

## Почему именно Cisco – лучший выбор в качестве партнера по информационной безопасности?

Выбор бизнес-партнера в области информационной безопасности основывается не только на типе и номенклатуре выпускаемых производителем средств защиты. Выбор должен учитывать множество аспектов – начиная от выполнения требований ФСТЭК и ФСБ в части оценки соответствия требованиям по безопасности и наличия программ обучения и сертификации специалистов и заканчивая наличием собственного исследовательского подразделения и возможностью финансирования проектов по информационной безопасности.

С целью облегчения такого выбора, мы сформулировали ряд критериев, демонстрирующих преимущества компании Cisco, как надежного в долгосрочной перспективе бизнес-партнера по широкому спектру вопросов информационной безопасности.

### 1. Cisco – мировой лидер в области информационной безопасности

Качество решений Cisco подтверждено не только внутренними процедурами, но и внешними наградами и оценками аналитиков — Synergy, Infonetics, Gartner, Forrester и т.п. Например, согласно исследованиям компаниям Synergy и Infonetics компания Cisco последние несколько лет занимает 1-е место на рынке сетевой безопасности, удерживая долю от 35% до 42%, что почти в три раза превышает показатели ближайшего конкурента (при положительном квартальном и годовом росте).

В сегменте защищенных маршрутизаторов доля компании Cisco составляет 70.8% (опережение ближайшего конкурента в 3.5 раза). Компания Cisco также является лидером в сегменте сетевых средств обнаружения и предотвращения вторжений (IDS/IPS), а также в сегменте устройств безопасности контента. В обоих случаях компании Cisco принадлежит свыше четверти всего мирового рынка этих средств защиты.

*Отличие от других производителей:* Доли компаний Juniper и Check Point на мировой рынке средств сетевой безопасности почти в три раза уступают компании Cisco, а доли Symantec, McAfee, Fortinet уступают чуть ли не в 10 раз. Компания StoneSoft вообще не числится среди мировых игроков рынка сетевой безопасности.

### 2. Обширное портфолио решений по информационной безопасности

Концепция Cisco Self-Defending Network, а за ней и Cisco Secure Borderless Network явилась отправной точкой для разработки нескольких десятков средств защиты (<http://www.cisco.com/go/security>), которые стали результатом работы как собственных подразделений компании Cisco, ориентированных на исследования и разработку в области информационной безопасности, так и грамотной политики поглощений и слияний, которая позволила за последние полтора десятилетия усилить портфолио компании лучшими в отрасли решениями по защите информационных активов и управлению ими на всех уровнях ИТ-инфраструктуры – от сетевого уровня до уровня приложений; от программных и аппаратных средств до технологий облачной безопасности.

Принципы, заложенные в стратегию Cisco в области информационной безопасности, говорят о том, что мы имеем возможность, как интегрироваться в уже существующую инфраструктуру, так и

поддерживать новые решения экосистемных партнеров Cisco. С этой целью компания Cisco поддерживает партнерские отношения с более чем 350 производителями средств защиты информации, среди которых можно упомянуть IBM ISS, Microsoft, HP, Intel, EMC RSA, ArcSight, netForensics, Check Point, Лаборатория Касперского, C-Terra CSP, Dr.Web, Sophos, Trend Micro, ESET, Aladdin, Positive Technologies, Infowatch и т.д.

*Отличие от других производителей:* Большинство других производителей средств защиты являются нишевыми игроками, предлагающими один-два продукта в области информационной безопасности и не имеют развитой системы партнерства в области совместных решений. Это может привести к невозможности или определенным сложностям с интеграцией разнородных средств защиты в единую и целостную систему.

### 3. Тесная интеграция с инфраструктурой Cisco

Тенденции последних лет убедительно показывают, что мало выпустить систему безопасности – она должна быть очень тесно связана с защищаемыми технологическими и ИТ-процессами. А это значит, что каким бы хорошим не был «навесной» продукт в области защиты информации, он остается не более чем придатком к основной информационной системе предприятия. Он не учитывает сложившуюся практику использования информационных технологий, не «понимает» уже реализованных процессов и даже не всегда корректно работает с ранее внедренными ИТ-решениями.

Это приводит к необходимости интеграции защитных механизмов в инфраструктуру корпоративной сети или сети оператора связи. Как только межсетевой экран, система предотвращения атак, модули построения VPN становятся неотъемлемой частью сети, их эффективность возрастает на порядок; не говоря уже о снижении совокупной стоимости владения таким целостным решением.

Именно поэтому компания Cisco уделяет такое большое внимание интеграции своих защитных технологий в весь спектр своего оборудования и программных решений. Любой наш коммутатор или маршрутизатор, IP-телефон или точка беспроводного доступа содержат большое количество встроенных механизмов защиты. Достаточно только посмотреть на маршрутизаторы Cisco Integrated Service Router (Cisco ISR G2), Cisco Wireless LAN Controller и т.п. Заказчики, сделавшие выбор в пользу нашего оборудования, сделали хорошие инвестиции и в свою информационную безопасность. Им не приходится заниматься внедрением и интеграцией «навесных» средств защиты в уже работающую инфраструктуру – им достаточно просто настроить уже существующие в сетевом оборудовании механизмы защиты и не бояться, что принятая технология обработки информации будет нарушена.

*Отличие от других производителей:* Большинство других производителей средств защиты предлагают только «навесные» продукты, которые никак не учитывают используемую ИТ-инфраструктуру организации. Создание такой второй инфраструктуры безопасности приводит как к проблемам с интеграцией с существующими процессами и технологиями, так и к удорожанию итоговой стоимости (в т.ч. и совокупной стоимости владения) системы обеспечения информационной безопасности.

### 4. Архитектурный подход

Сетевая инфраструктура является основой для предоставления различных сервисов и обеспечения жизнедеятельности многих процессов предприятия. Ее защита является важной составляющей

архитектуры ИБ. На основе опыта работы с десятками тысяч клиентов компания Cisco разработала архитектуру защищенной сети предприятия (Security Architecture for Enterprise, SAFE), главная цель которой состоит в том, чтобы предоставить заинтересованным сторонам информацию о современном опыте проектирования и развертывания безопасных сетей, не мешающих росту бизнеса, а способствующих ему. Исходя из принципа глубокоэшелонированной обороны сетей от внешних и внутренних атак, архитектура SAFE (<http://www.cisco.com/go/safe>) призвана помочь тем, кто проектирует сети и анализирует требования к сетевой безопасности. Данный подход нацелен не на механическую установку межсетевых экранов или системы обнаружения атак, а на анализ ожидаемых угроз и разработку различных методов борьбы с ними. Эта стратегия приводит к созданию многоуровневой и модульной системы защиты, при которой прорыв одного уровня не означает прорыва всей системы безопасности.

Архитектура Cisco SAFE с максимальной точностью учитывает как текущие, так и будущие функциональные потребности современных корпоративных сетей и решает следующие задачи (в порядке приоритетности):

- Обеспечение безопасности и противодействие атакам на основе политик.
- Внедрение мер безопасности по всей сетевой инфраструктуре (а не только на специализированных устройствах защиты), включающей маршрутизаторы, коммутаторы, точки беспроводного доступа, IP-телефоны, системы хранения и т.п.
- Безопасные средства управления и формирования отчетов.
- Аутентификация и авторизация пользователей и администраторов для доступа к критически важным сетевым ресурсам.
- Обнаружение атак на критически важные сетевые ресурсы и подсети.
- Поддержка новых приложений и сервисов.

К основным достоинствам архитектуры Cisco SAFE можно отнести следующие ее особенности:

- Обеспечение основы для построения безопасных, высокодоступных и интегрированных сетей.
- Открытая, модульная, расширяемая и масштабируемая структура.
- Упрощение разработки, внедрения и управления информационной безопасностью.
- Эффективное поэтапное внедрение с учетом альтернативных решений по защите.
- Использование лучших продуктов и сервисов информационной безопасности благодаря интеграции с решениями глобальных партнеров Cisco.

Принципы, заложенные в Cisco SAFE, позволили компании Cisco разработать на ее основе целый ряд новых сетевых защищенных архитектур, учитывающих отраслевую специфику. В качестве примера можно назвать две следующих отраслевые архитектуры - Cisco SAFE for PCN (Process Control Network) для защиты систем управления технологическими производствами и процессами АСУ ТП (SCADA) и Cisco Secure Store for PCI, ориентированную на выполнение требований стандарта PCI DSS и защиту предприятий розничной торговли.

Отличие от других производителей: Большинство других производителей средств защиты предлагают свои изделия, как коробочные продукты – без учета потребностей своих заказчиков и специфики защищаемых ресурсов, процессов и данных.

## 5. Рекомендации по дизайну решений

Компания Cisco много лет назад взяла курс на разработку не только лучших в своем классе решений, но и на помощь нашим заказчикам в их правильном внедрении в зависимости от условий функционирования. Программа Cisco Validated Design (<http://www.cisco.com/go/cvd>) включает в себя

описания различных сценариев использования решений Cisco. Эти сценарии разработаны, протестированы и задокументированы с целью облегчения внедрения и роста отдачи от реализованных проектов. Эти сценарии включают широкий диапазон технологий и продуктов Cisco и наших партнеров, которые были разработаны для решения бизнес-потребностей заказчиков.

Отличие от других производителей: Большинство других производителей средств защиты предлагают свои изделия, как коробочные продукты – без детальных рекомендаций по внедрению, настройке и эксплуатации.

## 6. Поддержка и защита самых современных технологий

Будучи разработчиком не только средств сетевой безопасности, но и множества иных решений (IP-телефония, видеоконференцсвязь, виртуализация, Wi-Fi, системы хранения, видеонаблюдение, маршрутизация, коммутация и т.д.) компания Cisco может учитывать все особенности указанных технологий с точки зрения информационной безопасности. Например, для защиты унифицированных коммуникаций важно учитывать высокую производительность при коротких длинах IP-пакетов и различные механизмы обеспечения качества обслуживания. Другой пример: для защиты систем хранения необходимо предусматривать поддержку не только протокола Ethernet, но и Fibre Channel, iSCSI и т.д.

Отличие от других производителей: Другие производители не могут обеспечить поддержку столь широкого спектра различных современных протоколов и технологий по причине своей узкой специализации.

## 7. Контроль качества

Любое программное или программно-аппаратное обеспечение компании Cisco проходит жесткий контроль качества. Дополнительную проверку с точки зрения безопасности проводит специальное подразделение Cisco Product Security Incident Response Team (PSIRT).

Помимо собственного подразделения PSIRT наша компания также входит в альянс FIRST. Это позволяет нам своевременно получать информацию о различных уязвимостях от других участников FIRST, что многократно увеличивает вероятность обнаружения и устранения уязвимостей еще до того, как об этом станет известно широкой общественности.

Дополнительную информацию о процессе поиска и устранения уязвимостей в оборудовании Cisco, вы можете  узнать  по  адресу: [http://www.cisco.com/en/US/products/products\\_security\\_vulnerability\\_policy.html](http://www.cisco.com/en/US/products/products_security_vulnerability_policy.html).

Отличие от других производителей: Большинство производителей средств защиты не имеют аналогов подразделения PSIRT и никто из них не входит в альянс FIRST, что вынуждает их «вариться в собственном соку» и рассчитывать только на свои силы в поиске уязвимостей в своих продуктах.

## 8. Сертификация на соответствие российским требованиям по безопасности

В России существует множество стандартов и требований по информационной безопасности (ФСТЭК, Ростехрегулирование, Мининформсвязи, Банк России и т.п.). Решения Cisco по информационной

безопасности соответствуют всем основным требованиям этих стандартов и рекомендаций. Во многих случаях это подтверждается соответствующими сертификатами. Общее число выданных Федеральной службой по техническому и экспортному контролю (ФСТЭК) компании Cisco сертификатов превысило 500, что на один-два порядка превышает число сертификатов, полученных какой-либо другой компанией (российской или зарубежной), работающей на рынке информационной безопасности России.

При этом компания Cisco проводит не только сертификацию своей продукции по схеме сертификации единичного экземпляра или партии средств защиты, но и по схеме серийного производства. Это означает, что компания, которой выдан сертификат на серийное производство, организует испытания каждого образца оборудования на соответствие сертифицированным параметрам, по утвержденным ФСТЭК России программам и методикам, и, при положительном результате выполнения проверок, выдает комплект документов и копию сертификата на каждое изделие, прошедшее через серийное производство. Для сертификации по схеме единичного образца или партии требуется от 9 до 12 недель. При сертификации по схеме «серия» время поставки сертифицированного изделия значительно сокращается (до 2-х недель); также возможно снижение стоимости сертификации.

В 2010-м году компания Cisco совместно со своим технологическим партнером – компанией С-Терра СиЭсПи, получила сертификат ФСБ на совместное VPN-решение на базе отечественных алгоритмов шифрования.

Отличие от других производителей: Остальные производители обычно либо не сертифицируют свои решения по требованиям безопасности ФСТЭК и ФСБ, нарушая тем самым требования российского законодательства, либо такая сертификация носит фрагментарный и единичный характер, что приводит к потенциальным рискам для заказчиков, использующих несертифицированные средства защиты информации.

## 9. Сертифицированное решение по криптографической защите

Совместно с компанией С-Терра СиЭсПи компания Cisco разработала и провела сертификацию в ФСБ двух своих продуктов, на базе которых возможно построение VPN – модуля NME-RVPN (в исполнении MCM) для маршрутизаторов Cisco ISR и ISR G2 и серверов UCS-C.

Отличие от других производителей: Большинство остальных производителей либо используют свои собственные средства шифрования (на базе зарубежных алгоритмов) в нарушении российского законодательства (таможенного и в области информационной безопасности). Отдельные производители встраивают в свои продукты сертифицированные криптобиблиотеки. Однако согласно разъяснениям ФСБ для VPN-решений этого недостаточно – необходимо сертифицировать все изделие целиком.

## 10. Сертификация производства по требованиям ФСТЭК

Компания Cisco активно взаимодействует с ФСТЭК с целью сертификации своих решений не только по схеме единичного экземпляра или партии, но и по схеме серийной сертификации (сертификация производства). Это позволит отказаться от сертификации отдельных экземпляров оборудования и ускорить поставку заказчикам средств защиты компании Cisco, соответствующих требованиям российского законодательства. Срок сертификации по схеме серийного производства сокращается с 9-12 недель до двух, а стоимость может быть снижена на порядок.

Отличие от других производителей: Практически все зарубежные производители идут по пути сертификации отдельных экземпляров своего оборудования для отдельных заказчиков, что увеличивает стоимость и срок поставки сертифицированного оборудования на 3-5 месяцев (при условии проведения всего спектра необходимых проверок).

## 11. Участие в разработке стандартов по информационной безопасности

Не будет преувеличением сказать, что на наших исследованиях «построен» Интернет и его безопасность - эксперты Cisco участвовали в разработке многих общепризнанных стандартов в области защиты информации, начиная от IPSec и заканчивая CVSS. Специалисты Cisco участвуют в работе различных консультационных советов, рабочих групп и комитетов по стандартизации, что позволяют нам предлагать решения, учитывающие специфику той или иной отрасли и вертикали рынка. В частности, сотрудники Cisco участвуют в работе:

- National Infrastructure Advisory Council (NIAC),
- NIAC Vulnerability Framework Committee,
- AGA-12,
- ISA SP 99,
- DNP,
- ODVA,
- Process Control Security Requirements Forum,
- IEC TC 57 WG 15,
- NCMS Manufacturing Trust,
- National Security Telecommunications Advisory Committee (NSTAC),
- National Cyber Security Alliance,
- Information Sharing and Analysis Centers (IT-ISAC),
- Advisory Board to National Security Agency,
- Network Reliability and Interoperability Council (NRIC),
- National Security Telecommunications and Information Systems Security Institute (NSTISSI),
- Infragard,
- Partnership for Critical Infrastructure Security.

В России Cisco принимает участие в работе:

- ПК 127 «Безопасность информационных технологий» в ТК 22 при Ростехрегулировании
- ТК 362 «Защита информации» при Ростехрегулировании и ФСТЭК
- ПК 3 «Защита информации в кредитно-финансовых учреждениях» в ТК 362 при Ростехрегулировании
- Консультационного центра АРБ по персональным данным
- Рабочей группы ЦБ / АРБ по разработке Комплекса стандартов Банка России по информационной безопасности
- Рабочих групп Минкомсвязи и Ассоциации документальной электросвязи (АДЭ).

Эта работа позволяет нам не только участвовать в разработке новых требований по информационной безопасности, но и заранее знать о готовящихся нормативных актах в области защиты информации, заблаговременно подготавливая свои решения к новым требованиям.

Отличие от других производителей: Ни один зарубежный производитель и ограниченное число отечественных разработчиков средств защиты не участвует в стандартизации вопросов информационной безопасности в России.

## **12. Участие в экспертизе нормативных актов по вопросам информационной безопасности**

Эксперты компании Cisco являются общепризнанными специалистами в области информационной безопасности и участвуют не только в разработке различных отраслевых стандартов по информационной безопасности, но и в экспертизе проектов федеральных законов, а также проектов нормативных актов российских регуляторов в области информационной безопасности.

Отличие от других производителей: Ни один зарубежный производитель и ограниченное число отечественных игроков рынка информационной безопасности не участвует в экспертизе нормативных актов по защите информации в России.

## **13. Исследования в области информационной безопасности и угроз**

Без исследований невозможно разрабатывать решения, которые бы удовлетворяли как требованиям заказчиков, так и рекомендациями различных регулирующих органов и нормативных документов. Именно поэтому компания Cisco инвестирует около 10% своего общего бюджета на исследования и разработки на нужды, связанные с информационной безопасностью.

Cisco Security Intelligence Services — исследовательская группа Cisco, базирующаяся в США, Австралии, Великобритании, Индии, Германии, Бельгии и Сингапуре. Ее эксперты занимаются анализом сотен источников информации об уязвимостях и угрозах, взаимодействуют с различными исследовательскими группами и производителями, а также проводят собственные исследования и тестирования в области ИБ.

Для поддержания систем защиты наших заказчиков в актуальном состоянии компания Cisco предлагает ряд платных и бесплатных сервисов, облегчающих ежедневную деятельность служб информационной безопасности:

- Cisco IntelliShield Alert Manager Service — Web-сервис (<http://www.cisco.com/go/intellishield>), позволяющий освободить технических специалистов от постоянного поиска и отслеживания уязвимостей в продуктах, используемых в корпоративной сети компании. На данный момент база данных уязвимостей содержит около 20000 записей о 5500 программных продуктах 1700 разработчиков.
- Cisco IntelliShield Periodic Security Activity Report (PSAR) — стратегический сервис, в рамках которого еженедельно публикуются бюллетени с описанием текущей активности в области безопасности и средне- и краткосрочными перспективами. В каждом бюллетене описывается 7 основных категорий рисков: уязвимости, физический доступ, юридические, человеческие, геополитические аспекты и т.д. Бюллетени PSAR — это результат совместной работы аналитиков Cisco из команды IntelliShield, ROS, PSIRT, Corporate Security Programs Organization (CSPO) и юридического департамента.
- Cisco Security Intelligence Opera — Web-ресурс (<http://www.cisco.com/go/sio>) с девизом «Информировать, защищать, реагировать» (Inform, Protect, Respond) является единой точкой контакта по всем вопросам информационной безопасности Cisco. На данном портале (<http://www.cisco.com/security>) можно найти информацию об уязвимостях в программно-

аппаратном обеспечении 5500 производителей, сигнатурах атак для Cisco IPS, рекомендации по отражению вторжений и устранению уязвимостей, аналитика по ИБ, источниках и уровне текущих угроз, вирусов, спама и т.д.

- Cisco Applied Mitigation Bulletin — регулярно публикуемые бюллетени Cisco, описывающие использование различных технологий Cisco, защищающих от новых уязвимостей.
- IronPort SenderBase — ресурс (<http://www.senderbase.org/>), который позволяет оценивать текущий уровень вирусных и спам-угроз, знакомиться с отчетами и рекомендациями экспертов в области ИБ, узнавать о рейтинге подозрительности тех или иных доменов или IP-адресов и т.п. Высокий уровень экспертизы достигается за счет анализа свыше 25% всего мирового Интернет-трафика.

Данная информация может быть получена как на сайте компании Cisco (<http://www.cisco.com/security>), так и с помощью бесплатного приложения Cisco SIO Go to iPhone, которое можно загрузить с сайта Apple AppStore или через программу Apples iTunes.

Отличие от других производителей: Деятельность большинства других производителей ограничивается только исследованиями в области вирусной угрозы и публикацией ежегодных отчетов о состоянии ИБ в мире — ежедневных обновлений по вопросам информационной безопасности не публикует практически никто.

## 14. Интеграция с российскими средствами защиты

Учитывая специфику российского рынка информационной безопасности и наличие своего собственного, локального рынка разработки средств защиты, компания Cisco активно сотрудничает с отечественными разработчиками и интегрирует свои решения с созданными в России системами контроля утечек информации (Infowatch и Инфосистемы Джет), антивирусами (Лаборатория Касперского), сканерами безопасности (Positive Technologies), VPN-решениями (С-Терра СиЭсПи и другие).

Отличие от других производителей: Практически никто из зарубежных производителей средств защиты не интегрирует свои продукты с отечественными разработками, исключая встраивание сертифицированных криптобиблиотек.

## 15. Обучение и сертификация российских специалистов

Компания Cisco имеет разветвленную региональную сеть из нескольких десятков учебных центров и сотен сетевых академий, которые проводят авторизованное обучение и сертификацию специалистов на знание информационных и сетевых технологий.

Обучение по курсам, подготовленным компанией Cisco в области информационной безопасности, можно пройти в авторизованных учебных центрах — Cisco Training Center, Комптек и REDCENTER и десятках других, разбросанных по территории Российской Федерации и стран СНГ. Более подробная информация по ним может быть найдена по адресу: <http://www.cisco.com/go/securitytraining>.

По информационной безопасности компания Cisco предлагает две схемы сертификации, ценящиеся во всем мире:

- Основная сертификация
  - Cisco Certified Internetwork Expert (CCIE Security)

- Cisco Certified Security Professional (CCSP)
- Специализированные сертификации по основным технологиям, в т.ч. и информационной безопасности
  - Cisco Advances Security Field Specialist
  - Cisco Firewall Specialist
  - Cisco IPS Specialist
  - Cisco Security Sales Specialist
  - Cisco Security Solutions and Design Specialist
  - Cisco VPN Specialist.

Более подробная информация по ним может быть найдена по адресам: <http://www.cisco.com/go/ccsp>, <http://www.cisco.com/en/US/learning/le3/ccie/security/index.html> и [http://www.cisco.com/web/learning/le3/le2/le41/le85/learning\\_certification\\_type\\_home.html](http://www.cisco.com/web/learning/le3/le2/le41/le85/learning_certification_type_home.html).

Отличие от других производителей: Остальные производители либо не имеют в России авторизованных учебных центров, либо эти центры ограничиваются двумя-тремя и располагаются только в Москве.

## 16. Публикации и книги по ИБ

С целью обучения и повышения осведомленности своих заказчиков по вопросам, связанным с информационной безопасностью, компания Cisco не только создала ресурс Cisco Security Intelligence Operations, но и ведет другую разнообразную просветительскую деятельность. В частности, публикует книги по вопросам информационной безопасности в собственном издательстве CiscoPress (<http://www.ciscopress.com/>). Многие из этих книг изданы и на русском языке.

Отличие от других производителей: Ни один производитель средств защиты не имеет собственного издательства.

## 17. Финансирование проектов по безопасности

Cisco Capital – специальное подразделение Cisco (<http://www.ciscocapital.ru/>), предлагает простые и гибкие схемы финансирования, приобретения, аренды и лизинга, оплаты с отсрочкой устройств безопасности и сетевого оборудования Cisco для организаций любого размера и формы собственности. Благодаря этому предприятия могут реализовывать проекты, повышающие защищенность важнейших бизнес-приложений, даже в условиях нехватки финансовых ресурсов и нестабильной экономической ситуации.

К преимуществам использования Cisco Capital можно отнести:

- Возможность быстрого внедрения. Минимальные начальные инвестиции и распределение платежей на период финансирования (например, лизинга или оплаты с отсрочкой) позволяют без существенных капитальных затрат приобрести технологию, необходимую уже сегодня.
- Экономия капитала. За счет распределения расходов на новые технологии по времени высвобождается ликвидный капитал для инвестиций в другие направления деятельности компании.
- Максимум простоты и гибкости. Cisco Capital предлагает широкий спектр условий и схем лизинга, включая отсрочку первоначального лизингового платежа сроком до одного года, а также возможность модернизации решений по безопасности в течение всего срока лизинга.

- Комплексная финансовая поддержка. Обеспечивается финансирование как затрат на приобретение решений по безопасности, так и расходов на оплату сервисной поддержки, которые также включаются в лизинговые платежи.
- Упрощение процессов бюджетирования. Лизинг позволяет предприятиям использовать бюджеты текущих расходов для приобретения тех решений по безопасности, которые максимально соответствуют потребностям предприятия.
- Налоговые преимущества. Лизинговые платежи относятся на себестоимость, снижая налогооблагаемую базу на прибыль. Ускоренная амортизация при использовании лизинга существенно сокращает отчисления по налогу на имущество.

Отличие от других производителей: Ни один из работающих на рынке производителей средств защиты больше не предлагает услуг по финансированию проектов по информационной безопасности.

## 18. Легитимный ввоз оборудования на территорию России

По российскому законодательству, ввоз продукции, содержащей шифрование, требует получения лицензии Министерства промышленности и торговли РФ, оформляемой на основании разрешения ФСБ России на каждую конкретную партию товаров. Также существуют разрешительные списки (нотификации), куда могут включаться продукты, которые могут ввозиться без получения лицензий.

Компания Cisco активно взаимодействует с Центром по лицензированию, сертификации и защите государственной тайны ФСБ с целью составления списка оборудования которое можно без проблем ввозить на территорию Российской Федерации и использовать в российских компаниях и федеральных органах государственной власти. На сегодняшний день разрешение на ввоз (нотификация) получены практически на все продукты компании Cisco.

Эти усилия компании Cisco гарантируют потребителю не только законное приобретение оборудования, но и защиту бизнеса и топ-менеджмента от обвинений в использовании контрабандного оборудования, приостановления деятельности лицензий ФСБ на деятельность в области шифрования и конфискации незаконно или обманно ввезенного оборудования.

Отличие от других производителей: Нередки случаи незаконного (контрабандного) ввоза оборудования других производителей в обход действующего законодательства о ввозе. Например, в обход писем ФСБ России (исх. № 8/ЛЗ/2/3-3394 от 22.12.2005 года) и ЦТУ РФ (N 08-12/7378 от 26.12.2005), которые требуют, чтобы оборудование других производителей должно в обязательном порядке проходить дополнительные проверки.

## 19. Круглосуточная техническая поддержка

Компания Cisco обеспечивает в России круглосуточную поддержку своих решений, что позволяет нашим заказчикам быстро и своевременно получить консультацию по любой возникшей технической проблеме независимо от часового пояса, в котором заказчик работает. Как правило, такая поддержка осуществляется на русском языке.

Отличие от других производителей: Остальные производители не обеспечивают круглосуточную техническую поддержку своих решений в России.

## **20. Локальные склады оборудования и запчастей**

Компания Cisco имеет на территории России 14 локальных складов, что позволяет своевременно выполнить гарантийные обязательства по поставленным решениям и сократить срок доставки запчастей с нескольких недель или месяцев (в случае поставки с европейских или американских складов) до нескольких часов или дней.

*Отличие от других производителей:* Другие производители не имеют в России сервисных складов и вынуждены поставлять запчасти к своему вышедшему из строя оборудованию из Европы, Америки или Азии, что увеличивает сроки поставки от нескольких недель до нескольких месяцев.

## **21. Развитая региональная партнерская сеть**

Компания Cisco имеет разветвленную сеть из нескольких сотен авторизованных региональных партнеров, которые могут эффективно внедрять и поддерживать решения Cisco во всех регионах и часовых поясах России, что позволяет снизить стоимость и повысить оперативность сопровождения.

*Отличие от других производителей:* Остальные производители не обладают столь разветвленной сетью региональных партнеров, что не позволяет им выполнять проекты в срок и с надлежащим уровнем стоимости и качества.