# Трансформация предприятия благодаря защищенным мобильным решениям

Сотрудники, которые могут безопасно работать из любого места, помогают Cisco увеличивать прибыль, повышать производительность и обслуживать заказчиков на еще более высоком уровне.

**Реализация компанией Cisco мобильных решений для своих сотрудников**

Благодаря защищенным мобильным решениям компания Cisco совершенно преобразилась. Если еще десять лет тому назад сотрудники Cisco работали в офисах, на своих рабочих местах, как правило в одном и том же здании на одном этаже со своим менеджером и остальными членами команды, то сегодня они абсолютно мобильны и могут работать в составе международных, территориально распределенных рабочих групп.

Так. например:

- В Cisco работают более 70 000 удаленных сотрудников или «работников с продленным рабочим днем»
- Более 70 % сотрудников работают из дома не менее одного дня в неделю, а более 25 000 сотрудников работают на дому три дня в неделю
- 63 % менеджеров руководят одним или несколькими сотрудниками удаленно
- 40 % сотрудников Cisco работают в разных городах со своим менеджером
- 28 % сотрудников Cisco работают в распределенных рабочих группах, а 23 % работают в дороге

Сотрудники стали мобильными благодаря тому, что мы поддерживаем каждого из них с помощью технологий и политик, которые обеспечивают им гибкость в работе с точки зрения времени, места и используемого устройства. Мы предлагаем эту возможность с помощью продуктов Cisco для защищенного беспроводного LAN (WLAN), домашнего и удаленного доступа (решение Cisco Virtual Office и VPN), а также программных телефонов, Cisco® WebEx®, Cisco Spark™ и возможностей мобильного использования добавочных внутренних номеров. Наши политики и программа «принеси свое устройство» (BYOD) позволяют сотрудникам использовать свои личные мобильные устройства для доступа к сети Cisco после регистрации такого устройства и подтверждения, что оно соответствуют нашим требованиям безопасности для того, чтобы сделать его защищенным или доверенным устройством.

Приведенная ниже статистика показывает объем развертываний защищенных мобильных решений, выполненный ИТ-отделом Cisco (по данным на конец 2015 года):

- Корпоративная беспроводная сеть (WLAN) насчитывает около 10 400 точек доступа в зданиях в разных странах мира, которые мы переводим на точки доступа Cisco Aironet® серии 3700.
- Доступ к такой сети WLAN осуществляется более с чем 135 000 корпоративных ноутбуков, большинство из которых работает под управлением Microsoft Windows, однако мы также поддерживаем компьютеры Apple Macintosh и некоторое число ПК под управлением Linux. Такое повсеместное беспроводное подключение позволяет сотрудникам Cisco свободно перемещаться в пределах офиса и сохранять широкополосное высококачественное подключение к сети Cisco.

- Возможность мобильного использования добавочных внутренних номеров на почти всех 129 000 аппаратных телефонах в офисах Cisco позволяет сотрудникам регистрироваться в любом офисном телефоне Cisco в мире и делать его своим собственным.
- Cisco Jabber® для программных телефонов, мгновенный обмен сообщениями и функция определения присутствия для всех 135 000 ноутбуков (ПК и Mac), а также для большинства из 70 000 мобильных телефонов и планшетов, принадлежащих и используемых сотрудниками Cisco, позволяет им использовать голосовые и видео подключения, когда они находятся вдали от видеотелефона или офисного устройства TelePresence™.
- Клиент Cisco AnyConnect® VPN на тех же 135 000 ноутбуках и около 30 000 доверенных мобильных устройствах BYOD дает возможность сотрудникам безопасно подключаться к сети Cisco из любого места с подключением к Интернету через проводное, беспроводное или 3G/4G соединение.
- Благодаря аппаратным VPN-маршрутизаторам с решением Cisco Virtual Office в более чем 29 000 домашних офисах отдельные сотрудники могут работать из дома по своему желанию. Таким образом, они могут сами регулировать время работы, что обеспечивает более гибкий баланс между работой и личной жизнью, а также упрощает проведение совещаний с сотрудниками в разных часовых поясах. Это решение также способствует отказу от поездок и уменьшению углеродных выбросов.
- В рамках нашей программы BYOD сотрудниками было зарегистрировано около 70 000 мобильных устройств, при этом почти половина сотрудников регистрировали несколько устройств. Почти 60 % устройств BYOD — это Apple iPhone, на втором месте — устройства Android и Apple iPad и замыкают список смартфоны под управлением Windows и Blackberry.

**КРАТКО О ПРЕИМУЩЕСТВАХ**

**ПРЕДПРИЯТИЕ**
- Экономии средств
- Новые доходы и ускоренные циклы продаж
- Улучшение обслуживания заказчиков
- Увеличение производительности
- Непрерывность бизнеса
- Уменьшение выбросов парниковых газов

**СОТРУДНИКИ**
- Гибкость в работе
- Глобальная командная работа
- Повышение уровня удовлетворенности

Компания Cisco получила многочисленные преимущества в бизнесе благодаря решениям защищенной мобильности, начиная с нашего первого внедрения WLAN в 2000 году, благодаря VPN-подключениям, а также перепланированному офисному пространству и политикам BYOD в последние годы. В этой статье основное внимание уделяется рассмотрению полученных преимуществ, а также подробно описывается, что мы внедрили на нашем пути к мобильности.

В основе всех полученных преимуществ лежит безопасность. В прошлом сотрудники корпорации работали в одном месте, и их безопасность обеспечивалась закрытыми дверями. Они выполняли свою работу с использование проводной частной сети предприятия, которая защищалась различными барьерами от Интернета и всего внешнего мира. Безопасность означала охрану стен между «внутренним» и «внешним».

В современной мобильной среде эти границы исчезли. Работа перестала быть местом, куда ты приходишь. Это действие, которое может происходить в офисе, дома или на объекте заказчика, в кафе, гостиничном номере или аэропорту. Такая новая мобильная среда обладает многочисленными преимуществами. Однако без новых способов обеспечения ее защиты ни одно из предприятий не могло бы позволить себе пренебрегать рисками безопасности гибких рабочих мест. Безопасность — это скрытая движущая сила новой мобильной культуры.

## Какие преимущества получает Cisco от защищенных мобильных решений

Как и для многих предприятий в информационной экономике, подключение к нашей корпоративной сети абсолютно необходимо, чтобы сотрудники Cisco могли выполнять свою работу. Обеспечивая безопасные беспроводные подключения к сети как внутри, так вне офиса, компания Cisco получила преимущества для коммерческой деятельности предприятия и наших сотрудников.

**Экономия затрат.** Благодаря предложению большего количества вариантов мобильных решений нашим сотрудникам нам удалось снизить затраты на офисное оборудование, устройства и тарифные планы.

Например, гибкая планировка офисов в виде открытого пространства, ставшая возможной благодаря мобильности сотрудников, которая называется подключенным рабочим местом Cisco, дает возможность сотрудникам выбирать, как и где они будут работать, находясь в офисе Cisco. При таком подходе учитывается, что многие наши сотрудники проводят большую часть времени, работая из дома, на объекте заказчика или в командировках, и им не нужно строго определенное рабочее место в здании Cisco на полный рабочий день. Поэтому в отдельных офисах Cisco в разных странах мира сотрудники могут работать в любом месте открытого рабочего пространства — за отдельным столом, в зоне для групповой совместной работы или в обычной переговорной.

В начале 2014 года приблизительно четверть сотрудников Cisco работала в среде подключенного рабочего пространства Cisco, обеспечивая ежегодную экономию порядка 51 млн долларов США за счет снижения расходов на аренду недвижимости, строительство зданий, обслуживание оборудования и коммунальные услуги, мебель, прокладку кабелей и площади для размещения оборудования.

Мы разработали программу BYOD в ответ на желание сотрудников использовать свои личные смартфоны и цифровые планшеты для коммуникаций и выполнения задач по работе. Они больше не хотели носить с собой отдельный выданный компанией телефон для использования в рабочих целях. Наши сотрудники остались довольны внедрением программы BYOD, которая обеспечила ежегодную экономию в размере 1,35 млн долларов, поскольку Cisco больше не платит за такое большое количество корпоративных устройств и тарифных планов. Онлайн-ресурсы поддержки для программы BYOD также обеспечивают экономию за счет снижения числа обращений в службу поддержки, связанных с мобильными решениями, на 33 %.

Однако у программы BYOD есть свои собственные риски безопасности. Например, что делать, чтобы злоумышленники не смогли загрузить корпоративные данные с потерянного или украденного телефона сотрудника? Или, как сделать так, чтобы они не могли использовать такое устройство для доступа к сети предприятия с целью получить еще более конфиденциальные данные? ИТ-отдел Cisco устраняет такие риски, требуя наличия определенных функций безопасности в устройстве, включая блокировки с помощью пароля и удаленную очистку. Мы называем это моделью доверенного устройства.

**Новые доходы и ускоренные циклы продаж.** Сотрудники отдела продаж Cisco проводят много времени вне офиса; их пример наглядно показывает, насколько эффективнее они работают благодаря защищенным мобильным решениям. Что примечательно, это то, насколько сильно мобильность влияет на получаемые доходы. Наша внутренняя разработка, приложение SalesMobile, позволяет быстро обрабатывать доходы Cisco в среднем в размере от 1,5 до 2 млрд долл. США ежеквартально. Еще один значительный результат: утверждение нестандартных сделок по продажам ускорилось на 40 %, помогая нам быстрее получать эти доходы. В дополнение к планшетам и смартфонам приложение SalesMobile доступно для отдельных носимых устройств, таких как часы Apple.

Cisco Sales Connect — еще одно приложение, популярное среди сотрудников отдела продаж, которые используют его для простого поиска соответствующих актуальных брошюр по решениям и связанного с ними контента, экономя порядка 15 минут в сравнении с обычным поиском. Это приложение также используется многими торговыми партнерами Cisco в разных точках мира.

Защищенные мобильные решения значительно повышают возможности продаж Cisco, а также производительность и эффективность работы отделов продаж. «Это действительно большое преимущество, когда можно потратить 30 минут и получить одобрение сделки на этой неделе, в этом месяце или квартале, и для этого всего лишь нужно сделать один звонок во внерабочее время, — говорит Стив Бингхэм (Steve Bingham), отраслевой директор по глобальным корпоративным продажам, — Если бы не возможность делать звонки в удобное время, мы бы не смогли действовать так быстро из-за разницы в часовых поясах».

Используя разработанные Cisco мобильные приложения, Бингхэм может просматривать информационные панели с данными о текущих продажах, а также обрабатывать утверждения для сделок и стандартные запросы. Он также использует облачные приложения Cisco Jabber и Cisco Collaboration Meeting Rooms

(CMR) для звонков со своего мобильного устройства для совместной работы со своей командой торговых представителей вне зависимости от того, где находятся сотрудники в этот момент.

«Я с нетерпением жду появления мобильных приложений, которые позволят нам обрабатывать еще больше задач, связанных с продажами, когда мы находимся вне офиса», — говорит Бингхэм.

**Улучшение обслуживания заказчиков и повышение оперативности.** Мобильность позволяет специалистам по продажам Cisco оперативно отвечать на текстовые сообщения или телефонные звонки заказчиков. ИТ-отдел Cisco разработал специализированные мобильные приложения, которые дают возможность торговым представителям проверять состояние заказа клиента или обращения в службу поддержки с помощью всего нескольких щелчков.

Мобильные приложения также играют жизненно важную роль при мониторинге и управлении нашими производственными операциями, которые выполняются сторонними производителями. Например, приложения направляют оповещения менеджерам цепочки поставок Cisco и руководителям компании в случаях, когда проблемы на производстве могут привести к задержке поставки продуктов.

«Мы обнаружили, что смартфоны используются больше, чем ноутбуки, и разрабатываем наши приложения, чтобы использовать преимущества этого интерфейса, — говорит Мукунда Йоши (Mukunda Joshi), технический руководитель группы цепочки поставок в ИТ-отделе Cisco, — Критически важные оповещения немедленно появляются на главном экране устройства, а после того, как сотрудник щелкнет по оповещению, оно автоматически открывает приложение и показывает соответствующую ситуацию, чтобы можно было сразу предпринять необходимые действия».

**Рост производительности благодаря мобильности.** Сотрудники выполняют больше задач, когда им удобно работать. Например:

- Сотрудники Cisco, работающие удаленно, получают в свое распоряжение время, которое они обычно затрачивают на поездки в офис. В среднем это более полутора часов ежедневно. Примерно половина приобретенного таким образом времени возвращается компании. Если им не приходится проводить 95 минут в дороге, то 45 минут они дополнительно затрачивают на работу.
- Сотрудники, которые помнят, как они были буквально «привязаны» к своим рабочим столам без беспроводной связи, говорят, что им удается увеличить время своей производительности на 45 минут каждый рабочий день. А это, по оценкам, обеспечивает рост производительности в размере приблизительно 280 млн долларов США в год.
- Согласно отчетам по рабочему времени сотрудников Cisco, использование мобильных устройств дает им дополнительно 15 минут рабочего времени каждый день, а это означает 300 млн долларов США для компании ежегодно.
- В дополнение к этому многие из 80 мобильных приложений в нашем внутреннем магазине Cisco eStore предназначены для того, чтобы помочь сотрудникам работать более производительно. Магазин eStore представляет собой комплексный каталог сервисов, в который включены все имеющиеся ИТ-сервисы. Он создан с использованием каталога сервисов Cisco Prime Service Catalog и оркестратора процессов Cisco Process Orchestrator. Доступ к магазину предоставляется с устройств всех типов через веб-браузер или мобильное приложение. Магазин интегрирован с решением управления корпоративными сервисами Enterprise Service Management для автоматизации подготовки сервисов для различных систем. Магазин Cisco eStore обеспечивает простое взаимодействие с пользователями и ускоряет их обслуживание.

В таблице 1 приведены разработанные Cisco или одобренные сторонние мобильные приложения, которые доступны для сотрудников и могут быть загружены из нашего внутреннего магазина eStore.

**Таблица 1.** Примеры мобильных приложений, используемых сотрудниками Cisco

| Сценарии применения решений обеспечения мобильности Cisco | Примеры мобильных приложений |
|---|---|
| **Производительность труда** | Карты офисов Cisco, каталог сотрудников, информация о мероприятиях Cisco, планирование поездок и отчеты о расходах, обработка утверждений, а также доступ к облачному хранилищу файлов |
| **Совместная работа** | Cisco Jabber, Cisco Spark, Cisco WebEx® meetings, сайты внутренней социальной сети |
| **Отдел продаж** | Отчеты о продажах, ценовые предложения и заказы, демонстрация приложений для продуктов Cisco |
| **Отдел кадров** | Информация о сотрудниках, отслеживание и отправка запросов на выходные дни |
| **Удаленный доступ** | Защищенный мобильный клиент Cisco AnyConnect |
| **Система коммуникаций с передачей мультимедиа** | Cisco TV |
| **Инструментальные панели управления** | Ключевые финансовые и коммерческие аналитические данные; мониторинг качества цепочки поставок; эскалации поддержки заказчиков |
| **Техническая поддержка** | Инструменты управления для обращений в службу поддержки заказчиков |

**Удовлетворенность сотрудников.** Мы формируем необходимые для работы рабочие группы из сотрудников вне зависимости от того, где они живут. В результате многие наши рабочие группы имеют глобальный характер с необходимостью охвата нескольких часовых поясов для коммуникаций по проекту и совместной работы. Наши технологии обеспечения мобильности и политики позволяют таким рабочим группам быстрее выполнять свою работу, привлекать к принятию решений нужных людей. При этом нет никакой необходимости, чтобы кто-то был в офисе очень рано или поздно для участия в сеансе конференц-связи.

Уровень удовлетворенности сотрудников также повышается благодаря гибкому рабочему пространству. В опросе 2014 года наши мобильные сотрудники оценили свой уровень удовлетворенности на 10 базисных пунктов выше в сравнении с сотрудниками, которые работают в традиционных офисах. Кроме этого, здания с подключенным рабочим пространством Cisco сотрудники оценили выше, чем здания без гибких рабочих зон. «Возможность работать из любого места — одно из преимуществ, которое для меня делает компанию Cisco отличным местом для работы», — говорит Арун Йоши (Arun Joshi), директор, Cisco on Cisco

Возможность удаленной работы стала один из самых больших движущих факторов для повышения уровня удовлетворенности сотрудников, а также при приеме на работу новых сотрудников. Более 70 % сотрудников Cisco работают из дома не менее одного дня в неделю, а более 35 сотрудников работают на дому три дня в неделю. Такие удаленные сотрудники могут работать больше, получая при этом большую удовлетворенность от возможности гибко подходить к распределению свободного и рабочего времени по своему усмотрению.

**Больше вариантов для поддержки непрерывности бизнеса.** Все сотрудники Cisco имеют в своем распоряжении средства VPN, которые позволяют им безопасно работать из любого места, включая домашний офис, с использованием наилучшего доступа к Интернету. Благодаря такой гибкости в работе своих сотрудников мы можем использовать разные варианты для обеспечения непрерывности своего бизнеса.

Непрерывность бизнеса обыкновенно означает резервное копирование информации в центрах обработки данных или резервирование доступа к сети с целью подготовки к крупным сбоям в работе, таким как серьезное стихийное бедствие или эпидемия. Однако большинство случаев остановки деятельности связано с более мелкими причинами, такими как закрытие дорог в результате наводнения или снегопада или закрытие зданий из-за прорыва водопровода.

В тех случаях, когда сотрудники Cisco не могут работать в своих обычных офисах Cisco, они просто могут работать из любого другого удобного им места — из дома, здания другой компании или любого места с доступом в Интернет. Несколько раз в офисах Cisco отключалась электроэнергия, однако мы не заметили никакого снижения производительности. Если сотрудник Cisco заболел, он скорее всего будет работать из дома, ведь он знает, что ему совсем необязательно находиться в офисе, чтобы быть продуктивным.

**Глобальная совместная работа.** Возможность удаленной работы позволяет расширить глобальную совместную работу. Несмотря на то, что благодаря сетевым технологиям проблема расстояния была практически решена, проблема с часовыми поясами осталась. Работая из дома, сотрудники могут

общаться друг с другом в течение большего периода времени (например, рано утром или поздно вечером) без необходимости идти на работу и нарушать распорядок дня. Удаленная работа позволила каждому сотруднику Cisco работать с большим числом людей за счет охвата нескольких дополнительных часовых поясов.

«Когда я использую свой смартфон для работы, мой офис находится у меня в кармане, — говорит Арун Йоши, который руководит группой ИТ-консультантов, живущих в США, Великобритании, Австралии и Индии, — Так как все члены моей группы часто находятся в поездках, защищенные мобильные решения имеют особенно большое значение. Мы можем легко связываться друг с другом, особенно когда требуется обсудить срочные проблемы заказчиков».

**Уменьшение выбросов парниковых газов.** Сотрудники, отказавшиеся от поездок на работу, экономят время и снижают уровень выбросов парниковых газов компании Cisco. Наш обычный удаленный сотрудник Cisco ежедневно экономит порядка 95 минут, оставаясь дома. Часть этого времени сотрудники тратят на более полноценную личную жизнь, а другую часть посвящают работе, что создает, по оценкам, дополнительную производственную ценность в размере 277 млн долларов США, согласно исследованию Cisco, проведенному в 2008 году. Это же исследование показало, что за счет удаленной работы сотрудники Cisco предотвратили выброс 47 тонн парниковых газов и сами сэкономили более 10 млн долларов США в год от расходов на топливо.

**Как компания Cisco внедряла защищенные мобильные решения**

Начиная с 1999 года, мы создавали защищенную сетевую инфраструктуру для поддержки мобильности через WLAN, удаленный доступ и в рамках программы BYOD.

**Покрытие WLAN в большинстве объектов.** Сети WLAN в офисах и зданиях большинства объектов Cisco обеспечивают повсеместную возможность подключения для передачи данных и голосовой связи сотрудникам, беспроводной доступ к Интернету для гостей, а также возможность подключения для мобильных устройств (таблица 2). Вне зависимости от места нахождения, в комплексах зданий или на удаленных объектах, пользователи с беспроводными доступом имеют одинаковые возможности при подключении к сервисам передачи данных, видео и голосовой связи в сети Cisco.

**Таблица 2.** Решения Cisco, внедренные для беспроводного подключения к сети

| Беспроводные сетевые решения | Описание |
|---|---|
| **Точки доступа Cisco Aironet серии 3700** | Поддерживает устройства Wi-Fi, которые соответствуют спецификации 802.11ac с развертыванием в условиях высокой плотности |
| **Беспроводные контроллеры Cisco серии 8500** | Обеспечивают централизованный контроль, управление и устранение неполадок для сетей WLAN |
| **Устройство Cisco Mobility Services Engine с решением CMX (Connected Mobile Experiences)** | Cisco Mobility Services Engine (Cisco MSE) — это физическое или виртуальное устройство, которое использует сети Wi-Fi для получения более полной информации о сети, развертывания мобильных сервисов на основе местоположения и повышения уровня защиты. Пакет приложений Cisco Connected Mobile Experiences запускается в среде Cisco MSE для определения местоположения мобильных устройств и предоставления соответствующих, персонализированных сервисов их пользователям. |

**Улучшенная защита беспроводных сетей.** Сотрудники Cisco осознали ценность беспроводных мобильных решений гораздо раньше ИТ-отдела Cisco. Многие сотрудники настраивали точки доступа на базе «теневых ИТ» при первом появлении технологии WLAN, поскольку беспроводной доступ обеспечивал им свободу перемещения в офисе при сохранении производительности. Внутренние исследования Cisco показали, что после широкого распространения WLAN, сотрудники оставались подключенными к таким сетям почти на 90 минут больше каждый рабочий день.

Работники «добеспроводной» эры помнят совещания, когда никто не мог получить доступ к необходимым данным, чтобы продолжить обсуждение или проект. Доступность беспроводного подключения обеспечила значительное повышение производительности, когда сотрудники смогли оставаться подключенными в любом месте в здании Cisco. С развитием беспроводных протоколов и расширением полосы пропускания у сотрудников практически отпала необходимость подключать свои ноутбуки через проводной порт Ethernet даже во время работы в офисе Cisco.

Однако расширение традиционной проводной сети до беспроводной сети общего доступа подвергает большой объем трафика риску потенциального перехвата. Хорошая защита стала критически важным предварительным условием, которое позволило ИТ-отделу Cisco осуществить широкое внедрение сетей

WLAN в зданиях компании. ИТ-отдел Cisco принимал активное участие в работе органов стандартизации, которые разработали протоколы защиты беспроводной связи, в том числе Wired Equivalent Privacy (WEP, уровень конфиденциальности на уровне проводной связи), Wi-Fi Protected Access (WPA, защищенный доступ к сети Wi-Fi) и WPA2 Enterprise.

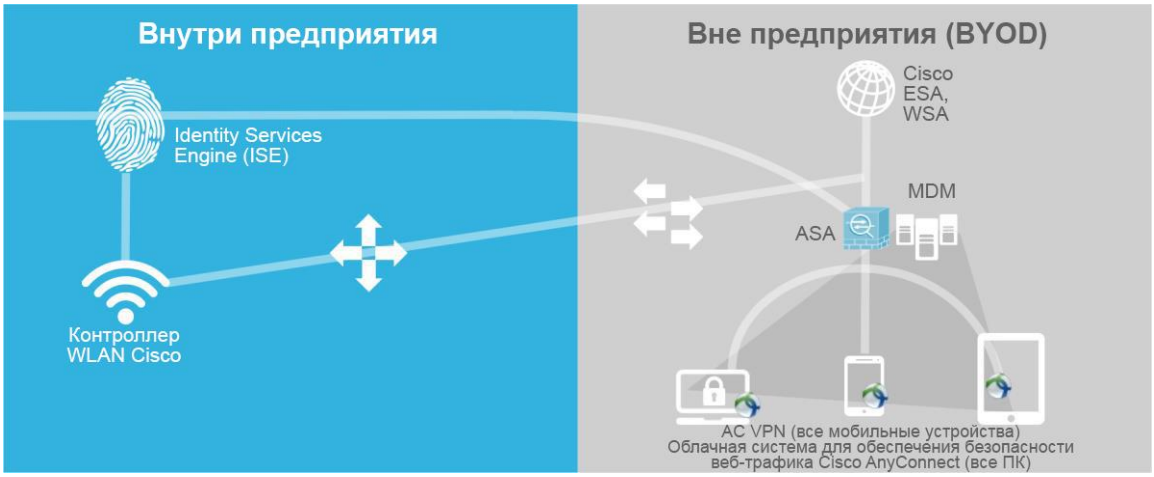
Обеспечивая широкое покрытие сетями WLAN, мы избежали рисков безопасности, которые возникают в случаях, когда сотрудники устанавливают неавторизованные точки доступа. Кроме этого, проверка подлинности и шифрование по протоколу WPA2 включены как составная часть во все развертывания беспроводных сетей, которые выполняет ИТ-отдел Cisco

**Защита удаленного доступа.** Удаленные сотрудники используют решение Cisco Virtual Office для подключения своих корпоративных ноутбуков, IP-телефона Cisco и, возможно, терминального устройства Cisco TelePresence®. Кроме этого, многие сотрудники часто работают из дома или других мест, используя свои мобильные устройства. Вне зависимости от их местоположения или используемого устройства таким сотрудникам необходим защищенный удаленный доступ к сети Cisco.

Для обеспечения удаленного доступа Cisco продолжает использовать такие функции, как двухфакторная аутентификация пользователей, туннели 2-го уровня протокола Secure Sockets Layer (SSL) и шифрование IP Security (IPsec) Internet Key Exchange (IKE) v2, а также межсетевой экран Cisco Adaptive Security Appliance (Cisco ASA) для защиты VPN-подключений.

На рисунке 1 показано, как инфраструктура безопасности, созданная ИТ-отделом Cisco, обеспечивает поддержку такого удаленного доступа для концепции «принеси на работу свое устройство» (BYOD).

**Рисунок 1.** Инфраструктура безопасности для удаленного и мобильного доступа




Одно из основных защитных средств — это обеспечение безопасности с учетом контекста с помощью решения Cisco Identity Services Engine (Cisco ISE). Учет контекста помогает оценить такие факторы как, где, когда и как выполняется попытка доступа, а также традиционные факторы, указывающие на то, кем представляются пользователи и что они пытаются сделать. Оценивая все эти контекстные факторы, решение Cisco ISE способно обнаружить потенциально мошенническую попытку входа или ограничить уровень и тип доступа пользователя, например в случае, если сотрудник использует общедоступную сеть Wi-Fi вместо безопасной VPN.

В таблице 3 перечислены дополнительные решения Cisco, которые используются для обеспечения защиты удаленного доступа.

**Таблица 3.** Решения Cisco, внедренные для обеспечения защиты удаленного доступа

| Решения для защиты удаленного доступа | Описание |
|---|---|
| **Cisco Cisco ISE** | Применяет наши требования безопасности на основе пользователя, устройства и контекста доступа, а также обеспечивает соответствие мобильного устройства корпоративной политике. |
| **Технология Cisco TrustSec®** | Использует программно-определяемую сегментацию для упрощения подготовки доступа к сети, ускорения операций обеспечения безопасности и согласованного применения политики в любом месте сети. |
| **Cisco ASA** | Выполняет аутентификацию пользователей и шифрует поток мобильных данных для того, чтобы их нельзя было прочитать в случае перехвата. |
| **Устройство защиты электронной почты Cisco Email Security Appliance (ESA)** | Сканирует все сообщения электронной почты, поступающие от источников вне Cisco, блокирует известный спам и осуществляет поиск на наличие подозрительного содержимого или иных нарушений в электронной почте. |
| **Устройство обеспечения безопасности веб-трафика Cisco Web Security Appliance (Cisco WSA)** | Сканирует все запросы на доступ к внешним веб-сайтам, поступающие от устройства, которое имеет установленный защищенный мобильный клиент Cisco AnyConnect Secure Mobility Client и подключено через шлюзы веб-безопасности ИТ-отдела Cisco. В соответствии с внутренней политикой безопасности Cisco устройство Cisco WSA может блокировать доступ (или осуществлять мониторинг доступа) к целым веб-сайтам или к конкретным функциям, таким как чат, обмен сообщениями, видео и аудио. |
| **Виртуальный офис Cisco Virtual Office** | Предоставляет защищенный, универсальный и управляемый IP-телефон, сервисы беспроводной связи, передачи данных и голоса удаленным сотрудникам через зашифрованные сети VPN, обеспечивая пользователям прозрачный интерфейс офисного уровня. |
| **Клиенты Cisco AnyConnect** | Обеспечивают надежное, зашифрованное и устойчивое подключение к корпоративной сети с ноутбуков, смартфонов и планшетов. Работают совместно с системой управления мобильными устройствами (MDM). |

**Безопасность BYOD.** Наша программа BYOD использует существующую архитектуру безопасности для удаленного доступа, но добавляет средства защиты, ориентированные на устройства.

Большая проблема любой программы BYOD связана с определением, к какой информации и приложениям может иметь доступ мобильное устройство при подключении к корпоративной сети. Мы решаем эту проблему, определяя категорию «защищенное» или «доверенное» для конкретных устройств.

Защищенные устройства должны поддерживать 10-минутное ожидание блокировки с помощью ПИН-кода, ПИН-код из 6 цифр и возможность удаленной очистки устройства для ИТ-отдела Cisco. Устройство без указанных настроек просто не может подключиться к нашей сети.

Доверенные устройства отвечают всем указанным выше требованиям и дополнительно поддерживают собственные средства шифрования контента операционной системы, а также удаленное управление ИТ-отделом Cisco. Шифрование играет важную роль, поскольку оно позволяет пользователям получать доступ к конфиденциальной информации из основной сети Cisco и сохранять ее. В дополнение к этому ИТ-отдел Cisco использует сторонние приложения MDM для проверки, что устройство зарегистрировано и соответствует корпоративным требованиям состояния безопасности.

На рисунке 2 показано, как различия между доверенными и защищенными устройствами позволяют определять, к каким приложениям и сетевым зонам пользователь может иметь доступ.

**Рисунок 2.** Сравнение доступа к приложениям для защищенных и доверенных устройств

Защищенные устройства могут получать доступ к электронной почте, календарям, контактам, конференциям Cisco WebEx, Cisco Spark и Cisco Jabber. Доверенные же устройства помимо этих базовых сервисов могут также получать доступ к приложениям и информации внутри основной сети Cisco, включая конфиденциальные корпоративные данные.

Чтобы подключиться к Интранет, сотрудникам необходимо загрузить на свои устройства защищенный мобильный клиент Cisco AnyConnect Secure Mobility Client, который доступен в магазине Cisco eStore. Cisco AnyConnect обеспечивает сотрудников защищенным доступом к корпоративным ресурсам и критически важным для бизнеса приложениям для того, чтобы они могли работать из любого места вне зависимости от использования корпоративного ноутбука или личного мобильного устройства. Клиент Cisco AnyConnect запускается за 1–2 секунды без необходимости выполнять вход со стороны пользователя.
Эта возможность позволяет сделать пользовательский интерфейс таким же простым и согласованным, каким бы он был без VPN-подключения.

### Реализация защищенных мобильных решений на вашем предприятии

Отделы ИТ и информационной безопасности всегда старались создать компаниям условия для выполнения большего количества задач при одновременном ограничении рисков, связанных с новыми возможностями. Сегодня технологии безопасности достигли такого уровня, при котором компании могут быть уверены в возможности предоставления мобильности большему числу сотрудников и бизнес-подразделений. Чтобы помочь заказчикам при планировании своих развертываний, мы предлагаем руководства и проверенные типовые проекты Cisco Validated Designs для реализации многих аспектов программы защищенной мобильности.

Cisco реализовывала мобильные возможности для сотрудников постепенно, шаг за шагом. Причем в основе всех этих шагов было стремление обеспечить комплексную безопасность сети. Наши заказчики могут следовать аналогичным путем для создания сред мобильной работы для своих сотрудников и использовать преимущества, связанные с преобразованием бизнеса, на этом пути.

## Дополнительная информация

Методы ИТ-отдела Cisco Проектирование защищенной архитектуры BYOD ИТ-отделом Cisco

Методы ИТ-отдела Cisco Развертывание и управление BYOD ИТ-отделом Cisco

Решения безопасности Cisco: www.cisco.com/go/security

Решения обеспечения мобильности Cisco: www.cisco.com/go/mobility

Решения удаленного доступа Cisco: www. cisco.com/go/vpn

Проверенные типовые проекты Cisco Validated Designs: краткие сведения о проектах LAN и беспроводной LAN в комплексах зданий

Руководство по разработке удаленного доступа с использованием технологии VPN

Руководство по разработке BYOD

Для доступа к дополнительным статьям ИТ-отдела Cisco IT и сценариям применения различных бизнес-решений посетите веб-сайт Cisco on Cisco: Сведения об ИТ-отделе Cisco www.cisco.com/go/ciscoit.

## Примечание

В этой публикации описываются преимущества, полученные компанией Cisco в результате развертывания своих собственных продуктов. На описанные результаты и полученные преимущества могут оказывать влияние различные факторы. Cisco не гарантирует получение сравнимых результатов в других местах.

КОМПАНИЯ CISCO ПРЕДОСТАВЛЯЕТ ДАННУЮ ПУБЛИКАЦИЮ БЕЗ КАКИХ-ЛИБО ГАРАНТИЙ, КАК ПРЯМЫХ, ТАК И КОСВЕННЫХ, ВКЛЮЧАЯ КОСВЕННЫЕ ГАРАНТИИ КОММЕРЧЕСКОЙ ЦЕННОСТИ И ПРИГОДНОСТИ ДЛЯ КОНКРЕТНЫХ ЦЕЛЕЙ.

Если действующее законодательство не допускает исключения оговоренных или подразумеваемых гарантий, то упомянутое выше исключение может к вам не относиться.


Россия, 121614, Москва,
ул. Крылатская, д.17, к.4 (Krylatsky Hills)
Телефон: +7 (495) 961 1410, факс: +7 (495) 961 1469
www.cisco.ru, www.cisco.com

Россия, 197198, Санкт-Петербург,
бизнес-центр «Арена Холл»,
пр. Добролюбова, д. 16, лит. А, корп. 2
Телефон: +7 (812) 313 6230, факс: +7 (812) 313 6280
www.cisco.ru, www.cisco.com

Украина, 03038, Киев,
бизнес-центр «Горизонт Парк»,
ул. Николая Гринченко, 4В
Телефон: +38 (044) 391 3600, факс: +38 (044) 391 3601
www.cisco.ua, www.cisco.com

Беларусь, 220034, Минск,
бизнес-центр «Виктория Плаза»,
ул. Платонова, д. 1Б, 3 п., 2 этаж.
Телефон: +375 (17) 269 1691, факс: +375 (17) 269 1699
www.cisco.ru, www.cisco.com

Казахстан, 050059, Алматы, бизнес-центр «Самал Тауэрс», ул. О. Жолдасбекова, 97, блок А2, 14 этаж
Телефон: +7 (727) 244 2101, факс: +7 (727) 244 2102

Азербайджан, AZ1010, Баку,
ул. Низами, 90А, «Лэндмарк» здание III, 3 этаж
Телефон: +994 (12) 437 4820, факс: +994 (12) 437 4821

Узбекистан, 100000, Ташкент,
бизнес центр INCONEL, ул. Пушкина, 75, офис 605
Телефон: +998 (71) 140 4460, факс: +998 (71) 140 4465