Архитектура и стратегия информационной безопасности Cisco

Информационная безопасность, как свойство архитектуры предприятия

Перед современным бизнесом стоит множество непростых задач, которые становятся еще актуальнее в условиях нестабильной экономической ситуации. К их числу можно отнести:

- увеличение доходов,
- повышение скорости реакции на изменяющиеся обстоятельства,
- снижение расходов и издержек,
- ускорение инноваций,
- сокращение времени выпуска на рынок продуктов и услуг,
- повышение лояльности заказчиков и партнеров,
- повышение конкурентоспособности,
- обеспечение соответствия нормативным требованиям.

Для решения всех упомянутых задач используется архитектура предприятия (Enterprise Architecture), позволяющая сформировать набор принципов, подходов и технологий, которые, учитывая текущее состояние организации, закладывают основу ее последующей трансформации, роста и развития. Сегодня существует немало подходов к созданию таких архитектур — TOGAF, Zachman Framework, FEAF, DoDAF и другие.
Но какой бы из подходов не был выбран, в современных условиях просто невозможно развиваться без использования информации и информационных технологий, которые должны не только поддерживать любые изменения в бизнесе, но и предвосхищать их, готовиться к ним заранее, а в ряде случаев и способствовать появлению новых бизнес-возможностей. Однако не всегда бизнес развивается предсказуемым образом. Риски различной природы могут нарушить рост и развитие предприятия и поставить его на грань вымирания. Немалую роль в этом играют информационные и операционные риски, связанные с утечками данных, выведением из строя элементов ИТ-инфраструктуры и т. п. Для того чтобы подготовить себя к рискам настоящего и будущего необходима архитектура информационной безопасности, пронизывающая все остальные архитектуры предприятия.

Рисунок 1. Архитектура предприятия и ее связь с другими архитектурами

Архитектура информационной безопасности

Архитектура ИБ описывает процессы, роли людей, технологии и разные типы информации, а также учитывает сложность и изменчивость современного предприятия, адаптируясь к ним, но не ограничивая бизнес-возможности. Иными словами, она описывает желаемое состояние системы информационной безопасности организации и других компонентов и интерфейсов, связанных с ней. При этом архитектура ИБ отражает как текущие и, что очень важно, будущие потребности бизнеса.

Обычно выделяется 3 уровня архитектуры (независимо от того, относится она к информационной безопасности, ИТ или предприятию в целом) — стратегический или концептуальный, логический и системный или технологический (его еще часто называют уровнем реализации). Аналитическая компания Gartner пошла дальше и расширила типовую архитектуру, оставив 3 тех же горизонтальных уровня и добавив еще 3 вертикальных деления (при этом верхний концептуальный уровень также был поделен на 3 подуровня) – люди, информация, технологии. На рисунке показана такая архитектура; при этом белым цветом выделена часть, которая обычно остается вне поля зрения службы информационной безопасности, ввиду их концентрации преимущественно на технологических аспектах.

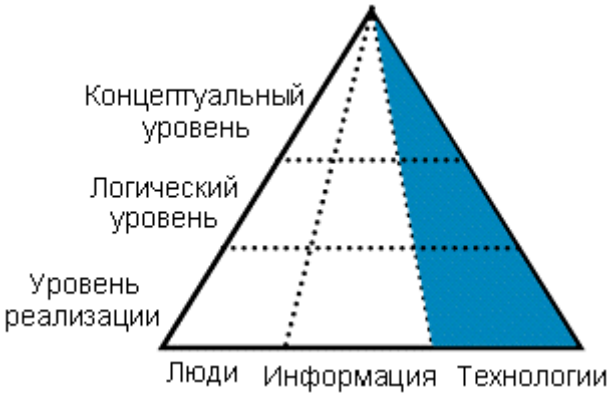

Рисунок 2. Архитектура информационной безопасности

Миссия компании Cisco в области информационной безопасности заключается в создании условий для безопасного роста бизнеса наших заказчиков. При этом безопасность обеспечивается прозрачным и невидимым для конечного пользователя способом – все, как в хорошем автомобиле, – пассивные защитные механизмы работают ежесекундно и, не создавая помех, обеспечивают безопасность как водителя и пассажиров, так и окружающих их людей. В минуты серьезной опасности включается активная защита, предотвращающая или снижающая последствия аварийных ситуаций. Разумеется, мы не ограничиваемся только техническими решениями, а предлагаем целый комплекс мер, по возможности, охватывающих все уровни архитектуры информационной безопасности предприятия.

Архитектура защищенной сети как составная часть архитектуры безопасности

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 призвана помочь тем, кто проектирует сети и анализирует требования к сетевой безопасности. Данный подход нацелен не на механическую установку межсетевого экрана 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.

Рисунок 3. Архитектура защищенной сети предприятия Cisco SAFE

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 примеров можно указать следующие отраслевые архитектуры:

- Cisco SAFE for PCN (Process Control Network) для защиты систем управления технологическими производствами и процессами АСУ ТП (SCADA).

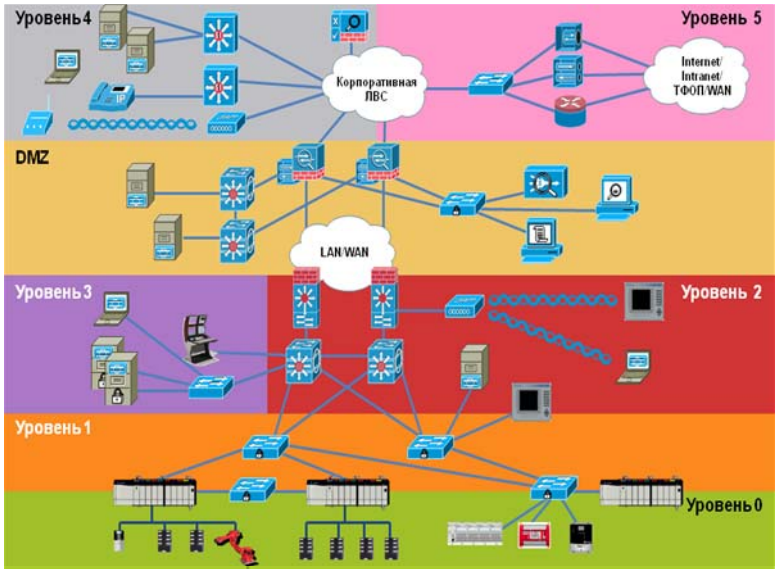

Рисунок 4. Архитектура защиты АСУ ТП Cisco SAFE for PCN

- Cisco Secure Store for PCI (http://www.cisco.com/go/pci), ориентированную на выполнение требований стандарта PCI DSS и защиту предприятия розничной торговли.

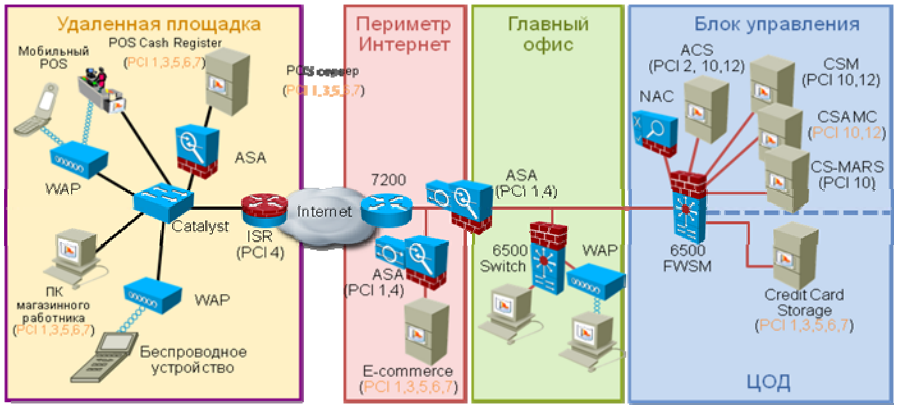

Рисунок 5. Архитектура защиты предприятия розничной торговли Cisco Secure Store for PCI

Отраслевая деятельность компании Cisco на ниве информационной безопасности не ограничивается названными архитектурами. Эксперты компании участвуют в работе различных консультационных советов и рабочих групп, что позволяют нам предлагать решения, учитывающие специфику той или иной 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,
- Ассоциации документальной электросвязи (АДЭ) и т.п.

Стратегия: на пути к архитектуре информационной безопасности

Архитектура ИБ отражает состояние информационной безопасности в определенный момент времени. И хотя сложно себе представить полностью застывшую систему, в которой не происходит никаких изменений, все же архитектура играет большую роль в деятельности любой службы ИБ. Но как достигнуть этого состояния? Как из текущего состояния перейти в новое, более совершенное и соответствующее целям бизнеса? Для этого существует стратегия, т.е. направление движения для достижения поставленных целей. В противном случае цели можно достичь не всегда единственным, и не всегда оптимальным путем.

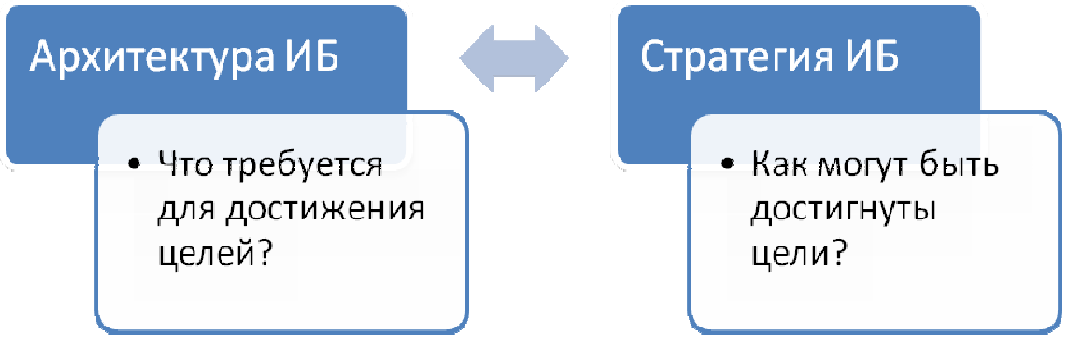

Рисунок 6. Взаимосвязь архитектуры и стратегии ИБ

Стратегия – это структурированный и взаимосвязанный набор действий, нацеленных на улучшение в долгосрочном плане благополучия предприятия. А для того чтобы обеспечение безопасности осуществлялось наиболее эффективным образом, компания Cisco разработала стратегию ИБ, позволяющую не только оценить текущий уровень защищенности наших заказчиков, но и разработать для них оптимальную схему перехода к разработанной архитектуре ИБ с учетом как лучших международных практик, так и национального законодательства в области защиты информационных ресурсов.

Чтобы реализовать на практике архитектуру защищенной сети Cisco SAFE, необходимо иметь в своем арсенале набор технических решений, которые смогут претворить в жизнь разработанные политики информационной безопасности.

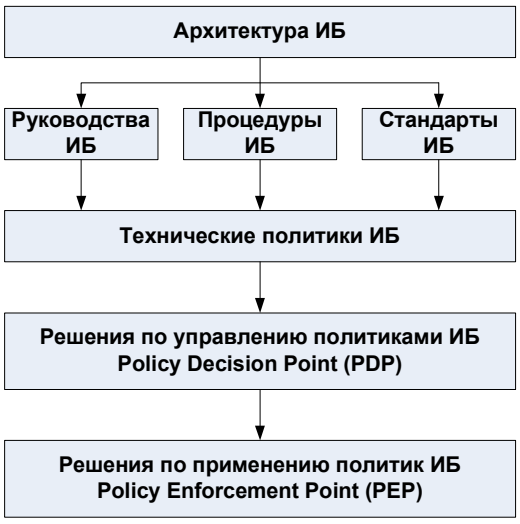

Рисунок 7. От концепции к техническим решениям

Два нижних уровня этой модели (PDP и PEP) – это и есть технические решения Cisco в области информационной безопасности, входящие в концепцию самозащищающейся сети Cisco Self-Defending Network (SDN). Ее идея достаточно проста: в настоящее время

поддержание целостности и конфиденциальности корпоративной информации, а также непрерывности бизнеса в течение всего жизненного цикла бизнес-процессов является ключом к успеху любой компании. Значение информации и контроля доступа к ней еще никогда не было так велико. Таким образом, задачей системы безопасности является обеспечение своевременного доступа законным пользователям с одновременной возможностью обнаружения и предотвращения нарушений безопасности. Современные сети должны реагировать на такие нарушения, сохраняя свою доступность, надежность и функциональность. Во многих отношениях, целью процесса обеспечения безопасности является обеспечение непрерывности бизнеса. Вместо того чтобы становиться жертвой, инфраструктура должна быть способна «поглощать» атаки и сохранять работоспособность, подобно иммунной системе человека, позволяющей организму функционировать при наличии в нем вирусов и бактериальных инфекций.

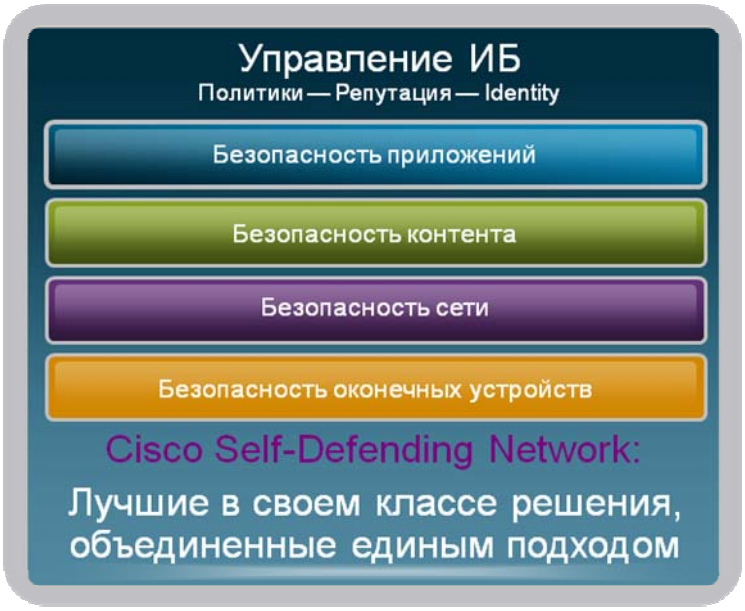

Рисунок 8. Стратегия самозащищающейся сети Cisco Self-Defending Network

Концепция самозащищающейся сети Cisco Self-Defending Network (http://www.cisco.com/go/sdn) является основой для защиты всех данных, приложений и бизнес-процессов. Она представляет собой основную составляющую стратегии организации по управлению рисками нарушения информационной безопасности, поскольку именно концепция SDN позволяет реализовать комплексный системный подход к проблеме сетевой безопасности, основанный на общепризнанных в отрасли механизмах контроля и передовых методах обеспечения защиты. Этот подход позволяет организациям усовершенствовать механизм управления операционными и информационными рисками, а также обеспечить соответствие принятых решений международным и национальных нормативно-правовым актам.

Концепция Cisco Self-Defending 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.

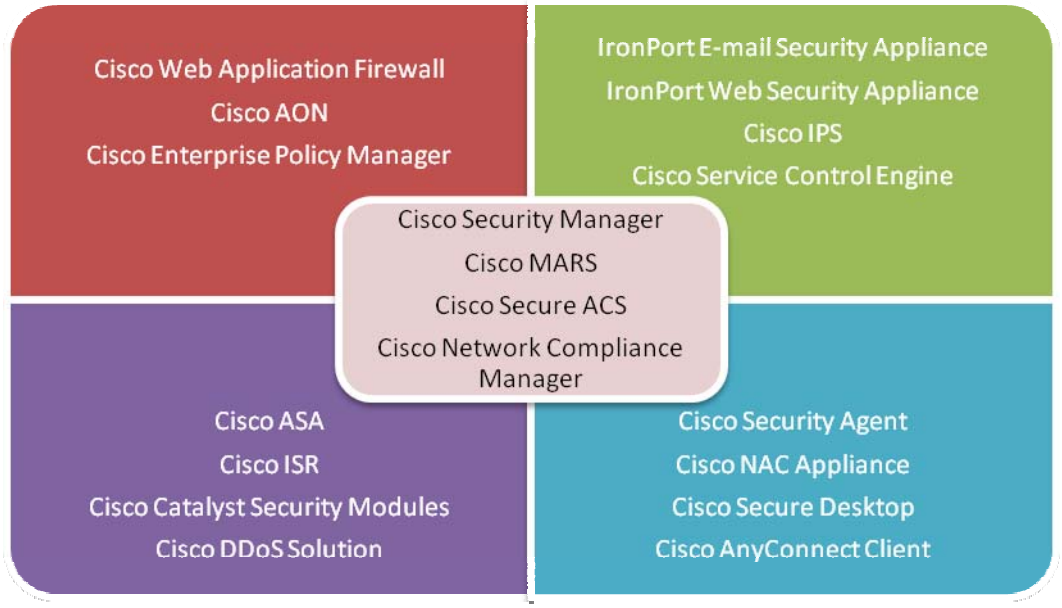

Рисунок 9. Продукты Cisco для обеспечения информационной безопасности

Однако принципы, заложенные в стратегию Cisco в области информационной безопасности, говорят о том, что мы должны 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-Терра CSP, Dr.Web, Sophos, Trend Micro, ESET, Aladdin и т.д.

О лидерстве и качестве технических решений Cisco

Без исследований невозможно разрабатывать решения, которые бы удовлетворяли как требованиям заказчиков, так и рекомендациям 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. В абсолютных цифрах эта сумма составляет около 500 миллионов долларов США ежегодно. Такой подход позволяет компании Cisco лидировать практически во всех сегментах рынка средств защиты информации, на которых представлены решения компании.

Рисунок 10. Слияния и поглощения Cisco в области ИБ

1500 сфокусированных на безопасности инженеров, специальные процедуры тестирования и контроля качества… Все это позволяет гарантировать высокое качество решений в области информационной безопасности. В качестве примера можно упомянуть запущенную в компании Cisco программу Safe Harbor (http://www.cisco.com/go/safeharbor), которая фокусируется на расширенном тестировании продуктов Cisco для особо критичных применений. В рамках Safe Harbor сертифицированы, например, Cisco Catalyst 6500, FWSM, IDSM2, ACE и др.

Наша лидирующая роль была бы невозможной не только без серьезных инвестиций в исследования и разработку, но и без участия в работе различных стандартизующих организаций и рабочих групп, упомянутых ранее. Не будет преувеличением сказать, что на наших исследованиях «построен» Интернет и его безопасность — эксперты Cisco участвовали в разработке свыше 60 общепризнанных стандартов в области защиты информации, начиная от IPSec и заканчивая CVSS. Но наша компания не останавливается на достигнутом и продолжает активно участвовать в разработке различных стандартов по информационной безопасности. Другой пример — специальная группа Cisco Product Security Incident Response Team (PSIRT), управляющая процессом поиска и устранения уязвимостей в решениях Cisco, получающая, исследующая и публикующая бюллетени о них, а также отвечающая за обработку инцидентов, связанных с этими уязвимостями, в сетях заказчиков.

Качество решений Cisco подтверждено не только внутренними процедурами, но и внешними наградами и оценками аналитиков — Synergy, Infonetics, Gartner, Cnews и т.п. Например, согласно исследованиям компании Synergy компания Cisco последние 6 лет занимает 1-е место на рынке сетевой безопасности, удерживая долю от 38% до 42%, что в три раза превышает показатели ближайшего конкурента. По данным российского аналитического агентства CNews наша компания уже не первый год подряд занимает первое место в России среди игроков рынка информационной безопасности.

Жизненный цикл системы защиты на предприятии

Для того чтобы обеспечить эффективное движение к принятой архитектуре ИБ необходимо реализовать на предприятии весь жизненный цикл системы информационной безопасности, включающий в себя не только внедрение технических средств защиты, но и множество дополнительных сервисов и услуг. Все они обеспечивают решение множества важных задач, среди которых анализ рисков, аудит безопасности, повышение осведомленности, реагирование на инциденты, мониторинг состояния защищенности и многие другие.

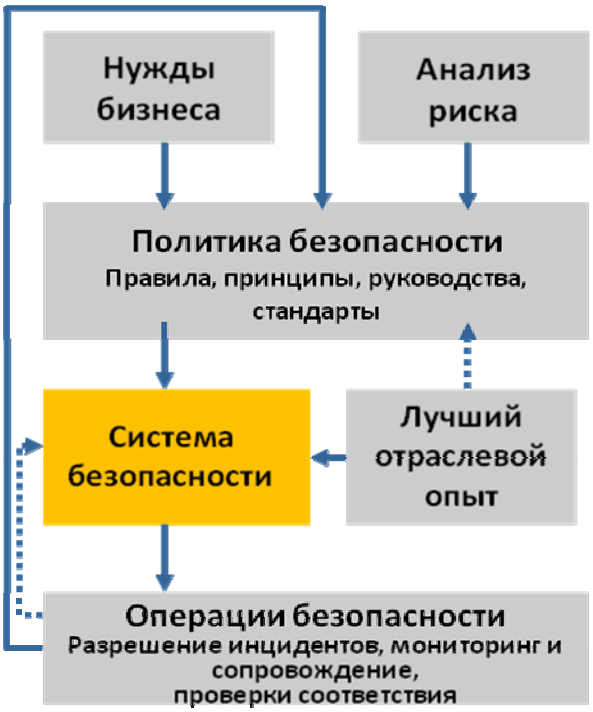

Рисунок 11. Жизненный цикл системы ИБ на предприятии

Сложность и масштабность современных информационных систем для бизнеса делают процесс обеспечения их безопасности далеко не простым делом. Группа консультантов компании Cisco (http://www.cisco.com/go/services) готова помочь вам:

- В разработке стратегии и архитектуры управления информационными и операционными рисками.
- В анализе существующей архитектуры и дизайна защищенной сети.
- Во внедрении и настройке средств управления рисками согласно утвержденной стратегии.
- В миграции на новые решения по обеспечению информационной безопасности.
- В оптимизации уже внедренных и настроенных средств защиты.
- В поддержке внедренных решений при помощи круглосуточной службы технической поддержки (Technical Assistance Center).
- В обработке и управлении инцидентов безопасности.
- В аудите созданной ИТ-инфраструктуры на соответствие требованиям международных стандартов ISO 27001/27002, CoBIT, ITIL, PCI DSS и т.п.
- В реализации многих других услуг, реализуемых в рамках всего жизненного цикла системы защиты.

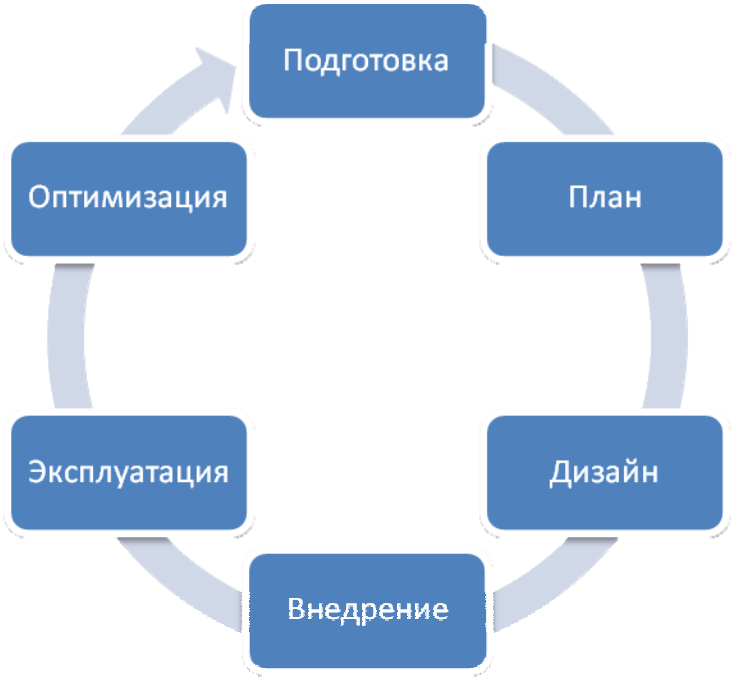

Рисунок 12. Жизненный цикл услуг Cisco

В качестве примера можно привести предлагаемую в России для крупных заказчиков и сервис-провайдеров уникальную услугу компании Cisco «Обследование сетевой инфраструктуры и анализ рисков безопасности». Эта услуга сочетает в себе преимущества локального присутствия компетентных консультантов и использования мирового опыта работы с ведущими поставщиками услуг и международными корпорациями, цена утечки информации или взлома сети для которых оценивается десятками миллионов долларов.

Услуга обеспечивает реализацию этапов «Подготовка» и частично «План» жизненного цикла услуг Cisco и выполняется консультантами подразделения Cisco Advanced Services. В результате работ по исследованию существующей инфраструктуры на основе предъявляемых к системе безопасности требований выявляются возможные угрозы, оцениваются риски; при этом широко используются и применяются международные практики и наработки. В результате заказчик получает документы с описанием результатов исследований, анализа и приоритезации рисков, отчет об архитектуре безопасности с рекомендациями и планом по уменьшению влияния этих рисков. На основе этого отчета можно планировать развитие архитектуры сетевой безопасности и устранение уязвимостей либо самостоятельно, либо с привлечением российских компаний, специализирующихся в соответствующих областях обеспечения безопасности, либо специалистов Cisco Advanced Services.

Как поддерживать систему защиты?

Анализ рисков, внедрение средств защиты, аудит безопасности — все это важные задачи, которые обеспечивают половину успеха в области движения к архитектуре ИБ. Вторая половина успеха – эффективное управление ежедневными операциями (security operations), которые включают в себя множество важнейших задач:

- Анализ текущей ситуации в области ИБ в мире и регионе, включая среднесрочный и краткосрочный прогноз развития ситуации.
- Расследование компьютерных преступлений.
- Исследования в области угроз.
- Мониторинг информационной безопасности.
- Управление уязвимостями, включая тестирование и установку обновлений (патчей).
- Проверка соответствия требованиям нормативных документов.

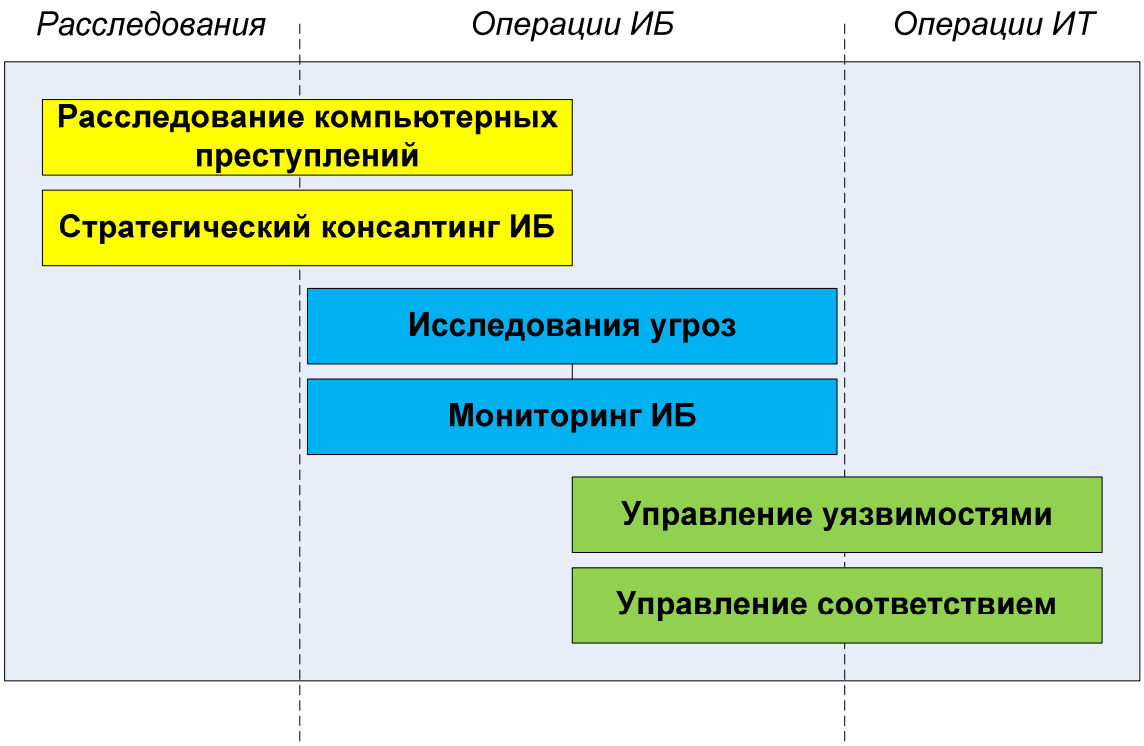

Рисунок 13. Операции в области ИБ

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 описание 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 Center —ресурс 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, об 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.

Рисунок 14. Услуги Cisco Security Intelligence Services

Все эти сервисы базируются на усилиях Cisco Security Intelligence Services — исследовательских группах Cisco, базирующихся в США, Австралии, Великобритании, Индии, Германии, Бельгии и Сингапуре, которые 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.

Обучение Cisco по вопросам информационной безопасности

С целью обучения и повышения осведомленности своих заказчиков по вопросам, связанным с информационной безопасностью, компания Cisco не только создала ресурс Cisco Security Center, но и ведет другую разнообразную просветительскую деятельность — публикует книги по вопросам информационной безопасности в издательстве CiscoPress (http://www.ciscopress.com/), а также проводит обучение по различным аспектам, связанным с собственными продуктами.

Компания Cisco имеет в России разветвленную региональную сеть из нескольких десятков учебных центров и сетевых академий, которые проводят авторизованное обучение и сертификацию специалистов на знание информационных и сетевых технологий. Авторизованные курсы позволяют подготовиться к сдаче экзаменов на получение различных уровней сертификации по безопасности Cisco Specialist или Cisco Certified Security Professional (CCSP). Статус Cisco Specialist может быть получен по одному из следующих направлений:

- Cisco Advances Security Field Specialist;
- Cisco Security Sales Specialist;
- Cisco Firewall Specialist;
- Cisco Security Solutions and Design Specialist;
- Cisco IPS Specialist;
- Cisco VPN Specialist.

Существует также ряд дополнительных курсов, рекомендованных инженерам, готовящимся к сдаче экзамена на высший статус эксперта Cisco Certified Internetwork Expert (CCIE) Security. Завершение обучения по программам CCNA и Cisco Specialist позволяет получить статус INFOSEC Professional (стандарт образования 4011), поддерживаемый Агентством национальной безопасности США (NSA) и Комитетом США по национальным системам безопасности (CNSS).

О соответствии требованиям регуляторов

Практически все организации испытывают повышенное давление со стороны правительства и отдельных ведомств, заинтересованных вопросами надлежащего использования информации, в особенности финансовых или персональных данных. Многие российские руководящие органы и общественность серьезно озабочены проблемами информационной безопасности и начинают предпринимать надлежащие действия, направленные на обеспечение целевого использования и защиты как корпоративной информации, так и персональных данных. Аналогичная задача возникает и при выходе компании на международный рынок (например, на IPO).

В результате всем компаниям, планирующим работать еще не один год, необходимо соответствовать сильно растущему числу законов и постановлений, стандартов и отраслевых требований. К их числу можно отнести акт Сарбейнса-Оксли, ISO 27001 и ISO 27002, Базель II, Руководящие документы Федеральной службы по техническому и экспортному контролю (бывшая Государственная техническая комиссия при Президенте России), «Специальные требования и рекомендации по технической защите конфиденциальной информации» (СТР-К), стандарт Банка России «Обеспечение информационной безопасности организаций банковской системы Российской Федерации», ГОСТ Р ИСО/МЭК 15408, законодательство по защите персональных данных и другие. Решения Cisco по информационной безопасности соответствуют практически всем требованиям этих стандартов и рекомендаций. Во многих случаях это подтверждается соответствующими сертификатами. На сегодняшний день решения компании Cisco имеют около 400 сертификатов ФСТЭК по требованиям информационной безопасности, выданных в России, что существенно превышает число сертификатов, полученных какой-либо другой компанией (российской или зарубежной), работающей на отечественном рынке информационной безопасности.

Финансирование проектов по информационной безопасности

Cisco Capital, специальное подразделение Cisco, 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.

Предоставляемые преимущества

- ***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.

Cisco в России

Дополнительно к уже вышесказанному стратегия Cisco в области информационной безопасности имеет и свою локальную специфику в каждой стране, в которой представлена компания Cisco. В России, помимо уже упомянутой сертификации по требованиям ФСТЭК и других регуляторов, Cisco:

- обеспечивает в России круглосуточную поддержку своих решений на русском языке, что позволяет нашим заказчикам быстро и своевременно получить консультацию по любой возникшей технической проблеме независимо от часового пояса, в котором работает заказчик.
- имеет на территории России локальные склады, что позволяет своевременно выполнять 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 дней или даже часов.
- имеет разветвленную сеть из нескольких сотен 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.
- разрабатывает специфичные продукты для выполнения национальных требований по ИБ. Среди таких решений можно назвать VPN-модуль NME-RVPN с сертифицированным в ФСБ криптографическим ядром, совместное решение с Лабораторией Касперского, совместное решение с компанией «Газинформсервис» и т.д.

Дополнительная информация

- ***Новости Cisco по ИБ*** . Для подписки на новости по информационной безопасности Cisco на русском языке достаточно написать запрос в свободной форме на адрес security-request@cisco.com
- ***Security Policy Builder*** (http://www.ciscowebtools.com/designer/). Web-помощник, автоматизирующий создание типовой политики информационной безопасности.
- ***Security Solution Designer*** (http://www.ciscowebtools.com/designer/). Web-помощник, автоматизирующий создание защищенного сетевого дизайна для небольших предприятий.
- ***PCI Advisor*** (http://www.pcicomplianceadvisor.com). Web-помощник по стандарту PCI DSS и решениям Cisco, помогающим соответствовать требованиям данного стандарта.
- ***Secure Business Advisor*** (http://www.securitybusinessadvisor.com). Web-помощник, автоматизирующий подбор решений Cisco по информационной безопасности, исходя из уже внедренных решений и бизнес-потребностей.
- ***Cisco Security Center*** (http://www.cisco.com/security). Единая точка входа на все ресурсы Cisco по информационной безопасности.

Cisco
Россия, 115054, Москва,
бизнес-центр «Риверсайд Тауерс»,
Космодамианская наб., 52, стр. 1, 4-й этаж.
Телефон: +7 (495) 961 1410
Факс: +7 (495) 961 1469
www.cisco.ru
www.cisco.com

Cisco
Россия, 191186, Санкт-Петербург,
бизнес-центр «Регус»,
Невский пр-т, 25, 2-й этаж, офисы 9, 30.
Телефон: +7 (812) 336 6531
Факс: +7 (812) 346 7800
www.cisco.ru
www.cisco.com

Cisco
Россия, 630099, Новосибирск,
бизнес-центр «Росевроплаза»,
Димитрова пр-т, 2, 5-й этаж.
Телефон: +7 (383) 230 2670
Факс: +7 (383) 230 1795
www.cisco.ru
www.cisco.com

Cisco has more than 200 offices worldwide. Addresses, phone numbers, and fax numbers are listed on the Cisco Website at **www.cisco.com/go/offices.**