, целостности и доступности за счет применения интегрированных средств защиты

Угроза	C	I	A	Интегрированные функции
Подмена DHCP-серверов	■	■	■	– DHCP Snooping
Исчерпание пулов DHCP-серверов			■	– DHCP Snooping – PortSecurity (при отсутствии 802.1X)
ARP-спуфинг			■	– DHCP Snooping – Dynamic ARP Inspection

Деградация производительности из-за большого потока входящих ARP-пакетов	■	■	■	– DHCP Snooping – Dynamic ARP Inspection
IP-спуфинг	■		■	– DHCP Snooping – IP Source Guard – uRPF – Anti-spoofing ACL
Перехват трафика в локальной сети	■			– MACSec (необходимо внедрение 802.1X)
Атаки на протокол связующего дерева	■		■	– STP Toolkit
Переполнение CAM-таблиц	■		■	– PortSecurity (при отсутствии 802.1X)
Уязвимые сервисы сетевого оборудования	■		■	– Отключение сервисов
Защита от отказа в обслуживании			■	– QoS
Деградация производительности из-за большого количества трафика			■	– Traffic Strom Control
Невозможность доступа к управлению устройств из-за атаки отказ в обслуживании			■	– CoPP
Изоляция хостов внутри одного сегмента	■			– Downloadable ACL
Получение доступа к транковым интерфейсам на уровне доступа	■			– Конфигурация DTP
Атаки, связанные с нарушением механизмов разграничения доступа между VLAN	■			– Настройки безопасности VLAN

## Преимущества

### Преимущества для администраторов безопасности

- Исключение возможностей для реализации многих угроз локальных сетей.
- При масштабировании информационной системы компании, функции безопасности будут масштабироваться автоматически.

### Преимущества для руководителей

- Сократить расходы на средства защиты конечных устройств, обеспечивая безопасность за счет глобальных интегрированных функций сетевого оборудования.
- Отсутствие расходов при масштабировании информационных систем из-за распространение действия интегрированных функций на всю инфраструктуру.



# Решение по организации безопасного доступа в Интернет

Комплексное решение защиты ваших сотрудников от угроз сети Интернет

Интернет – это не отъемлемая часть любого современного бизнеса. Наряду со всеми преимуществами его использование сопряжено с рисками информационной безопасности, таких как воздействие вредоносного кода на устройства пользователей и инфраструктуру, утечка корпоративных данных снижение производительности труда сотрудников из-за нецелевого использования.

## Предпосылки к применению

**Сокращение расходов от последствий нарушения безопасности пользователей при работе в сети Интернет**

Метрика	Значение
Количество звонков в Help Desk, связанных с нарушением работы устройств пользователей из-за воздействия вредоносного кода из сети Интернет в год	12 000
Процент снижения звонков в Help Desk после внедрения предлагаемого решения	75%
Среднее время звонка	10 мин.
Средняя ставка специалиста Help Desk в час	1 200 р.
Среднее время, затрачиваемое на устранение последствий	6 000 ч.

воздействия вредоносного кода в год	
Средняя ставка специалиста по антивирусной защите в час	1 000 р.
<b>Затраты в год</b>	<b>9 000 000 р.</b>

**Повышение производительности труда сотрудников за счет анализа проводимого времени на различных сайтах**

Статья затрат	В месяц, руб.	В год, руб.
Средняя заработная плата одного сотрудника	60 000	720 000
Среднее время, проводимое сотрудником в Интернете в личных целях		<b>30%</b>
<b>Итого</b>	<b>18 000</b>	<b>216 000</b>

## Другие предпосылки

- Снижение рисков связанных с утечкой корпоративных данных через канал Интернет.

- Повышение производительности каналов доступа в Интернет за счет кеширования данных на 30-40%.

## Описание решения

**Cisco IronPort Web Security Appliance**, объединяющее несколько механизмов защиты, таких как передовая защита от угроз, прозрачный контроль приложений, детальная отчетность о действиях пользователей в одном решении.



## Преимущества

### Преимущества для пользователей

- Ускорение работы в Интернете, за счет кеширования данных.
- Отсутствие рекламы и нежелательного контента на страницах сайта.
- Безопасное посещение сайтов. Возможна ситуация, когда доступ к популярному ресурсу предоставлен пользователю (например, сайт валютных котировок), однако сегодня нередко случается, что такие сайты подвергаются атакам и начинают нести в себе угрозу пользователям. Но даже в такой ситуации предлагаемое решение обеспечит защиту за счет анализа и фильтрации загружаемых страниц и файлов.

### Преимущества для администраторов безопасности

- Гибкая настройка политики доступа в Интернет. Пользователей можно формировать по группам, например, в соответствии с организационной структурой, или бизнес-функциями. После чего каждой группе предоставить доступ к перечню категорий сайтов (например, финансы, новости, социальные сети, интернет-магазины и др.). Для формирования политики доступа можно использовать как встроенный категоризатор, в который входят наиболее посещаемые сайты, или же сформировать собственные категории. Встроенный категоризатор обновляется несколько раз в сутки.
- Контроль приложений. Для ряда приложений, таких как YouTube, Facebook, Skype, WebEx и других, можно предоставить доступ в соответствии с функциями бизнес подразделений. Например, отделу PR можно предоставить доступ на управление контентом страницы компании в социальной сети, но запретить любую другую активность.
- Интеграция с каталогом MS AD для идентификации и аутентификации пользователей, а также для формирования групп доступа.
- Управление доступом внутри HTTPS-туннеля. Это достигается за счет встраивания системы в HTTPS-туннель между защищенным ресурсом в сети Интернет и пользователем.
- Контроль передаваемых файлов.

### Преимущества для руководителей

- Повышение продуктивности сотрудников на рабочих местах.
- Отчетность о действиях пользователей. По каждому пользователю можно получить детальный отчет о том, какие сайты он посещал, в какое время, а также, сколько времени проводит в Интернете.
- Защита от угроз сети Интернет.
- Защита от утечек корпоративных данных через Интернет.

# Решение по организации удаленного доступа

Возможность расширить границы бизнеса и снизить затраты на каждого сотрудника на 500 000 рублей ежегодно

Удаленный доступ стал необходимой функцией для сотрудников, находящихся вне офиса или работающих из дома. Все больше и больше организаций предоставляют удаленный доступ своим сотрудникам и партнерам для эффективной совместной работы.



## Предпосылки к применению

### Экономические показатели

#### Арендная ставка

На каждого сотрудника, работающего в офисе, приходится более двух квадратных метров площади. Арендная ставка в городе Москве в офисах класса А, В, С:

Офис	1 м <sup>2</sup> в год, руб.	2 м <sup>2</sup> в год, руб.
Класс А	36 000	72 000
Класс В	27 000	54 000

Класс С	21 000	42 000
Средняя	24 000	56 000

Средняя арендная ставка составляет 56 000 рублей на каждого сотрудника ежегодно.

#### Фонд оплаты труда

- Наем сотрудников из регионов с более низкой рыночной заработной платой.
- Средняя заработная плата в Москве 45 000 руб., средняя заработная плата в регионах России около 20 000.
- Согласно исследованиям, 30% сотрудников согласились бы на снижение заработной платы на 10% при возможности работать удаленно.

Суммарные затраты на сотрудника в Москве относительно сотрудников, работающих в регионах:

Статья затрат	В месяц, руб.	В год, руб.
Дополнительные затраты на сотрудника в Москве	25 000	300 000
Дополнительно 10% за работу в офисе	2 000	24 000
Итого	27 000	324 000

**Затраты на питание**

Статья затрат	В месяц, руб.	В год, руб.
Обеды	5 000	60 000
Дополнительное питание в офисе	1 000	12 000
<b>Итого</b>	<b>6 000</b>	<b>72 000</b>

**Транспортные затраты**

Статья затрат	В месяц, руб.	В год, руб.
Единый билет на все виды транспорта	2 380	28 569
<b>Итого</b>	<b>2 380</b>	<b>28 569</b>

**Коммунальные платежи**

Статья затрат	В месяц, руб.	В год, руб.
Коммунальные платежи	300	3 600
<b>Итого</b>	<b>300</b>	<b>3 600</b>

**Другие затраты**

Существуют дополнительные затраты, связанные с организацией и поддержанием рабочего места в офисе:

- Оснащение рабочего места (стол, стул, настольная лампа и другая инфраструктура офиса);
- Канцелярские принадлежности;
- Уборка рабочего места;
- Офисная печать;
- Амортизация офисной техники;
- Техническая поддержка: трудозатраты на прием звонков, писем и других форм заявок, время и ресурсы на решение проблем с рабочими станциями и приложениями конечных пользователей.

**Все затраты**

Объединим все затраты в одну таблицу:

Статья затрат	Ежемесячные, руб.	Ежегодные, руб.
Арендная ставка	24 000	56 000
Фонд оплаты труда	27 000	324 000
Питание	6 000	72 000
Транспортные расходы	2 380	28 560
Коммунальные платежи	300	3 600

<b>Итого</b>	<b>59 680</b>	<b>484 160</b>
--------------	---------------	----------------

Получаем около полумиллиона затрат на одного сотрудника в год без учета других затрат. При суммировании других видов затрат сумма затрат вырастет примерно еще на четверть.

Перевод офисных сотрудников на удаленную работу не повлияет на безопасность бизнеса.

**Безопасность**

- Возможность организации доступа по смарт-карте или токену позволяет ограничить доступ к корпоративным приложениям только при наличии уникального предмета.
- Информация защищена от просмотра и искажения средствами шифрования и обеспечения целостности.
- Политика безопасности снижает риск несанкционированного доступа к защищаемой информации.

**Оперативность реагирования на бизнес задачи**

- В случае производственной необходимости, появляется возможность оперативного привлечения специалистов для работы в выходные дни или в период отпуска вне офиса.
- Где бы не находился сотрудник, автоматизированное рабочее место всегда находится с ним: в командировке, на встрече, в отпуске. У сотрудника имеются все условия для работы, аналогичные офису.
- Возможность работы организации в разных часовых поясах за счет привлечения сотрудников из разных регионов.
- Наверняка вы сталкивались с проблемой, когда необходимо оказывать сложную услугу, требующую достаточно высокой квалификации от сотрудников круглосуточно. Решение такой задачи в одном часовом поясе может быть трудным или затратным, поскольку на работу в ночную смену кандидатов намного меньше, а их вознаграждение обычно выше, чем у сотрудников с дневным графиком работы.

Оперативность	Работа в офисе	Удаленная работа
Время реакции на решение бизнес задачи в нерабочее время	от 90 мин.	1 мин.
Возможность работы компании в круглосуточном режиме	Ограничена	24 ч.

**Расширение географии при найме сотрудников**

Отличный способ приобретения для вашей компании любых компетенций и опыта за счет



найма сотрудников из любой точки мира. При поиске кандидата на удаленную работу, вы сможете рассматривать в десятки раз больше соискателей, чем при поиске на работу в офис.

### Повышение занятости сотрудников

- Возможность привлечения к работе сотрудников, находящихся в отпуске по уходу за ребенком или вне офиса по состоянию здоровья.
- Возможность сохранения занятости при неблагоприятном финансовом положении, что не потребует изменения штатного расписания и длительных согласований.
- Полезное время работы сотрудника в офисе составляет 30-40%. При удаленной работе может он может быть задействован до 80% времени.

### Работа с любого устройства

Предлагаемое решение позволяет работать на различных операционных системах:

- Windows;
- MAC;
- Linux;
- iOS;
- Android.

Это позволяет не ограничивать ваших сотрудников в выборе устройств для работы.

### Мотивация для сотрудников

- Повышение дохода за счет гибкости графика.
- Снижение трудоемкости за счет выполнения смежной работы.
- Снижение расходов: проезд, офисная одежда, еда.

## Описание решения

В основе решения лежат лучшие в отрасли продукты Cisco AnyConnect Secure Mobility в качестве программного VPN-клиента (VPN – виртуальная частная сеть), Cisco ASA 5500-X Series Adaptive Security Appliance в качестве VPN-шлюза и Aladdin eToken, обеспечивающего двухфакторную авторизацию. Данные продукты предлагают полный набор функций для организации VPN доступа наряду с мощными функциями безопасности. Администраторы безопасности могут предоставлять гибкий доступ к приложениям на основе политике безопасности.

Для обеспечения непрерывности работы решение может иметь отказоустойчивое исполнение.

### Схема решения удаленного доступа



## Преимущества

Решение Cisco AnyConnect Secure Mobility, используемое в качестве технологии организации удаленного доступа занимает лидирующую технологическую и концептуальную позицию по версии *Gartner* – самой авторитетной исследовательской компании мира на рынках информационных технологий.

Ниже приведены основные преимущества предлагаемого решения.

### Преимущества для пользователей

- Доступность на широком ряде платформ и операционных систем.
- Простота использования для конечного пользователя за счет получения преднастроенного клиента.
- Решение позволяет организовать устойчивое соединение с корпоративной сетью, несмотря на низкое качество связи.
- Простота интерфейса.

### Преимущества для администраторов безопасности

- Контекстно-зависимая политика безопасности, позволяющая учесть множество атрибутов доступа таких как время доступа, местоположение, тип операционной системы и другие.
- Возможность двухфакторной аутентификации.
- Гибкий контроль доступа. Позволяет организовать доступ к определенным приложениям и сервисам.

- Самая широкая поддержка операционных систем в отрасли.
- VPN-шлюз обладает интегрированными функциями межсетевого экрана.
- Масштабируемость. Решение имеет большие возможности по масштабированию. Поддержка до 10 000 удаленных пользователей на одном VPN-шлюзе и до 100 000 шлюзов с балансировкой нагрузки.
- Возможны сценарии без применения устанавливаемых клиентов.

#### **Преимущества для руководителей**

- Повышение производительности труда, за счет мобильного доступа с любого устройства без ущерба для безопасности.
- Сотрудники смогут осуществлять доступ к корпоративным ресурсам, откуда угодно, когда угодно и с любого устройства.
- Уверенность в том, что удаленная работа не нарушает безопасность организации.
- Низкая совокупная стоимость владения.

# Обнаружение и предотвращение вторжений в информационные системы предприятия

Подход, обеспечивающий предупреждение инцидентов информационной безопасности

Повышение уровня контроля за безопасностью вызвано из-за складывающихся тенденций мобильности, облачных вычислений, а также распространения целевых атак. Модель обеспечения безопасности на основе предлагаемого решения позволяет предотвращать атаки на различных векторах в любое время в течение всего времени.

## Предпосылки к применению

### Повышение операционной эффективности

- Сокращение времени реакции на инцидент информационной безопасности.
- Сокращение времени на расследование инцидента.
- Сокращение времени на восстановление после инцидента.

## Экономические показатели

Показатели	Cisco SourceFire	Ближайший конкурент
Уровень защиты	98,9%	92,76%
Общая стоимость владения (за 1 Mbps)	\$ 15,23	\$ 37,82

## Описание решения

### Система сенсоров

В основе решения лежит система сенсоров **Cisco Next Generation (NG) SourceFire Intrusion Prevention System (IPS)**.



### Положение сенсора на рынке

- Лидер в квадранте *Gartner*.
- Топ рейтинга самых производительных и точных сенсоров по версии *NSS Labs*.
- Наиболее эффективное средство защиты от вредоносных программ, рекомендованное Enterprise Strategy Group.
- Сертифицировано ICSA Labs.
- Получено более 40 патентов.

**Gartner**

**NSS Labs**

**ESG**

**ICSA Labs**

### Система управления сенсорами

Для управления сенсорами применяется система управления **Cisco FireSIGHT Defense Center**, позволяющая получать полную информацию от сенсоров в режиме реального времени и оперативно принимать решения по инцидентам безопасности.

## Преимущества

### Преимущества для администраторов безопасности

- Беспрецедентная защита от угроз в отрасли.
- Возможность увидеть и сопоставить большие объемы данных о событиях в условиях постоянно меняющейся информационной среды: приложений, пользователей, устройств, операционных систем, уязвимостей, сервисов, процессов, инфраструктуры, сетей, что дает большие возможности для обеспечения безопасности. Такие данные недоступны для средств защиты конечных устройств.

- Возможность автоматизированной оценки событий, настройки политик, анализа поведения сети и идентификации пользователей в сетевых потоках.
- Непревзойденная производительность, достигаемая за счет аппаратного ускорения, малого времени задержки при этом обеспечивая непревзойденную защиту в широком диапазоне нагрузок и скорости соединения.
- Обеспечение безопасности в виртуальных средах VMware, Citrix, Red Hat
- Частые и оперативные обновление правил выявления попыток несанкционированного доступа, формируемые глобальной аналитической системой безопасности на основе данных обрабатываемых от миллионов источников по всему миру.
- Реализованный метод траекторий для нахождения источника распространения угрозы.
- Интеграция с множеством сторонних систем через открытый API.

### Преимущества для руководителей

- Обеспечение безопасности критически важных информационных систем.
- Выявление попыток несанкционированного доступа к информационным активам.
- Ответность о состоянии уровня информационной безопасности, обладающих полнотой сведений о попытках несанкционированного доступа.
- Комплексный анализ одновременно всех сетевых потоков.
- Возможность предотвратить реализацию угрозы.



# Система сбора и анализа событий безопасности

## Основа центра обеспечения информационной безопасности

С ростом числа элементов инфраструктуры растет сложность анализ событий безопасности, поступающих от этих систем. Решение задачи анализа и корреляции большого объема данных возможно за счет применения предлагаемого решения.



### Предпосылки к применению

- Обнаружение инцидентов в режиме реального времени.
- Возможность проведения криминалистического анализа для обеспечения безопасности от кибератак.

- Автоматизированный сбор и архивирование событий безопасности.

### Описание решения

- Продуктивная линейка **HP ArcSight**.
- Продуктивная линейка **Splunk**.

### Преимущества

#### Преимущества для администраторов безопасности

- Сбор данных от различных элементов инфраструктуры и нормализация событий.
- Приоритезация событий.
- Корреляция потока данных.
- Мониторинг и расследование инцидентов.
- Анализ безопасности и отчетность.
- Хранение и архивация данных.

#### Преимущества для руководителей

- Прогнозирование рисков.
- Оперативное расследование инцидентов безопасности.
- Выявление инсайдеров.
- Защита информационных активов.

# Корпоративное облако

## Повышение масштабируемости, гибкости и безопасности вашего бизнеса

### Предпосылки к применению

#### Обеспечение конфиденциальности информационных активов бизнеса

Первое и самое главное преимущество корпоративного облака – это географическое расположение. Все корпоративные данные и приложения могут обрабатываться в любой точке мира, из которой компания получает все информационные технологии, используя только средства для отображения информации. Для защиты от компьютерных атак применяется комплекс технических мер, направленный на исключения риска от реализации внешних и внутренних угроз.



#### Обеспечение непрерывности бизнес-процессов

Основной принцип применяемый при проектировании корпоративного облака – это использование избыточности устройств и связей для повышения надежности. Непрерывность работы обеспечивается технологиями, позволяющими быстро определить отказ и произвести восстановление работы без нарушения бизнес-процессов в компании.

#### Обеспечить масштабируемость и гибкость

Рост организации обуславливает необходимость роста ИТ-инфраструктуры. Продукты и решения, применяемые в корпоративном облаке, выбираются таким образом, чтобы обеспечить модульный принцип масштабирования. При этом каждый этап масштабирования имеет прозрачную структуру капитальных и операционных затрат.

#### Обеспечить простоту в управлении

Разработка бизнес процессов управления и подробной эксплуатационной документации, позволит упростить процедуру поддержки для специалистов заказчика. Аутсорсинг сопровождения корпоративного облака позволит эффективно эксплуатировать ИТ-ресурсы и исключить непрофильный вид деятельности.

#### Повысить экономическую эффективность информационных технологий

Закладывался как основной руководящий принцип при проектировании для обеспечения всем необходимым развивающуюся организацию.

#### Получение ресурсов по запросу

Корпоративное облако представляет собой объем ресурсов в виде процессоров, оперативной памяти, жестких дисков, сетей, сервисов и этим можно распоряжаться как угодно в любое время для решения бизнес задач: запуск нового приложения, создание автоматизированного рабочего места для сотрудника, автоматизации целого офиса или филиала в любой точке мира. Если бизнес

задача теряет актуальность, ресурсы просто возвращаются в общий объем доступных ресурсов до следующей потребности.

### Увеличить скорость запуска бизнес приложений и сервисов

Время на ввод в эксплуатацию сервера или рабочей станции не превысит 15 минут. Таким образом, запуск и тестирование новых бизнес идей в виде приложений и сервисов может осуществляться очень быстро. Процесс создания автоматизированных рабочих мест для новых сотрудников будет выглядеть не сложнее и не занимать больше времени, чем оплата сотовой связи в терминале. Скорость создания офиса из рабочих мест также будет осуществляться очень быстро, при этом все сотрудники смогут получить любые имеющиеся корпоративные сервисы на свое рабочее место, где бы оно ни находилось.

## Описание решения

Корпоративное облако меняет экономические показатели, объединяя вычислительные и сетевые компоненты, а также компоненты для хранения, виртуализации и управления в единую платформу. Результатом является повышение удобства эксплуатации и оперативности деятельности — важные факторы для применения облачных технологий и внедрения концепции «информационные технологии как сервис».

### Интеллектуальная бизнес-ориентированная архитектура

Компанией Cisco Systems была разработана интеллектуальная бизнес-ориентированная архитектура (Smart Business Architecture – Data Center, SBA – DC). Применение данной архитектуры в растущих организациях позволяет провести миграцию от собственной серверной комнаты к масштабируемому и отказоустойчивому корпоративному облаку.

Данная архитектура состоит из трех основных взаимосвязанных компонентов.



### Основа центра обработки данных

Основа корпоративного облака обеспечивает вычисления, необходимые для поддержки приложений, которые обрабатывают информацию и прозрачную передачу между серверами, системами хранения и конечными пользователями, которые получают доступ к приложениям.

### Сервисы центра обработки данных

Сервисы корпоративного облака являются следующим слоем в иерархии. Например, вам может понадобиться большая площадь помещения для производства, или высокий забор с системой контроля доступа. Наличие сервисного уровня позволяет сделать среду удобной для использования, повышая операционную эффективность.

Сервисы включают межсетевые экраны, системы сенсоров предотвращения вторжений, а также сервисы приложений, такие как балансировка нагрузки и мониторинг для оперативного реагирования.

### Пользовательские сервисы

Пользовательские сервисы находятся на вершине пирамиды. Пользовательские сервисы это такие приложения, которые позволяют сотрудникам выполнять их должностные обязанности и улучшать показатели бизнеса. В контексте здания это может быть лифт, который позволит перемещаться между этажами сотрудникам, освещение в офисе, или кнопка проверки сообщений на телефоне.

Пользовательские сервисы в корпоративном облаке включают почту, обработку заказов и файловые хранилища, а также безопасный доступ в Интернет. Другие приложения, которые зависят от основы корпоративного облака и сервисов, как например, системы управления базами данных, обработки транзакций, моделирования также находятся на самой вершине пирамиды.

### Отказоустойчивость

Все технические решения, функционируют в помещениях, оснащенных системами бесперебойного питания на случай временных перебоев, дизель-генераторами, мощными интеллектуальными системы кондиционирования и климат-контроля, независимыми системами подачи электроэнергии. Помещения располагаются в сейсмобезопасных районах.

### Географическое разнесение

Возможны две модели обеспечения катастрофоустойчивости корпоративного облака на географическом уровне:

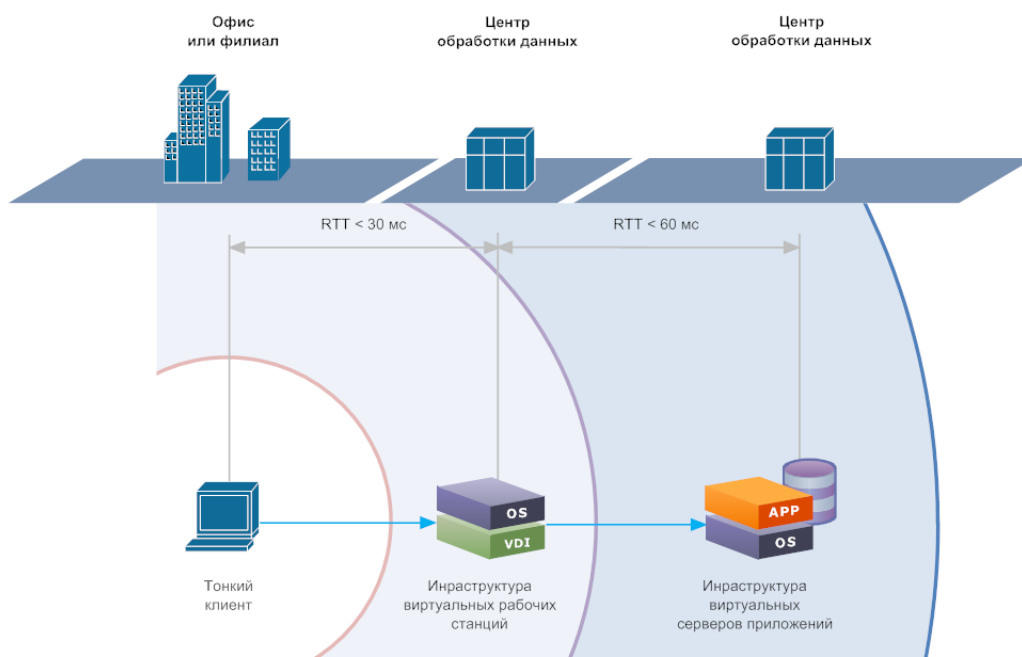
- **Один машинный зал** в любой точке мира.
- **Два машинных зала на расстоянии до 60 километров**, объединенных оптическими каналами в любой точке мира.

Оба варианта представляют собой одно корпоративное облако с различной степенью катастрофоустойчивости.

Также допускается выделение отдельной инфраструктуры виртуальных рабочих столов, которая может быть размещена на расстоянии, при котором время задержки сигнала (RTT) не превысит 30 мс, что связано с комфортностью работы пользователей. Такой принцип позволит, полностью, исключить зависимость от информационно-технологической инфраструктуры привязанной к географии размещения рабочих мест.



Возможности по географическому разнесению инфраструктуры



Структурная схема получения доступа к информационным активам компании

### Узлы и связи

Узлы и связи в корпоративном облаке имеют резервирование. Для обеспечения непрерывной работы, используются технологии и протоколы с различным показателем времени восстановления после сбоев от миллисекунд до минут.

### Каналы связи

Среди каналов связи корпоративного облака выделяют:

- **Арендные каналы.** Применяются в том случае, когда запрашиваемый из корпоративного облака сервис чувствителен к качеству канала. Например, IP-телефония или видеоконференцсвязь, когда потеря данных приводит к ухудшению сервиса.
- **Каналы Интернет** используются для подключения корпоративного облака к сети Интернет и в качестве транспортной среды для создания корпоративной сети.

Применяя технологии и методы резервирования каналов связи, можно добиться оптимальных

результатов сетевой доступности корпоративного облака по глобальным каналам связи. Например, обеспечить стабильную доступность веб-портала для клиентов или корпоративных приложений для всех пользователей.

## Безопасность

### Доступ

Подключиться к корпоративному облаку могут только те офисы, сотрудники, партнерские организации или клиенты которым будет явно предоставлен доступ. Никто другой не сможет подключиться к корпоративному облаку.

Подключение мобильных клиентов возможно только с определенных устройств или по токену.

### Каналы связи

Все каналы доступа в корпоративное облако защищены криптографическими средствами, что позволяет подключаться через сеть Интернет или любые другие публичные сети.

Расшифровать данные даже в случае перехвата будет невозможно.

### Сегментирование и межсетевое экранирование

Доступ пользователей к приложениям предоставляется на основе правил доступа системы межсетевого экранирования. Сегментирование сетей позволяет сгруппировать информационные ресурсы по уровню доступа.

### Системы обнаружения и предотвращения вторжений

Для выявления и предотвращения компьютерных атак применяются сенсоры систем обнаружения и предотвращения вторжений.

### Контроль сетевого доступа

Для разграничения доступа в сетях корпоративного облака применяется система контроля и учета доступа.

### Безопасность виртуальных сетей в облаке

Атаки в сетях корпоративного облака исключаются за счет технологий обеспечения безопасности коммутируемой среды.

## Масштабируемость

Модульный принцип, заложенный в архитектуре SBA-DC, позволяет широко масштабировать ресурсы центра обработки данных с минимальными финансовыми затратами.

## Гибкость

### Балансировка нагрузки

Обеспечивается стабильная работа высоконагруженных прикладных сервисов за счет организации кластеров.

### Оптимизация трафика

Система оптимизации прикладных данных позволяет существенно расширить возможности каналов связи за счет алгоритмов сжатия данных.

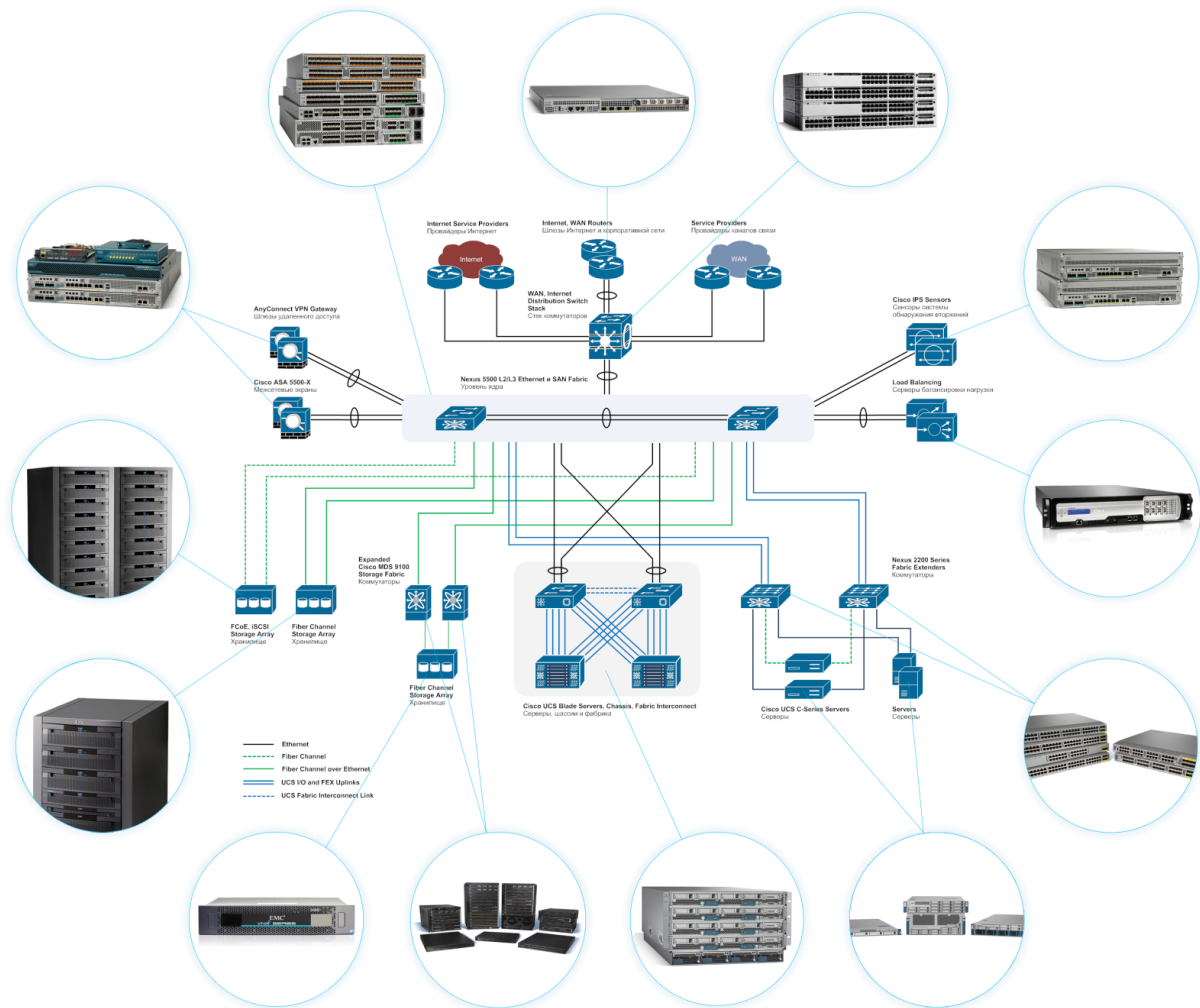
## Управляемость

Обслуживать корпоративное облако может внутренняя ИТ-служба или служба технической поддержки по запросу.

В любой момент времени доступ к корпоративному облаку может быть ограничен для любых из подключаемых площадок или сотрудников. Сделать это возможно оперативно с любого устройства из любой точки мира.

## Поддержка

При изменении потребностей бизнеса и возникновении новых задач, они будут оперативно решены в корпоративном облаке обращением в техническую поддержку, которая работает круглосуточно 365 дней в году.



Пример структуры корпоративного облака



## Технико-экономическое обоснование

### Преимущества конвергенции и консолидации

#### Увеличение вычислительной мощности на одну единицу арендуемой площади в машинном зале центра обработки данных (Rack Unit, RU)

Решение	Влияние на CapEx	Влияние на OpEx
<ul style="list-style-type: none"><li>Увеличение емкости памяти: 32 DIMM слота с процессорами Intel Xeon серии 7500 на один слот блейд-шасси.</li><li>Увеличение операций ввода-вывода (IOPS): применение блейд-серверов Cisco UCS B200M3, обеспечивающих производительность до 80 Gbps.</li></ul>	<ul style="list-style-type: none"><li>Большой объем памяти и более высокие возможности ввода-вывода в сочетании с преимуществами Cisco UCS Manager позволяют достичь большей плотности виртуальных машин на одном физическом сервере, обеспечивая при этом безупречную производительность.</li><li>Эта возможность значительно уменьшает количество серверов и в свою очередь занимаемую арендуемую площадь.</li><li>Уменьшение количества серверов также влияет на сетевой уровень корпоративного облака, существенно уменьшая потребление портов и коммутаторов, снижает количество связей, что в свою очередь снижает сложность управления.</li><li>При сравнении блейд-серверов на базе процессора Intel Xeon 7500 с подобными серверами, система Cisco UCS может обеспечить на 25% больше вычислительных ресурсов на одну единицу арендуемой площади.</li></ul>	<ul style="list-style-type: none"><li>Более высокая плотность серверов эквивалентна уменьшению арендуемой площади.</li><li>Более высокая вычислительная плотность. Это ускорение означает повышение рентабельности и потенциального конкурентного преимущества на рынке.</li><li>Продвижения отложенных проектов и инициатив, связанных с корпоративным облаком, что позволяет повысить эффективность и достичь большей доходности.</li></ul>

### Снижение капитальных затрат на серверы, необходимые для функционирования приложений с высокой нагрузкой на память

Решение	Влияние на CapEx	Влияние на OpEx
<ul style="list-style-type: none"> <li>Cisco UCS объединяет технологию Cisco Extended Memory, которая обеспечивает в два раза больший объем памяти (384 Гб), как и традиционные 2-процессорные сервера, повышая производительность и емкость для больших наборов данных и нагрузок.</li> </ul>	<ul style="list-style-type: none"> <li>За счет увеличения степени консолидации для 2-процессорных серверов, Cisco UCS сохраняет как CapEx и стоимость лицензий на обеспечение функционирования программного обеспечения на больших 4-процессорных серверов.</li> <li>За счет возрастания утилизации серверных ресурсов, Cisco UCS позволяет сократить количество серверов, обеспечивающих требуемую рабочую нагрузку, сохраняя текущий CapEx.</li> </ul>	<ul style="list-style-type: none"> <li>Снижение расходов на электроэнергию, необходимую для охлаждения и электропитания.</li> <li>Улучшенная система охлаждения и электропитания, уменьшающая на 50% число компонентов требующих охлаждения и электропитания.</li> <li>Системы Cisco UCS требуют на 37% меньше арендуемого стоечного места, поддерживая на 60% больше серверов на одно арендуемое стоечное место.</li> <li>Снижение стоимости сервисных контрактов за счет снижения аппаратные платформы.</li> </ul>

### Исключение нежелательных инвестиций для увеличения пропускной способности сети и операций ввода-вывода

Решение	Влияние на CapEx	Влияние на OpEx
<ul style="list-style-type: none"> <li>Cisco UCS объединяет большую пропускную способность сети и возможности по экономически эффективному масштабированию</li> <li>Cisco UCS включает в себя виртуальную интерфейсную карту (VIC) без дополнительных затрат на ввод/вывод при масштабировании от 20 60 GBps, и потребует только одну дополнительную виртуальную (без конвергентных коммутаторов) для каждых следующих 20 GB.</li> </ul>	<ul style="list-style-type: none"> <li>Традиционные серверы требуют 2 конвергентных коммутатора плюс конвергентный сетевой адаптер (CNA) для каждых дополнительных 20 GB после первых 20 GB.</li> </ul>	<ul style="list-style-type: none"> <li>Операционные затраты, исключаящие рост стоимости на энергопотребление, охлаждение и арендуемого места, связанных с установкой дополнительных коммутаторов и сетевых карт.</li> <li>Трудозатраты, направленные на развертывание и управление растущего количества коммутаторов и сетевых карт.</li> <li>Затраты на дополнительные сервисные контракты, связанные с поддержкой дополнительных коммутаторов и карт используя традиционные серверы.</li> </ul>

**Снижение расходов на поддержку и управление**

Решение	Влияние на CapEx	Влияние на OpEx
<ul style="list-style-type: none"> <li>▪ Cisco UCS Manager выступает в качестве единой программной платформы управления для серверов</li> </ul>	<ul style="list-style-type: none"> <li>▪ Сокращение затрат на лицензирование отдельных платформ управления (традиционная инфраструктура предусматривает 9 платформ для управления).</li> </ul>	<ul style="list-style-type: none"> <li>▪ Снижение затрат на обучение администраторов (за счет сокращения количества платформ для работы на которых требуется обучение).</li> </ul>

**Повышение сетевой эффективности, обеспечивающей необходимое качество обслуживания несмотря на централизации серверов**

Решение	Влияние на CapEx	Влияние на OpEx
<ul style="list-style-type: none"> <li>▪ Консолидация серверов позволит исключить их присутствие в офисах, где их близость обусловлена высококачественным обеспечением пользователей требуемыми сервисами. Использование Cisco WAAS позволяет обеспечивать производительность для приложений при предлагаемом подходе консолидации аналогичную локальному присутствию.</li> </ul>	<ul style="list-style-type: none"> <li>▪ Сокращение капитальных затрат за счет консолидации серверов и снижению стоимости лицензий.</li> </ul>	<ul style="list-style-type: none"> <li>▪ Сокращение затрат на арендуемое место, энергопотребление и охлаждение, а также сервисные контракты, связанные с консолидацией.</li> </ul>

**Объединение сетей передачи данных и сетей хранения**

Процесс консолидации сетей позволяет существенно сократить затраты. При традиционном подходе, обычный корпоративный сервер должен иметь от шести до восьми исходящих от него соединений включая соединения для передачи сетевых данных и данных систем хранения, а также выделенные соединения для управления или резервного копирования. Однако, каждое из этих соединений увеличивает стоимость:

- Для каждого соединения необходима PCI-карта
- Для каждой карты необходим слот.
- Для большого количества слотов требуются большие серверы. Большие серверы в свою очередь требуют большего арендуемого места для размещения и больших затрат на электропитание.
- Необходимы интерфейсы для подключения инфраструктуры систем хранения и сетей передачи данных (включая коммутаторы, HBA порты и сетевые адаптеры).
- Для каждого интерфейса необходим кабель, кроме того, для соединения большого количества кабелей требуются большие трудозатраты.

Каждый кабель должен быть подключен к портам коммутаторов, что в свою очередь означает увеличение количества коммутаторов, а это приводит к увеличению стоимости аренды, энергозатратам и затратам на охлаждение.

Решение **Cisco Unified Fabric** позволяет заменить все эти интерфейсы на два порта Ethernet пропускной способностью 10 Гбит/с, а также позволяет объединить две сети – Ethernet и Fiber Channel в одной физической инфраструктуре. Такой подход позволяет исключить необходимость в приобретении, установке, настройке и управлении двух наборов коммутаторов, которые требуют соответствующие CapEx (например, стоимость сетевых интерфейсных карт, HBA-портов и сетевых адаптеров) и OpEx (стоимость арендуемого места, энергозатрат и затрат на охлаждение). Комбинация двух этих преимуществ при объединении сетей хранения и передачи данных предоставляет преимущества, представленные в таблице.

**Снижение стоимости и сложности сетевых соединений**

Решение	Влияние на CapEx	Влияние на OpEx
<ul style="list-style-type: none"> <li>Cisco Unified Fabric позволяет заменить 6 – 8 традиционных соединения на два 10 Gigabit Ethernet, что значительно сокращает связанные с этим расходы (PCI карты, серверные слоты и кабели)</li> </ul>	<ul style="list-style-type: none"> <li>Сокращение капитальных затрат на 50 – 70% на сервер.</li> <li>Уменьшение количества необходимых слотов на 60 – 70%, что позволяет организациям приобретать меньшее количество серверов или отсрочить закупки больших серверов (с соответствующим снижением эксплуатационных расходов)</li> <li>Средняя стоимость одного соединения составляет \$750. Для среднестатистического облака удается сократить количество соединений на 75% с 400 до 100.</li> </ul>	<ul style="list-style-type: none"> <li>Объединенный эффект от значительного сокращения соединений и возможность приобретения меньших серверов (или отсрочка покупки больших серверов) позволяет сократить затраты на энергопотребление, охлаждение и арендуемую площадь для размещения оборудования в центрах обработки данных.</li> <li>Снижение трудозатрат на коммутацию за счет снижения количества кабелей.</li> </ul>

**Снижение затрат за счет объединения сетей хранения и передачи данных**

Решение	Влияние на CapEx	Влияние на OpEx
<ul style="list-style-type: none"> <li>Объединение SAN и LAN сетей позволяет достигаться за счет конвергентных коммутаторов</li> </ul>	<ul style="list-style-type: none"> <li>Расходы, связанные с коммутаторами SAN инфраструктуры, NIC и HBA картами, кроссировочными кабелями, необходимыми в традиционных архитектурах LAN существенно снижаются.</li> </ul>	<ul style="list-style-type: none"> <li>Сокращение на 50% затрат, связанных с энергопотреблением, охлаждением, арендой стоечного места для размещения дополнительного сетевого оборудования.</li> <li>Снижение затрат на поддержку за счет упрощения инфраструктуры. Все заказчики добились сокращения соответствующих трудозатрат на 20%.</li> </ul>

**Повышение утилизации серверов и плотности виртуальных машин через распространение виртуализации**

Решение	Влияние на CapEx	Влияние на OpEx
<ul style="list-style-type: none"> <li>Интегрированная архитектура Cisco UCS в сочетании с такими инновациями как расширяемая память, новейшими процессорами Intel, высокой скоростью доступа к памяти, которая на 27% превосходит ближайших конкурентов</li> </ul>	<ul style="list-style-type: none"> <li>Увеличенная утилизация серверов позволяет сократить CapEx и расходы, связанные с лицензированием.</li> <li>Например, используя возможности виртуализации Cisco UCS, компания NetApp смогла консолидировать 51 блейд-серверное шасси и 714 серверов в 15 Cisco UCS шасси и 120 серверов для одного из своих облачных сервисов.</li> </ul>	<ul style="list-style-type: none"> <li>Снижение затрат на сервисные контракты для оборудования, энергопотребление, охлаждение, арендованную площадь за счет увеличения утилизации сервера.</li> <li>Например, компания Trademark заменила свои традиционные серверы на Cisco UCS и смогла увеличить серверную утилизацию на 400% при сохранении таких же затрат на энергопотребление и охлаждение.</li> </ul>

## Экономически эффективное динамическое выделение ресурсов

Решение	Влияние на CapEx	Влияние на OpEx
<ul style="list-style-type: none"> <li>Решение Cisco UCS является решением, которое позволяет манипулировать конфигурацией каждого аспекта любого из серверов с помощью серверных профилей</li> <li>По требованию бизнеса, Cisco UCS менеджер может автоматически предоставить дополнительные ресурсы для поддержания уровня обслуживания</li> <li>Cisco Unified Fabric, встроенная в Cisco UCS расширяет возможности для удовлетворения изменяющихся условий бизнеса и характеристик инфраструктуры (безопасность, пропускная способность и латентность) без необходимости демонтажа.</li> </ul>	<ul style="list-style-type: none"> <li>Использование сервисных профилей и технологий единовременной кроссировки для автоматизации выделения и изменений может сократить утилизацию ресурсов, влияющих на CapEx.</li> <li>Поскольку серверы автоматически присоединяются к ресурсным пулам, то эти серверы могут использоваться несколькими группами приложений.</li> </ul>	<ul style="list-style-type: none"> <li>Преимущества для бизнеса при реализации этих ресурсов и способности быстрой реакции на изменения.</li> </ul>

## Дополнительные преимущества

Решение	Кратковременные преимущества	Долговременные преимущества
<ul style="list-style-type: none"> <li>Реинвестирование сохраненных CapEx и OpEx расходов в дополнительную ИТ-инфраструктуру</li> </ul>	<ul style="list-style-type: none"> <li>Отслеживание немедленного влияния на бизнес дополнительной инфраструктуры и приложений.</li> </ul>	<ul style="list-style-type: none"> <li>Долгосрочные перспективы наличия лучшей инфраструктуры в короткие сроки</li> </ul>
<ul style="list-style-type: none"> <li>Преимущества сниженных OpEx расходов на энергопотребление, охлаждение и уменьшение занимаемого стойко-места</li> </ul>	<ul style="list-style-type: none"> <li>Достижение цели экологичности</li> <li>Возможность отложить увеличение затрат на информационные технологии</li> </ul>	
<ul style="list-style-type: none"> <li>Процент ИТ ресурсов инвестируемых в инновационные технологии вместо поддержки существующих</li> </ul>	<ul style="list-style-type: none"> <li>Возможность запуска новых проектов</li> </ul>	<ul style="list-style-type: none"> <li>Чем больше ваши сотрудники работают с инновационными продуктами и системами, тем сильнее снижается текучесть кадров</li> </ul>
<ul style="list-style-type: none"> <li>Дополнительные внутренние инициативы</li> </ul>	<ul style="list-style-type: none"> <li>Повышение производительности труда</li> </ul>	<ul style="list-style-type: none"> <li>Влияние инновационных подходов</li> </ul>
<ul style="list-style-type: none"> <li>Дополнительные (внешние) инициативы</li> </ul>	<ul style="list-style-type: none"> <li>Увеличение удовлетворенности клиентов</li> <li>Возможность предоставления новых сервисов с требуемым качеством сервиса</li> </ul>	<ul style="list-style-type: none"> <li>Конкурентные преимущества</li> <li>Повышение лояльности клиентов</li> <li>Увеличение доли рынка</li> <li>Долговременное воздействие на доходы и рентабельность</li> </ul>

## Предлагаемые услуги

### Создание корпоративного облака

Отлаженные производственные процессы позволяют быстро реализовать все этапы создания корпоративного облака: сбор и анализ входных данных, постановка задачи, эскизное проектирование, планирование, проектирование и разработка, закупка и поставка оборудования и лицензий, внедрение, пусконаладочные работы и тестовая эксплуатация, корректировка по результатам тестирования.

### Перенос существующих данных и сервисов в корпоративное облако

Наш опыт переноса сервисов, серверов и приложений сократит время продуктивного запуска корпоративного облака.

### Развертывание типовых офисов и филиалов

Подготовка инфраструктурных шаблонов для быстрого развертывания типовых офисов и филиалов с доставкой в них необходимых корпоративных сервисов.

## Поддержка решения

### Зона ответственности Клиента

#### Бизнес-приложения

- Операционные системы.
- Базы данных.
- Бизнес-приложения.

### Зона ответственности Исполнителя

#### Виртуализация

- Виртуализация серверов и рабочих станций.

#### Безопасность инфраструктуры

- Межсетевое экранирование и сегментирование сетей.
- Защита каналов связи.
- Безопасный удаленный доступ с двухфакторной аутентификацией.
- Системы сенсоров обнаружения и предотвращения вторжений.
- Системы балансировки нагрузки.
- Система обеспечения безопасности при работе в сети Интернет.
- Интегрированные функции безопасности.

#### Сети

- Локальная вычислительная сеть корпоративного облака.
- Сеть хранения данных.
- Корпоративная сеть.

#### Вычисления

- Система унифицированных вычислений.

#### Системы хранения данных

- Распределенное хранилище данных.

## Business Ecosystems

Компания Business Ecosystems специализируется на оказании услуг системной интеграции, разработке систем автоматизации и обучении специалистов в области информационных технологий.

### Направления деятельности

- Системная интеграция по направлениям: информационная безопасность, вычислительные сети, центры обработки данных и виртуализация.
- Разработка систем автоматизации.
- Оказание услуг в области информационных технологий: аудит, техническая поддержка, аутсорсинг, консалтинг.
- Обучение ИТ-специалистов.

### Профиль специалистов

- Кандидаты технических и физ.-мат. наук;
- CCIE: R&S, Security, Data Center, Voice, Service Provider; CISSP; CISA; JUNCIP; HCDA;
- Oracle Certified Professional; MCSE; LPIC;
- 15 лет – средний опыт работы в сфере ИТ;
- 5 лет – опыт поддержки разработанных решений.

**Тел.:** 8 800 555 93 36

**Факс:** 8 800 555 93 36

**E-Mail:** info@becsys.ru

**Сайт:** www.becsys.ru