Решения Cisco для выполнения требований СТО БР ИББС-1.0-2008

Проблема

По данным опроса Межбанковского Финансового Дома (МФД) и Ассоциации Российских Банков (АРБ), проведенного еще в 2003 году, бизнес-процессы 88% российских финансовых организаций полностью опираются на информационные технологии. С тех пор уровень информатизации не только не снизился, но наоборот вырос. Такая зависимость не позволяет эффективно реализовывать бизнес-процессы без решения вопросов безопасности информационной инфраструктуры.

Банк по праву считается организацией повышенного риска, болезненно реагирующей на любые удары по имиджу. Эпидемии червей, нарушение функционирования серверов платежной информации, перехват важной финансовой информации, утечка клиентской базы, DDoS-атаки на Интернет-банкинг и другие угрозы наносят очень серьезный ущерб по репутации и являются серьезным препятствием для развития бизнеса любого банка. Как только становится известным какое-либо неблагоприятное событие (в том числе и связанное с нарушением защищенности автоматизированной банковской системы), то у банка сразу же могут наступить трудности с пристальным вниманием регуляторов, судебными исками, оттоком клиентов к конкурентам и т.п.

Помимо репутации, важным является сохранение в тайне различной внутренней информации, на которой зачастую и строится принятие решений, измеряемых десятками и сотнями миллионов долларов. Утечка такой конфиденциальной информации позволяет игрокам банковского рынка делать упреждающие ходы, препятствующие тем или иным финансовым мероприятиям (слияния, покупка, продажа и т.д.), что также сказывается на бизнесе любого банка.

Также надо учитывать, что банк, работая с большим числом физических и юридических лиц, должен быть, с одной стороны, открытым, прозрачным и доступным для всех своих вкладчиков, а с другой – защищенным и минимизирующим ущерб от различных умышленных и неумышленных действий собственных сотрудников, клиентов, а также посторонних лиц.

Стандарт СТО БР ИББС-1.0-2008

Понимая данную проблему и являясь ответственным за банковскую систему страны, Центральный банк с 1 декабря 2004 года (Распоряжением Банка России от 18 ноября 2004 года № Р-609) ввел в действие стандарт «Обеспечение информационной безопасности организаций банковской системы Российской Федерации», нацеленный на повышение уровня защищенности российских банков и защиту банковской тайны вкладчиков. С 1 мая 2009 года вводится в действие уже 3-я версия данного стандарта – СТО БР ИББС-1.0-2008.

Основными целями создания данного стандарта явились:

- развитие и укрепление банковской системы России;
- повышение доверия к банковской системе России;
- поддержание стабильности функционирования финансовых организаций и на этой основе – стабильности функционирования банковской системы в целом;
- достижение адекватности мер по защите от реальных угроз информационной безопасности;
- предотвращение и/или снижение ущерба от инцидентов информационной безопасности;

- установление единых требований по обеспечению информационной безопасности российских банковских организаций;
- повышение эффективности мероприятий по обеспечению и поддержанию информационной безопасности организаций банковской системы РФ.

Система обеспечения информационной безопасности (СОИБ) любой финансовой структуры состоит из двух ключевых элементов - совокупности защитных мер, составляющих систему информационной безопасности (СИБ), и совокупности процессов менеджмента ИБ (СМИБ).

Рисунок 1. Система обеспечения ИБ финансовой организации

Жизненный цикл СОИБ и процессы менеджмента ИБ в финансовой организации

Для реализации и поддержания ИБ в финансовой организации необходимо реализовать весь жизненный цикл системы информационной безопасности. Он включает в себя не только внедрение технических средств защиты, но и множество дополнительных сервисов и услуг, обеспечивающих решение множества других задач, среди которых анализ рисков, аудит безопасности, повышение осведомленности, реагирование на инциденты, мониторинг состояния защищенности и многие другие.

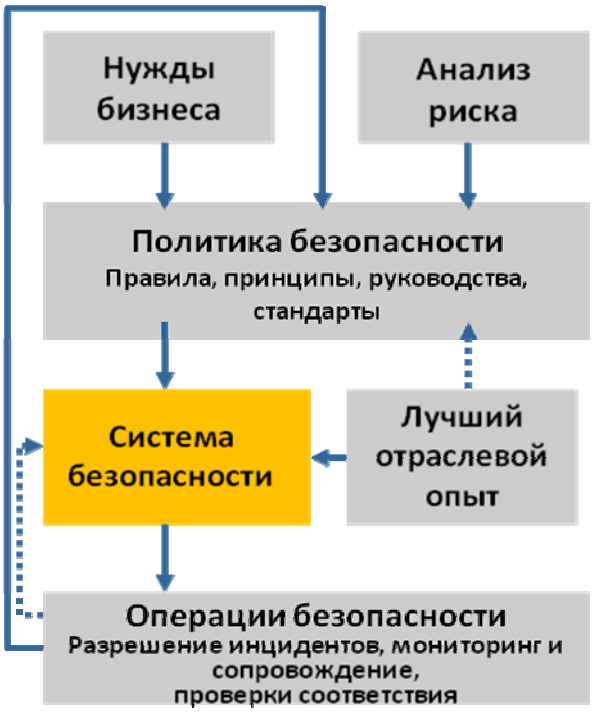

Рисунок 2. Жизненный цикл системы ИБ на предприятии

Учитывая сложность и масштабность современных информационных технологий для бизнеса обеспечить их безопасность — не такое простое дело. Группа консультантов компании Cisco готова помочь в решении следующих вопросов:

- разработка стратегии и архитектуры управления информационными рисками;
- разработка планов обработки рисков нарушения ИБ и внутренних документов, регламентирующих деятельность в области обеспечения ИБ;
- разработка и реализация плана обеспечения непрерывности бизнеса и его восстановления после прерываний;
- анализ существующей архитектуры и дизайна защищенной сети с точки зрения информационной безопасности;
- внедрение и настройке средств управления рисками согласно утвержденной стратегии;
- миграция на новые решения по информационной безопасности;
- оптимизация уже внедренных и настроенных средств защиты;
- поддержка внедренных решений при помощи круглосуточной службы технической поддержки (Technical Assistance Center) на русском языке;
- реагирование на инциденты безопасности;
- аудит созданной инфраструктуры на соответствие требованиям международных стандартов ISO 27001/27002, CoBIT, ITIL, PCI DSS и т. п.;
- реализация многих других услуг, реализуемых в рамках всего жизненного цикла системы защиты.

Рисунок 3. Жизненный цикл услуг Cisco

Базовые защитные меры системы информационной безопасности

К базовым защитным мерам СИБ, применимым к большинству финансовых предприятий, можно отнести следующие (в конкретной организации требования к защитным мерам могут быть расширены):

- управление ролями и уровнями доверия;
- защита от НСД, управление доступом и регистрация всех действий в автоматизированной банковской системе (АБС), телекоммуникационном оборудовании и т. п.;
- антивирусная защита;
- использование ресурсов Интернета;
- использование средств криптографической защиты;
- защита банковских платежных и информационных технологических процессов.

Реализация стандарта СТО БР ИББС-1.0-2008 с помощью Cisco Self-Defending Network

Решения Cisco в области защиты объединены в стратегию самозащищающейся сети Cisco Self-Defending Network. Ее идея достаточно проста: в настоящее время поддержание целостности и конфиденциальности корпоративной информации, включая и банковскую тайну, а также непрерывности бизнеса в течение всего жизненного цикла бизнес- и организационных 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 предоставление своевременного доступа законным пользователям с одновременной возможностью обнаружения и предотвращения вторжений и иных нарушений безопасности на всех уровнях информационной системы. Современные сети должны реагировать на такие нарушения, сохраняя свою доступность, надежность и функциональность. 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.

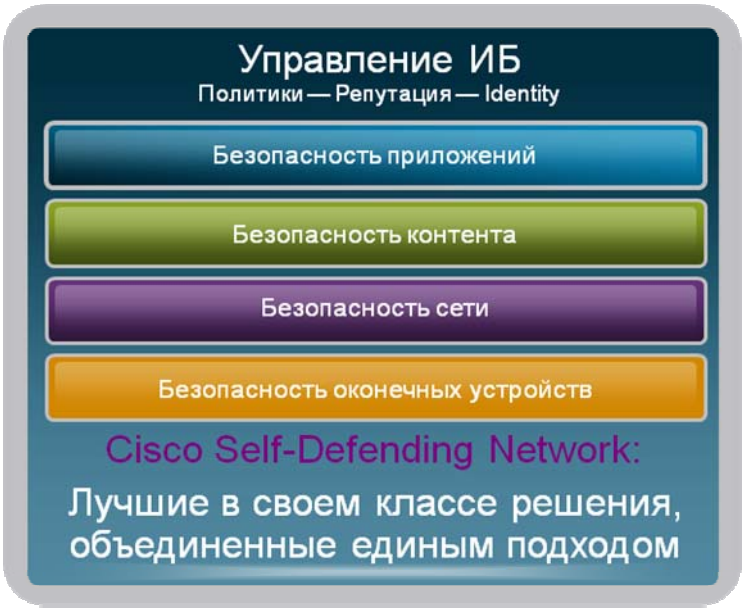

Рисунок 4. Стратегия самозащищающейся сети Cisco Self-Defending Network

Концепция самозащищающейся сети Cisco Self-Defending Network — это сквозная стратегия корпоративной обороны, поскольку она является основой для защиты всех данных, приложений и бизнес-процессов. Она представляет собой основную составляющую стратегии банковских организаций по управлению рисками нарушения информационной безопасности, поскольку она предоставляет комплексный и системный подход к проблеме сетевой безопасности, поддерживающий общепризнанные в отрасли механизмы контроля и передовые методы безопасности, соответствующие требованиям российских регуляторов и Банка России. Этот подход позволяет организациям защитить банковскую тайну и иные конфиденциальные сведения, усовершенствовать механизмы управления операционными и информационными рисками и обеспечить их соответствие российским и международным нормативным документам.

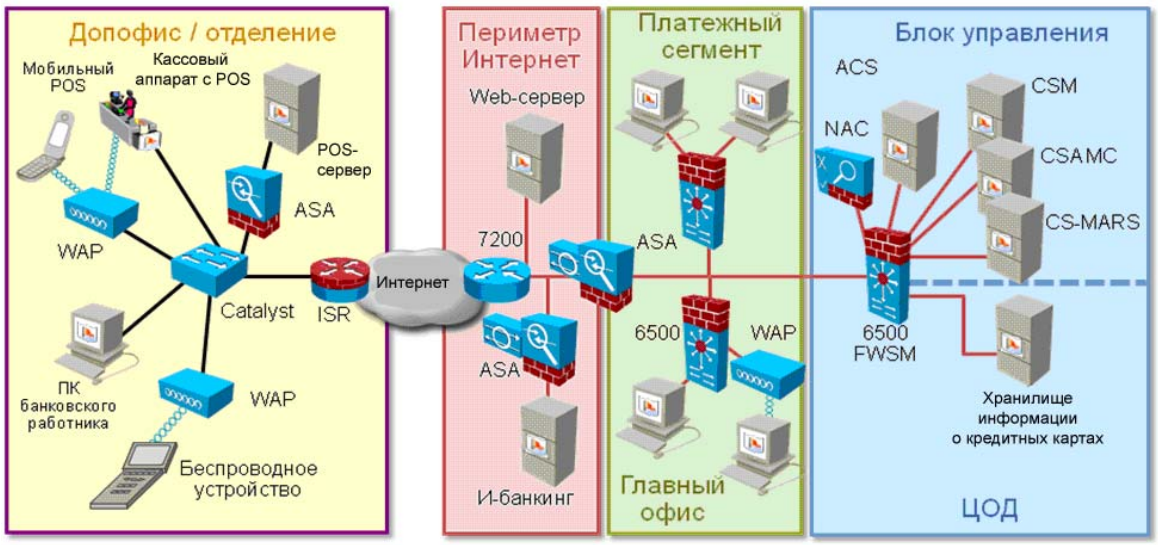

Рисунок 5. Архитектура Cisco для реализации СТО БР ИББС-1.0-2008 (отображены не все элементы)

Решения Cisco, входящие в Self-Defending Network, позволяют выполнить требования к СИБ, указанные в стандарте СТО БР ИББС-1.0-2008. Учитывая, что основной для построения СОИБ являются требования законодательства РФ (например, в области защиты коммерческой тайны или персональных данных), а также рекомендуется использовать сертифицированные или разрешенные руководством предприятия

средства защиты, компания Cisco предлагает организациям банковской системы России сертифицированные решения по информационной безопасности. На сегодняшний день решения компании Cisco имеют около 400 сертификатов 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.

Таблица 1. Продукты Cisco по ИБ, реализующие требования СТО БР ИББС-1.0-2008

Требования	ASA	IPS	CSA	ISR	RVPN	Catalyst	NAC	IronPort	WAF	ACS
Управление ролями и уровнями доверия	+	+	+	+		+	+	+	+	+
Защита от НСД	+	+	+	+		+	+		+	+
Управление доступом	+	+	+	+		+	+		+	+
Регистрация и учет	+	+	+	+	+	+	+	+	+	+
Антивирусная защита	+		+					+		
Использование Интернет	+	+	+	+	+	+	+	+	+	+
Криптографическая защита	+			+	+			+		
Защита банковских процессов	+	+	+	+	+	+	+	+	+	+

Примечание:
ASA — многофункциональные защитные устройства Cisco ASA 5500, а также модуль CSC-SSM,
IPS — Cisco IPS 4200, Cisco IOS IPS, Cisco IPS-AIM, Cisco AIP-IPS,
CSA — система защиты серверов, ПК и лэптопов Cisco Security Agent,
ISR — маршрутизаторы с интегрированными сервисами Cisco ISR,
RVPN — криптографический модуль Cisco NME-RVPN Module для машрутизаторов Cisco ISR,
Catalyst — коммутаторы Cisco Catalyst и сервисные модули для Cisco Catalyst 6500 (IDSM, FWSM, ACE, PISA и т.д.),
NAC — система контроля доступа Cisco NAC Appliance,
IronPort — системы защиты электронной почты и Web-трафика IronPort E-mail Security Appliance и Web Security Apliance,
WAF — защитный шлюз прикладного уровня Cisco Web Application Firewall,
ACS — система аутентификации, авторизации, регистрации и учета Cisco Secure Access Control Server.

Для управления решениями, указанными в таблице, используются системы Cisco Security Manager и Adaptive Security Device Manager. Для мониторинга и анализа событий регистрации, действий и операций, позволяющие выявлять неправомерные или подозрительные операции и транзакции, используется система Cisco MARS. Для проверки качества и эффективности настройки технических защитных мер используется Cisco Network Compliance Manager.

Заключение

Особенности банковской системы РФ таковы, что негативные последствия сбоев в работе отдельных организаций могут привести к быстрому развитию системного кризиса платежной системы РФ, нанести ущерб интересам собственников, акционеров и клиентов. В случаях наступления инцидентов ИБ значительно возрастают результирующий риск и возможность нанесения ущерба банковским организациям. Поэтому для таких предприятий угрозы ИБ представляют существенную опасность.

Для противостояния таким угрозам и обеспечения эффективности мероприятий по ликвидации неблагоприятных последствий инцидентов ИБ (их влияния на операционный, репутационный, стратегический и иные риски) в финансовых организациях следует обеспечить достаточный уровень информационной безопасности. Необходимо также сохранить этот уровень в течение всего срока существования банка. По этим причинам обеспечение ИБ является для финансовых институтов одним из основополагающих аспектов их деятельности.

Компания Cisco Systems, помогая своими решениями реализовать стандарт СТО БР ИББС-1.0-2008, поддерживает эту деятельность, предлагая своим заказчикам не

точечные продукты для защиты отдельных участков автоматизированной банковской системы и ее пользователей, а комплексное решение, интегрируемое в инфраструктуру финансовой организации для обеспечения информационной безопасности бизнеса на всех уровнях. Это позволяет банкам быть уверенными в том, что его бизнес-процессы и ресурсы защищены от посягательств внешних и внутренних злоумышленников, воздействия вредоносных программ и других негативных воздействий через информационную среду.

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.**