ОГЛАВЛЕНИЕ

Предисловие

Согласно RFC 2196 под политикой информационной безопасности компании понимается «формальное изложение правил поведения лиц, получающих доступ к конфиденциальным данным в корпоративной информационной системе». При этом различают общую стратегическую политику безопасности компании, взаимоувязанную со стратегией развития бизнеса и ИТ-стратегией компании, а также частные тактические политики безопасности, детально описывающие правила безопасности при работе с соответствующими ИТ-системами и службами компании.

В соответствии с этим определением и рекомендациями ведущих международных стандартов в области планирования информационной безопасности (ИБ) и управления ею (BS 7799-2:2002, ISO/IEC 17799:2005, ISO/IEC TR 13335, ISO/IEC 10181-7:1996, ISO/IEC 15288:2002, ISO/IEC TR 15443, BSI, CobiT, ITIL, ГОСТ Р ИСО/МЭК 15408-2002) политики безопасности должны содержать следующее:

- предмет, основные цели и задачи политики безопасности;
- условия применения политики безопасности и возможные ограничения;
- описание позиции руководства компании в отношении выполнения политики безопасности и организации режима информационной безопасности компании в целом;
- права и обязанности, а также степень ответственности сотрудников за выполнение политики безопасности компании;
- порядок действия в чрезвычайных ситуациях в случае нарушения политики безопасности.

Актуальность разработки политик безопасности для отечественных компаний и организаций объясняется необходимостью формирования основ планирования информационной безопасности и управления ею на современном этапе. В настоящее время большинством российских компаний определены следующие приоритетные задачи развития и совершенствования своей деятельности:

- минимизация рисков бизнеса путем защиты своих интересов в информационной сфере;
- обеспечение безопасного, доверенного и адекватного управления предприятием;
- планирование и поддержка непрерывности бизнеса;
- повышение качества деятельности по обеспечению информационной безопасности;
- снижение издержек и повышение эффективности инвестиций в информационную безопасность;

- повышение уровня доверия к компании со стороны акционеров, потенциальных инвесторов, деловых партнеров, профессиональных участников рынка ценных бумаг, уполномоченных государственных органов и других заинтересованных сторон.

Успешное выполнение перечисленных задач в условиях воздействия внутренних и внешних факторов, а также действий конкурентов и злоумышленников проблематично. Это связано с возрастающей необходимостью повышения уровня информационной безопасности и недостаточной проработанностью политик информационной безопасности в отечественных компаниях. При разработке политик безопасности важно иметь в виду:

- в разрабатываемых политиках безопасности отечественных компаний необходимо учитывать в равной мере нормативные, экономические, технологические, технические и организационно-управленческие аспекты планирования информационной безопасности и управления ею. Только в этом случае можно достигнуть разумного баланса между стоимостью и эффективностью разрабатываемых правил политик безопасности;
- политики безопасности российских компаний не должны противоречить отечественной нормативной базе в области защиты информации в автоматизированных системах на территории РФ, в том числе нормативно-правовым документам (федеральным законам, указам Президента, постановлениям Правительства) и нормативно-техническим документам (государственным стандартам, руководящим документам Гостехкомиссии (ФСТЭК) России, Министерства обороны РФ и ФСБ РФ);
- при создании политик безопасности желательно учесть текущие реформы действующей Государственной системы стандартизации (ГСС) согласно Федеральному закону № 184-ФЗ «О техническом регулировании», рекомендации ГОСТ Р ИСО/МЭК 15408-2002, рекомендации функционального стандарта ГОСТ Р 51583-2000, описывающего этапность построения защищенных информационных систем, рекомендации функционального стандарта — документа ФСТЭК, под названием СТР-К, для выработки требований по технической защите конфиденциальной информации;
- при отражении в политиках безопасности нормативного аспекта рекомендуется следовать требованиям новой российской национальной системы стандартизации, основанной на системе технического регулирования в соответствии с рекомендациями Федерального закона № 184-ФЗ «О техническом регулировании». Это отвечает последним веяниям формирования в Российской Федерации технического законодательства, обеспечивающего выполнение Соглашений Всемирной торговой организации (ВТО) по техническим барьерам в торговле (ТБТ) и санитарным и фитосанитарным мерам (СФС) с учетом принципов нового подхода к технической регламентации в Европейском союзе (ЕС). Следование данным требованиям позволит устранить существующие технические

барьеры для отечественных компаний в торговле и обеспечении конкурентоспособности продукции;

- использование в политиках безопасности современных подходов и принципов обеспечения информационной безопасности, основанных на лучшем мировом и отечественном опыте (BS 7799-2:2002, ISO/IEC 17799:2005, ISO/IEC TR 13335, ISO/IEC 10181-7:1996, ISO/IEC 15288:2002, ISO/IEC TR 15443, BSI, CobiT, ITIL, ГОСТ Р ИСО/МЭК 15408-2002 и пр.), позволит выработать обоснованную парадигму планирования информационной безопасности и управления ею — концептуальную схему обеспечения информационной безопасности, а также требуемые модели постановки проблем в области управления информационной безопасностью и предложить разумно достаточные решения этих проблем. В частности, сформулировать основные принципы обеспечения информационной безопасности и доверия к ней, а также разработать требования по обеспечению информационной безопасности, адекватные целям и задачам развития бизнеса отечественных компаний;
- при отражении в разрабатываемых политиках безопасности отечественных компаний экономического подхода к планированию информационной безопасности и управлению ею на основе концепции управления рисками рекомендуется обратить внимание на методы: прикладного информационного анализа (Applied Information Economics, AIE); расчета потребительского индекса (Customer Index, CI); расчета добавленной экономической стоимости (Economic Value Added, EVA); определения исходной экономической стоимости (Economic Value Sourced, EVS); управления портфелем активов (Portfolio Management, PM); оценки действительных возможностей (Real Option Valuation, ROV); поддержки жизненного цикла искусственных систем (System Life Cycle Analysis, SLCA); расчета системы сбалансированных показателей (Balanced Scorecard, BSC); расчета совокупной стоимости владения (Total Cost of Ownership, TCO); функционально-стоимостного анализа (Activity Based Costing, ABC). В частности, для расчета расходной части на техническую архитектуру обеспечения информационной безопасности рекомендуется использовать метод совокупной стоимости владения (TCO), а для обоснования инвестиций в корпоративную систему защиты информации — методы ожидаемых потерь, оценки свойств системы безопасности, а также анализа дерева ошибок. При этом следует учитывать, что только метод ожидаемых потерь позволяет получить количественную оценку стоимости и выгод от контрмер безопасности;
- при разработке детальных технических политик безопасности отечественных компаний целесообразно воспользоваться стандартами BSI IT Protection Manual (www.bsi.de), NIST США серии 800 (www.nist.gov), CIS (www.cisecurity.org), NSA (www.nsa.gov). Это позволит определить облик технической архитектуры корпоративных систем защиты конфиденциальной информации российских компаний, в частности:

  - определить цели создания технической архитектуры корпоративной системы защиты информации;
  - разработать эффективную систему обеспечения информационной безопасности на основе управления информационными рисками;
  - рассчитать совокупности детализированных не только качественных, но и количественных показателей для оценки соответствия информационной безопасности заявленным целям;
  - выбрать и использовать требуемый инструментарий обеспечения информационной безопасности и оценки ее текущего состояния;
  - реализовать требуемые методики мониторинга и управления информационной безопасностью с обоснованной системой метрик и мер обеспечения информационной безопасности. Эти метрики и меры позволят объективно оценить защищенность информационных активов и управлять информационной безопасностью отечественных компаний;
- политики безопасности должны представлять собой законченные нормативные документы, содержащие единые нормы и требования по обеспечению информационной безопасности, обязательные для утверждения и применения соответствующими органами управления, руководством служб безопасности, руководством служб информационно-технологического обеспечения отечественных компаний.

По мнению авторов, книга является первым полным русскоязычным практическим руководством по вопросам разработки политик информационной безопасности в отечественных компаниях и организациях и отличается от других источников, преимущественно изданных за рубежом, тем, что в ней последовательно изложены все основные идеи, методы и способы практического решения: разработки, внедрения и поддержки политик безопасности в различных российских государственных и коммерческих организациях и структурах.

Эта книга может быть полезна следующим основным группам читателей:

- руководителям служб автоматизации (CIO) и служб информационной безопасности (CISO), ответственным за утверждение политик безопасности и организацию режима информационной безопасности, адекватного текущим целям и задачам бизнеса компании;
- внутренним и внешним аудиторам (CISA), которым приходится комплексно оценивать политики безопасности и текущее состояние организации режима информационной безопасности компании на соответствие некоторым требованиям корпоративных, национальных и международных стандартов, например ISO 15408, ISO 17799 (BS 7799-2), BSI, CobiT и пр.;
- менеджерам высшего эшелона управления компанией (TOP-менеджерам), которым приходится разрабатывать и внедрять политики безопасности в компании;
- администраторам безопасности, системным и сетевым администраторам, администраторам БД, которые отвечают за соблюдение правил безопасности в отечественных корпоративных информационных системах.

Книга также может использоваться в качестве учебного пособия студентами и аспирантами соответствующих технических специальностей, тем более что материалы многих глав основаны в том числе и на опыте преподавания авторов в Московском и Санкт-Петербургском госуниверситетах.
В книге четыре главы, которые посвящены:

- актуальности политик безопасности компании;
- лучшим практикам создания политик безопасности;
- рекомендациям международных стандартов по созданию политик безопасности;
- реализации политик безопасности.

В первой главе показано значение разработки политик информационной безопасности для создания эффективного режима информационной безопасности в российских компаниях и организациях. Доказывается, что одного только технического подхода для эффективной организации режима информационной безопасности компании недостаточно. Проведен анализ современного рынка средств защиты конфиденциальной информации, показаны «подводные» камни существующих технологий безопасности, а затем обоснована необходимость разработки политик безопасности в отечественных компаниях. Рассмотрены возможные постановки задач по разработке и реализации корпоративных политик безопасности, а также возможные способы решения названных задач.

Во второй главе рассмотрена так называемая лучшая практика (best practices) создания политик безопасности таких признанных технологических лидеров, как IBM, Sun Microsystems, Cisco Systems, Microsoft, Symantec, SANS и пр. Приводятся соответствующие практики и рекомендации для разработки политик безопасности в отечественных компаниях.

Третья глава содержит обзор сравнительно новых международных стандартов в области защиты информации, посвященных практическим вопросам разработки политик безопасности, в частности ISO/IEC 17799:2002 (BS 7799-1:2005), ISO/IEC 15408, ISO/IEC TR 13335, германского стандарта BSI, стандартов NIST США серии 800, стандартов и библиотек CobiT, ITIL, SAC, COSO, SAS 78/94.

В четвертой главе рассмотрена практика разработки политик безопасности. Приведены примеры задания детальных технических правил безопасности, а также настройки соответствующих корпоративных аппаратно-программных средств защиты конфиденциальной информации.

Книга написана доктором технических наук, CISO С.А. Петренко и CISSP В.А. Курбатовым, за исключением следующих ее частей:

- параграфа 3.7 — совместно с М. Пышкиным («Крок»);
- приложения 2 — © «Эрнст энд Янг (СНГ) Лимитед», 2003 г.;
- приложения 3 — совместно с доктором физико-математических наук, профессором В.А. Галатенко;
- приложения 5 — совместно с Е.М. Тереховой («АйТи»).

Авторы выражают глубокую благодарность докторам технических наук, профессорам А.Д. Хомоненко, Ю.И. Рыжикову, В.Н. Кустову, Б.Н. Соколову, А.Г. Ломако, кандидату технических наук, профессору В.В. Ковалеву за ценные советы и сделанные ими замечания по рукописи, устранение которых способствовало улучшению ее качества.

Благодарим также центр GIAC и институт SANS в лице Стивена Нортката (Stephen Northcutt)) и Эрика Коула (Eric Cole), общество ISC в лице CISSP Дмитрия Шепелявого, CISSP Чарльза Крессона Вуда (Charles Cresson Wood) и CISSP Шона Харриса (Shon Harris), ассоциацию ISACA в лице президента лондонского отделения CISA Чарльза Мансура (Charles Mansour), CISA Андрея Дроздова (KPMG) и CISA Александра Астахова, а также компанию Cisco Systems в лице CCIE Максима Мамаева, CCIE Михаила Кадера, CCIE Мерике Кэо (Merike Kaeo).

Авторы заранее выражают признательность всем читателям, которые готовы сообщить свое мнение о данной книге. Вы можете отправлять свои письма в издательство «АйТи-Пресс» Академии АйТи (itpress@it.ru).

Глава 1

Актуальность политик безопасности компании

Как правило, руководители отечественных предприятий рассматривают проблему защиты конфиденциальной информации преимущественно с технической точки зрения. При этом решение данной проблемы связывается с приобретением и настройкой соответствующих аппаратно-программных средств защиты информации. Однако для эффективной организации режима информационной безопасности компании этого недостаточно. Для того чтобы убедиться в этом, давайте сначала проведем анализ современного рынка средств защиты конфиденциальной информации, покажем «подводные» камни существующих технологий безопасности, а затем обоснуем необходимость разработки политик безопасности в отечественных компаниях. И наконец, рассмотрим возможные постановки задач по разработке и реализации корпоративных политик безопасности, а также способы решения названных задач.

1.1. Анализ отечественного рынка средств защиты информации

Современный рынок средств защиты информации можно условно разделить на две группы:

- средства защиты для госструктур, позволяющие выполнить требования нормативно-правовых документов (федеральных законов, указов Президента РФ, постановлений Правительства РФ), а также требования нормативно-технических документов (государственных стандартов, руководящих документов Гостехкомиссии (ФСТЭК) России, силовых ведомств РФ;
- средства защиты для коммерческих компаний и структур, позволяющие выполнить требования и рекомендации федеральных законов, указов Президента РФ, постановлений Правительства РФ, а также документа СТР-К Гостехкомиссии России, ГОСТ Р ИСО/МЭК 15408 и некоторых международных стандартов, главным образом ISO 17799: 2005.

Например, к защите конфиденциальной информации в органах исполнительной власти могут предъявляться следующие требования:

1. Выбор конкретного способа подключения к сети Интернет, в совокупности обеспечивающего межсетевое экранирование с целью управления доступом, фильтрации сетевых пакетов и трансляции сетевых адресов для сокрытия структуры внутренней сети, а также проведение анализа защищенности

интернет-узла, использование средств антивирусной защиты и централизованное управление, должен производиться на основании рекомендаций документа Гостехкомиссии РФ СТР-К.

2. Автоматизированные системы (АС) организации должны обеспечивать защиту информации от несанкционированного доступа (НСД) по классу «1Г» в соответствии с Руководящим документом Гостехкомиссии РФ «РД. Автоматизированные системы. Защита от НСД к информации. Классификация АС и требования по защите информации».
3. Средства вычислительной техники и программные средства АС должны удовлетворять требованиям четвертого класса РД Гостехкомиссии России «РД. Средства вычислительной техники. Защита от НСД к информации. Показатели защищенности от НСД к информации».
4. Программно-аппаратные средства межсетевого экранирования, применяемые для изоляции корпоративной сети от сетей общего пользования, должны удовлетворять требованиям «РД. Средства вычислительной техники. Межсетевые экраны. Защита от НСД к информации. Показатели защищенности от НСД к информации» по третьему классу защиты.
5. Информационные системы должны удовлетворять требованиям ГОСТ ИСО/ МЭК 15408 по защищенности информационых систем в рамках заданных профилей защиты.
6. Программно-аппаратные средства криптографической защиты конфиденциальной информации, в том числе используемые для создания виртуальных защищенных сетей (Virtual Privat Network, VPN), должны быть легитимны.
7. Обязательным является использование средств электронно-цифровой подписи (ЭЦП) для подтверждения подлинности документов.
8. Для использования персональных цифровых сертификатов и поддержки инфраструктуры открытых ключей, средств ЭЦП и шифрования необходимо создать легитимный удостоверяющий центр (систему удостоверяющих центров).
9. Политика информационной безопасности должна предусматривать обязательное включение в технические задания на создание коммуникационных и информационных систем требований информационной безопасности.
10. Должен быть регламентирован порядок ввода в эксплуатацию новых информационных систем, их аттестации по требованиям информационной безопасности.

Для выполнения перечисленных требований и надлежащей защиты конфиденциальной информации в госструктурах принято использовать сертифицированные средства, например средства защиты от несанкционированного доступа, межсетевые экраны и средства построения VPN, средства защиты информации от утечки за счет ПЭМИН и пр. В частности, для защиты информации от несанкционированного доступа рекомендуется использовать аппаратно-программные средства семейства Secret Net («Информзащита»), семейства Dallas Lock («Конфидент»), семейства «Аккорд» (ОКБ САПР), электронные замки «Соболь» («Информзащита»), USB-токены (Aladdin) и пр. Для защиты информации, передаваемой по открытым каналам связи,

рекомендованы аппаратно-программные межсетевые экраны с функциями организации VPN, например Firewall-1 (Check Point), «Застава» («Элвис+»), VipNet («Инфотекс»), «Континент» («Информзащита»), ФПСУ-IP (АМИКОН) и др.
Средства защиты информации для коммерческих структур более многообразны и включают в себя средства:

- управления обновлениями программных компонент,
- межсетевого экранирования,
- построения VPN,
- контроля доступа,
- обнаружения вторжений и аномалий,
- резервного копирования и архивирования,
- централизованного управления безопасностью,
- предотвращения вторжений на уровне серверов,
- аудита и мониторинга средств безопасности,
- контроля деятельности сотрудников в сети Интернет,
- анализа содержимого почтовых сообщений,
- анализа защищенности информационных систем,
- защиты от спама,
- защиты от атак класса «отказ в обслуживании»,
- контроля целостности,
- инфраструктуры открытых ключей,
- усиленной аутентификации и пр.

Дадим краткую характеристику перечисленным средствам защиты.

1.1.1. Средства управления обновлениями

Внедрение средств управления обновлениями программных компонент АС, например Microsoft Software Update Services, позволяет уменьшить объем интернет-трафика компании в целом, так как становится возможным организовать и контролировать необходимые обновления программных компонент АС компании с одной точки — выделенного внутреннего сервера. При этом предприятие получает следующие преимущества:

- уменьшаются расходы по оплате трафика;
- увеличивается надежность функционирования программных компонент АС;
- уменьшается время на техническую поддержку и сопровождение программных компонент АС;
- повышается защищенность АС в целом, в частности уменьшается количество инцидентов, связанных в вирусами и враждебными апплетами.

1.1.2. Средства межсетевого экранирования

Межсетевые экраны (МЭ) используются как средства защиты от несанкционированного доступа периметра сети и основных критичных компонент АС. Межсетевые экраны (МЭ) позволяют обеспечивать защиту на уровне доступа

к компонентам и сети в целом (MAC-адреса), на сетевом уровне (контроль IP-адресов), на транспортном уровне («машины состояний» основных протоколов), на прикладном уровне (proxy-системы).

Характеристика рынка МЭ представлена на рис. 1.1.

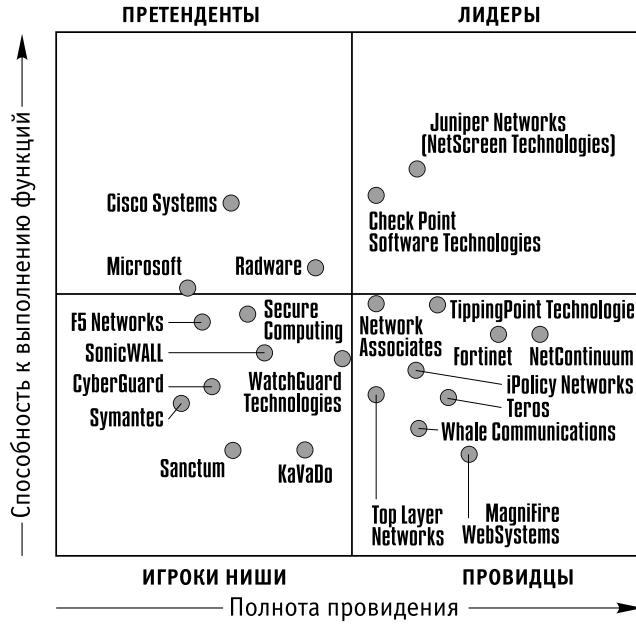

Рис. 1.1. Магический квадрант для Firewall
Источник: Gartner Group, 2004

1.1.3. Средства построения VPN

Средства построения виртуальных частных сетей (VPN) используются для организации защиты трафика данных, передаваемых по открытым каналам связи. При этом защита организуется на физическом уровне (защита кабелей, экранизация наводок), на сетевом уровне (например, шифрование трафика от компьютера до компьютера на основе протокола IPsec), на транспортном уровне (например, шифрование данных, передаваемых одним приложением другому приложению на другом компьютере, на основе протокола SSL), на прикладном уровне (например, шифрование данных самостоятельно приложением).

На рис. 1.2 представлена оценка рынка SSL VPNs.

1.1.4. Средства контроля доступа

Появление средств контроля доступа обусловлено необходимостью регламентировать доступ множества пользователей к приложениям и информационным

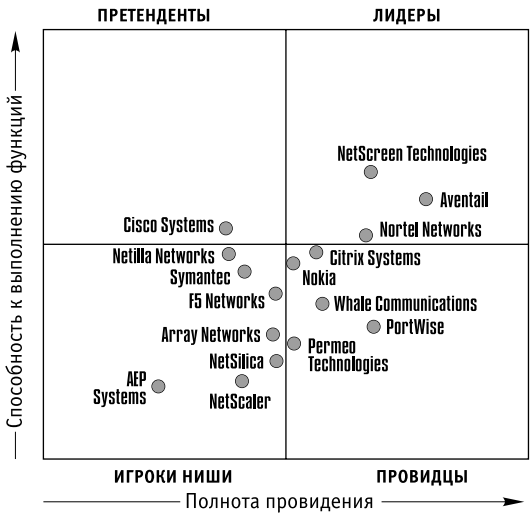

Рис. 1.2. Магический квадрант для SSL VPNs
Источник: Gartner Group, 2004

ресурсам компании. Данные средства осуществляют аутентификацию (точное опознание) подключающихся к АС пользователей и процессов, авторизацию (наделение определенными полномочиями) пользователей и процессов.

Состояние рынка средств контроля доступа представлено на рис. 1.3.

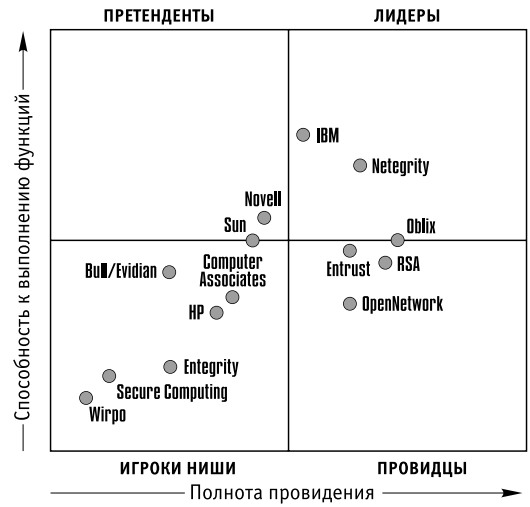

Рис. 1.3. Магический квадрант для Extranet Access Management
Источник: Gartner Group, 2004

1.1.5. Средства обнаружения вторжений и аномалий

Средства обнаружения вторжений (Intrusion Detection Systems, IDS) позволяют с помощью некоторого регламента проверок контролировать состояние безопасности корпоративной сети в реальном масштабе времени. Общий анализ рынка систем обнаружения вторжений и аномалий представлен на рис. 1.4.

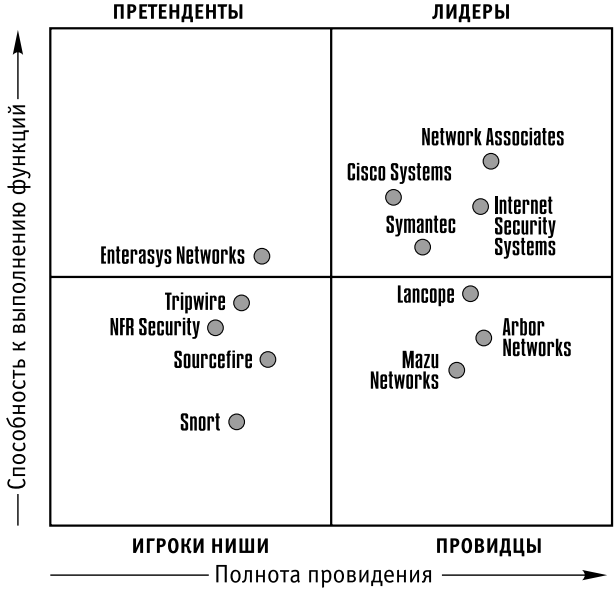

Рис. 1.4. Магический квадрант для IDA
Источник: Gartner Group, 2004

1.1.6. Средства резервного копирования и архивирования

Средства резервного копирования и архивирования применяются для обеспечения целостности хранилищ данных в случаях аппаратных и программных сбоев, ошибочных действий администраторов и пользователей, а также отказов средств вычислительной техники. Текущее состояние рынка систем резервирования представлено на рис. 1.5.

1.1.7. Средства централизованного управления безопасностью

Средства централизованного управления информационной безопасностью позволяют эффективно создавать, проверять и поддерживать технические политики безопасности программных компонент АС. Так, например, система централизованного управления Cisco Works VPN/Security Management Solution позволяет контролировать и управлять политиками безопасности следующих устройств безопасности компании Cisco Systems:

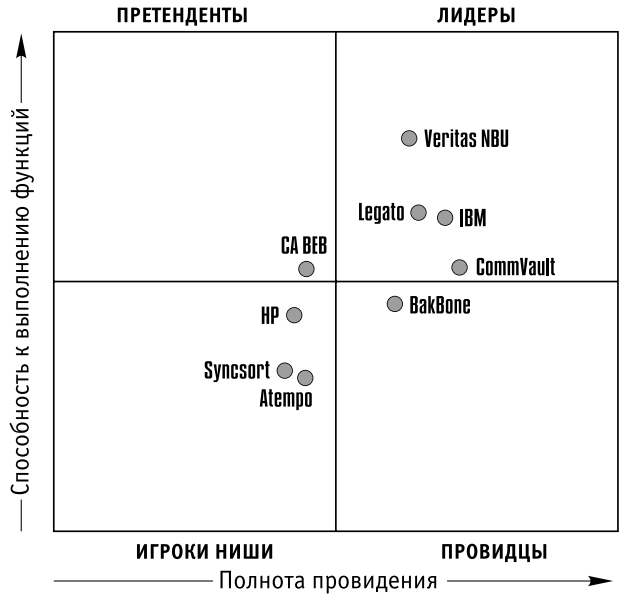

Рис. 1.5. Магический квадрант для средств резервирования
Источник: Gartner Group, 2004

- Cisco PIX Firewall,
- Cisco VPN Router,
- Cisco IDS 4200,
- Cisco Security Agent.

1.1.8. Средства предотвращения вторжений на уровне серверов

Так как серверы компании обычно являются основной целью атак злоумышленников (на них обрабатывается основная часть конфиденциальной информации компании), то необходимо использовать средства предотвращения вторжений на уровне серверов, например Cisco Security Agent. Другие возможные решения представлены на рис. 1.6.

1.1.9. Средства мониторинга безопасности

Большое количество средств обеспечения информационной безопасности (межсетевые экраны, системы обнаружения вторжений, маршрутизаторы, средства создания виртуальных частных сетей, журналы безопасности серверов, системы аутентификации, средства антивирусной защиты и т.д.) генерирует огромное количество сообщений. Для успешного мониторинга и управления этими средствами рекомендуется использовать соответствующие средства аудита безопасности, например Cisco Security Information Management Solution (net-Forensics). Другие возможные решения представлены на рис. 1.7.