Сергей Александрович Петренко Владимир Анатольевич Курбатов
Политики безопасности компании при работе в Интернет

Сергей Александрович Петренко, Владимир Анатольевич Курбатов
Политики информационной безопасности

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 (СЮ) 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

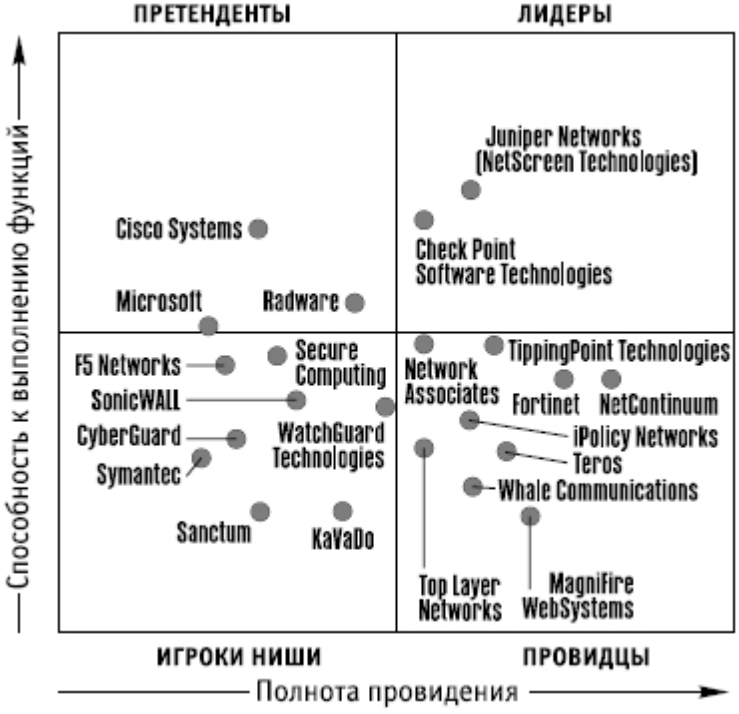
Внедрение средств управления обновлениями программных компонент АС, например Microsoft Software Update Services, позволяет уменьшить объем интернет-трафика компании в целом, так как становится возможным организовать и контролировать необходимые обновления программных компонент АС компании с одной точки – 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.

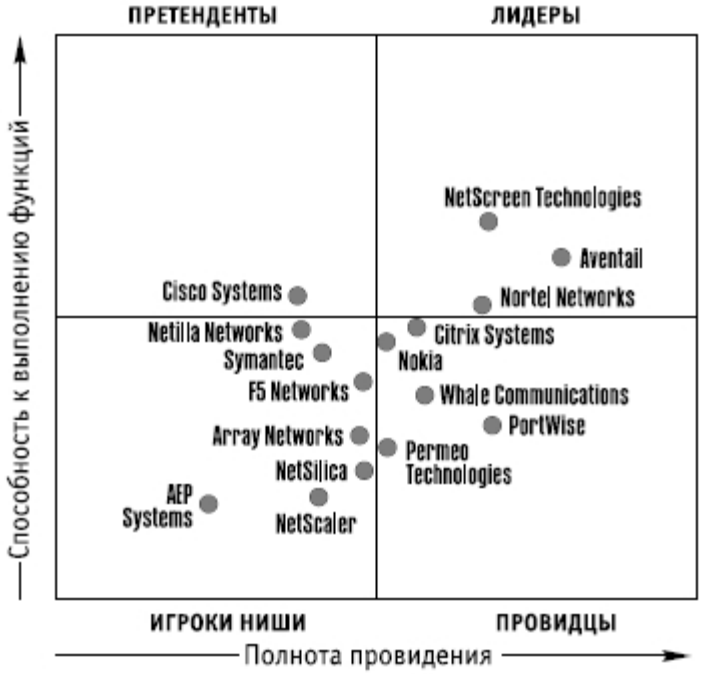


...

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

1.1.3. Средства построенияVPN

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.



...

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

1.1.4. Средства контроля доступа

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

...

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

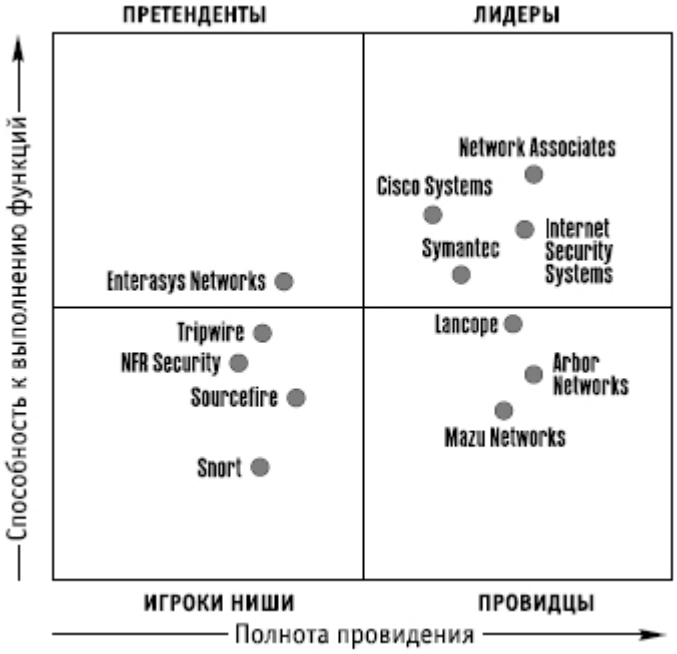
1.1.7. Средства централизованного управления безопасностью

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:

- 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.



...

Рис. 1.6. Магический квадрант для IDS
Источник: Gartner Group, 2004

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.

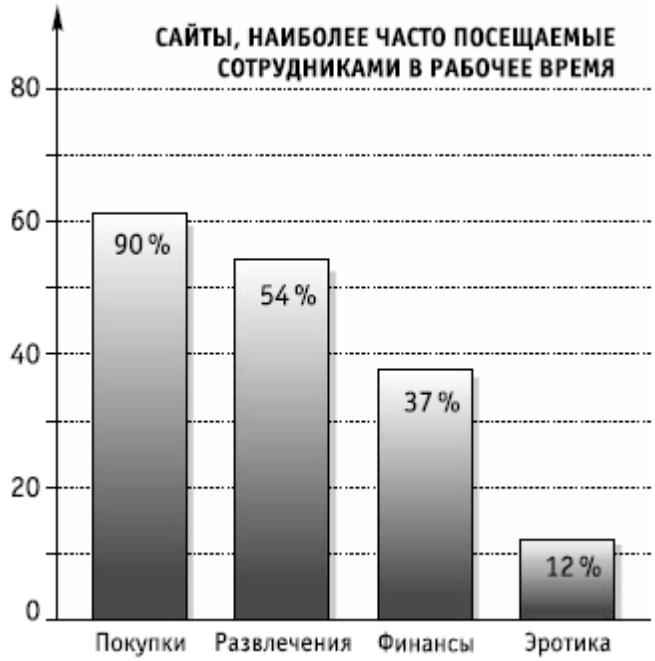
...

Рис. 1.7. Магический квадрант для управления информационной безопасностью
Источник: Gartner Group, 2004

1.1.10. Средства контроля деятельности сотрудников в Интернете

В настоящее время одной из серьезных проблем в работе отечественных служб безопасности является предотвращение попыток использования интернет-ресурсов компании в личных целей (загрузка видео, аудио, картинок, нелицензионного программного обеспечения). Нецелевое использование Интернета приводит к потере продуктивности сотрудников компании приблизительно на 30–40 % (см. рис. 1.8).

Для предупреждения подобных действий рекомендуется применять соответствующие средства, например Websense, которые позволяют анализировать и формировать отчеты по использованию сотрудниками компании ресурсов Интернета и программного обеспечения на рабочих местах, а также проводить анализ сетевой активности и пропускной способности сети компании в целом.



...

Рис. 1.8. Статистика потерь продуктивности сотрудников компании
Источник: Surfcontrol

1.1.11. Средства анализа содержимого почтовых сообщений

Средства анализа содержимого почтовых сообщений предназначены для обнаружения и предотвращения передачи конфиденциальной информации с помощью корпоративной электронной почты. В настоящее время на отечественном рынке средств защиты информации имеются такие системы, в частности «Дозор-Джет» компании «Инфосистемы Джет» и MAILsweeper компании Clearswift (поставляется «Информзащитой»).

1.1.12. Средства анализа защищенности

Анализ защищенности АС является одним из ключевых аспектов построения надежной системы обеспечения информационной безопасности предприятия и основан на применении сканеров безопасности. На рынке коммерческих сканеров можно выделить четыре основные

группы производителей сканеров – поставщиков решений согласно 7-уровневой модели OSI (сверху вниз) (см. рис. 1.9):

- прикладного уровня – 1-й уровень;
- представительного уровня – 2-й уровень;
- сеансового и ниже уровней – 3-5-й уровни;
- сетевого уровня – 6-7-й уровни.

...

Рис. 1.9. Классификация сканеров по уровням модели OSI

Первая группа производителей (Application Security, Pentest, ISS Database Scanner, NGS Squirrel и пр.) предлагает сканеры прикладного уровня (приложения, распределенные БД, системы электронного документооборота, ERP и пр.). Среди них выделяется компания Application Security (www.appsecinc.com). которая предлагает решения для Oracle, MS SQL, Sybase, DB2 IBM, MySQL, Lotus Notes, то есть практически всех основных лидеров и поставщиков решений электронного оборота, ERP, CRM.

Вторая группа (KAVADO, Sanctum, SPI Dynamics) предлагает услуги и продукты для сканирования представительного уровня.

Третья группа (Foundstone, ISS, XSpider, eEye Retina, Nessus, NetlQ и пр.) предлагает решения для 3-5-го уровня модели OSI. Популярны в России сканеры семейства ISS, а также сканеры Nessus, XSpider, eEye Retina.

Четвертая группа (Network Associates, Symantec) предлагает решения преимущественно для 6-7-го уровня модели OSI.

Основной особенностью наиболее продаваемых и используемых коммерческих сканеров является возможность как минимум еженедельно обновлять базы данных уязвимостей путем взаимодействия с крупнейшими центрами по сбору новых уязвимостей и с ведущими производителями сетевого оборудования и программного обеспечения.

1.1.13. Средства защиты от спама

Согласно статистическим данным за 2004 год, в Российской Федерации объем спама в сообщениях электронной почты достиг 60 %. Сотрудникам приходится тратить свое рабочее время, а это деньги предприятия, на просмотр таких сообщений, их удаление, настройку правил по нейтрализации. Спам также содержит программы типа «Троянский конь», программы-шпионы (spyware) и вирусы. Таким образом, предприятию наносится значительный ущерб. Для предотвращения получения сотрудниками сообщений, содержащих спам, можно воспользоваться одним из продуктов следующих фирм: Symantec (использует технологию фирмы Brightmail), Trend Micro (использует технологию фирмы

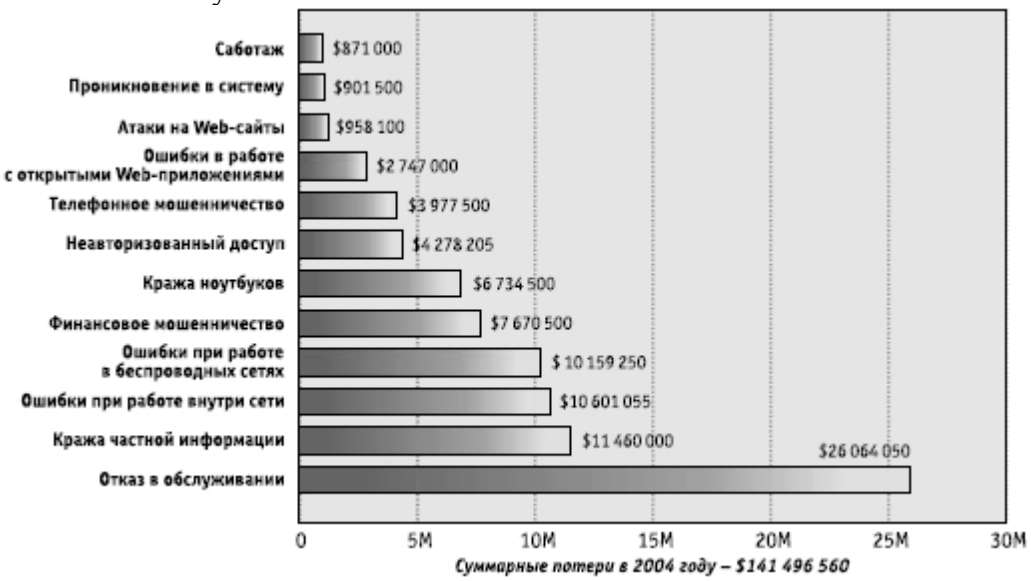
Postini) или «Лаборатории Касперского» (см. рис. 1.10).

...

Рис. 1.10. Магический квадрант для средств защиты от спама
Источник: Gartner Group, 2004

1.1.14. Средства защиты от атак класса «отказ в обслуживании»

В связи с тем что атаки класса «отказ в обслуживании» приносят значительные убытки отечественным и западным компаниям (см. рис. 1.11), можно воспользоваться специальными средствами защиты, например продуктами компании Riverhead, приобретенной компанией Cisco Systems. Сейчас продукты Riverhead продаются под торговой маркой Cisco Guard XT 5650 и Cisco Traffic Anomaly Detector XT 5600.



...

Рис. 1.11. Наиболее опасные атаки в 2004 году
Источник: Отчет CS/FBI, 2004

1.1.15. Средства контроля целостности

Внесение некорректного изменения в конфигурацию сервера или маршрутизатора может привести к выходу из строя необходимого сервиса или целой сети. Очень важно предупредить и отследить несанкционированные изменения. Для быстрого реагирования на такую ситуацию нужно иметь средство отслеживания всех производимых изменений. Данную возможность предоставляет, например, серия продуктов компании Tripwire.

1.1.16. Средства инфраструктуры открытых ключей

Внедрение инфраструктуры открытых ключей очень трудоемкая задача, требующая тщательной проработки и анализа. При решении этой задачи можно воспользоваться продуктами компании RSA Security (Keon) и отечественной компании «КриптоПро» («Криптопровайдер»), При этом хранение сертификатов осуществлять на аппаратных устройствах Aladdin USB eToken.

1.1.17. Средства усиленной аутентификации

На критичных элементах сетевой инфраструктуры следует реализовать систему усиленной аутентификации, например на базе продукта Cisco Secure Access Control Server с использованием системы однократных паролей RSA Security SecurlD.

1.2. Характеристика зрелости технологий защиты информации

Практика обеспечения защиты информации в отечественных компаниях насыщена инцидентами. Анализ этих инцидентов свидетельствует о том, что одних только технических средств защиты недостаточно. В чем причины такого положения дел?

Во-первых, появление новых сетевых «червей», пусть даже в день опубликования сообщения об очередной уязвимости приложений и/или операционных систем, практически сводит на нет все усилия поставщиков антивирусного программного обеспечения. Они просто не успевают выпустить обновления для своих антивирусов, так как необходимо время на исследование нового вируса, разработку и публикацию соответствующей сигнатуры, а потребителям антивирусов необходимо время на тестирование и установку обновлений в корпоративной сети. За этот период корпоративная информационная система уже может быть выведена из строя. Кроме того, большинство конфигураций операционных систем установлено по умолчанию, что способствует быстрому распространению сетевых «червей». Например, в 2003–2004 годах примерно 90 % инцидентов было вызвано атаками сетевых «червей». Более того, теоретически доказано, что множество всех вирусов не поддается перечислению и что нельзя создать универсальный детектор, способный отличить «чистую» программу от зараженной (Л. Адлеман и Ф. Коэн).

Во-вторых, операционные системы, как бы ни заявляли разработчики о своих новых успехах, все равно остаются самым слабым местом в корпоративной системе защиты информации. Согласно исследованиям университета Carnegie-Mellon, на каждую 1 тыс. строк кода программы приходится от 5 до 15 ошибок. Можно посчитать, сколько ошибок потенциально содержит каждая из перечисленных операционных систем:

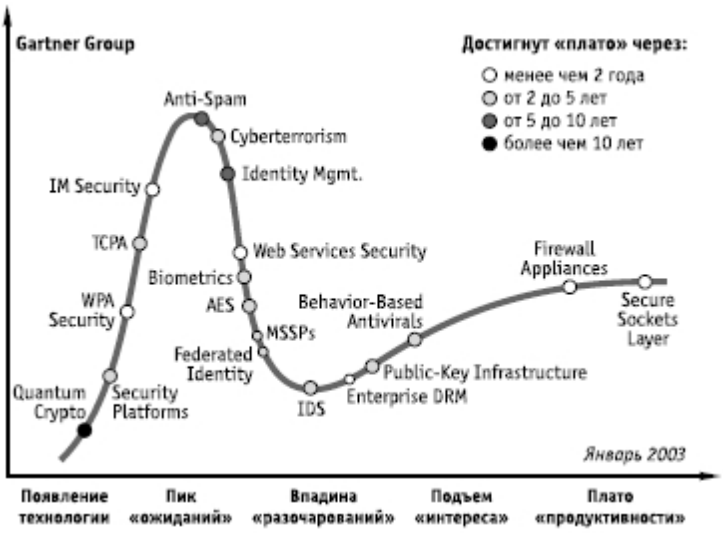
- Windows 2000 – 35–60 млн. строк кода;
- Windows XP – 45 млн. строк кода;
- Debian GNU/Linux 2.2-55 млн. строк кода;
- Linux Red Hat – 30 млн. строк кода.

В-третьих, по данным независимых аналитических центров на начало 2005 года, системы обнаружения вторжений (IDS) обнаруживают не более 14–18 % всех осуществляемых атак. При этом большинство систем обнаружения вторжений построены на

принципах обнаружения на основе сигнатур атак (см. табл. 1.1), то есть обладают теми же недостатками, что и антивирусное программное обеспечение. Таблица 1.1. Характеристика современных методов обнаружения вторжений и аномалий в сетях TCP/IP

Методы обнаружения вторжений и аномалий	Достоинства	Ограничения	Реализация
1. Корреляционные методы	Способность обнаруживать не заложенные в базу аномалии	Высокий уровень ложных срабатываний	
1.1. Статические профили	Специфичных преимуществ нет	Неспособность адаптироваться к валидным изменениям сетевого трафика	NIDES (исследовательский проект, демонстрационный прототип IDS)
1.2. Динамические профили	Пониженный уровень ложных срабатываний за счет адаптации	Возможность умышленного «обхода» за счет плавного целенаправленного изменения параметров трафика	EMERALD (исследовательский проект, демонстрационный прототип IDS), работы E.Eskin (исслед.)
1.3. Профили на основе нейросетей	Пониженный уровень ложных срабатываний за счет адаптации Повышение качества обнаружения за счет элементов искусственного интеллекта	Высокий уровень ложных срабатываний для некоторых классов атак (не укладывающихся в нейросетевую модель обнаружения)	Работы E.Moreira (исслед.)
2. Сигнатурные методы	Нулевой уровень ложных срабатываний	Вероятность обнаружения аномалии, не заложенной в базу сигнатур, очень низка	
2.1. Поиск по полной базе шаблонов	Специфичных преимуществ нет	Специфичных недостатков нет	RealSecure (промышленный прототип IDS), CiscoIDS (промышленный прототип IDS)
2.2. База шаблонов с обратной связью	Повышение качества и скорости обнаружения путем анализа истории атак	Специфичных недостатков нет	Snort (промышленный прототип IDS)
2.3. Граф переходов, соответствующий атаке	Построение («поверхностной») модели атаки и атакуемой системы с целью определения реализуемости атаки и возможного ущерба от нее	Увеличение уровня ложного пропуска для некоторых классов атак (внесенных в базу графов сигнатур)	BRO (исследовательский проект, демонстрационный прототип IDS)
3. Инвариантные методы	Способность обнаруживать новые (отсутствующие в базах сигнатур) типы аномалий при нулевом уровне ложных срабатываний	Трудность разработки представительных моделей межсетевого взаимодействия	
3.1. Инвариантные методы обнаружения вторжений на основе инвариантов подобия	Более достоверны по сравнению с сигнатурными и менее трудоемки по сравнению с корреляционными методами обнаружения вторжений и аномалий	Не обнаруживают атаки, не вызывающие нарушения семантической корректности межсетевого взаимодействия	Работы Петренко С.А., Ковалева В.В., Беляева А.В. (исследовательский проект, демонстрационный прототип IDS)

В-четвертых, системы контроля доступа на основе биометрических параметров тоже не идеальны. Отпечатки пальцев не настолько уникальны, как утверждают производители: существует вероятность 0,1, что постороннее лицо будет идентифицироваться как имеющее право доступа. Аналогичные выводы можно сделать практически по каждой технологии защиты информации. Наглядно оценки зрелости современных технологий защиты информации представлены на диаграмме аналитической компании Gartner Group (см. рис. 1.12).

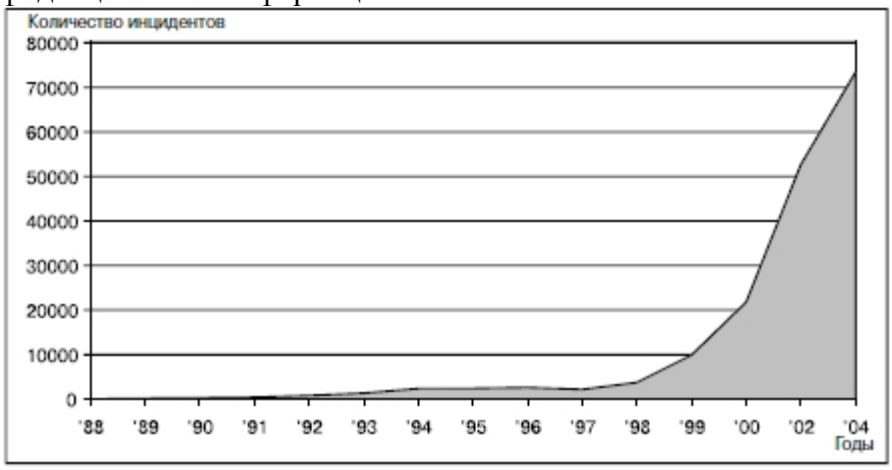


...

Рис. 1.12. Оценки зрелости технологий защиты информации

В целом анализ инцидентов безопасности начиная с 2001 года и по настоящее время свидетельствует о ежегодном росте их числа в среднем на 200–300 % (см. рис. 1.13). При этом, согласно исследованиям Института компьютерной безопасности США, в 2004 году из 750 млн. долларов, потерянных компаниями из-за инцидентов в области информационной безопасности, более 500 млн. долларов убытков были обусловлены следующими видами инцидентов:

- неавторизованный доступ к ресурсам внутренних сотрудников,
- неразрешенное использование Интернета,
- саботаж,
- сканирование и взлом систем,
- кража конфиденциальной информации.



...

Рис. 1.13. Статистика инцидентов безопасности

Анализ статистики инцидентов в АС отечественных предприятий показывает, что для российских компаний наиболее злободневны вопросы нейтрализации следующих основных

угроз (см. табл. 1.2)

Таблица 1.2. Актуальные угрозы безопасности для отечественных АС

Характер угрозы	% случаев	Требования к ИТС по отражению атаки
Умышленные нападения (теракты)	17	Катастрофоустойчивость
Пожары	17	Катастрофоустойчивость
Ураганы	14	Катастрофоустойчивость
Землетрясения	11	Катастрофоустойчивость
Отключения электроэнергии	10	Отказоустойчивость
Выход из строя программ	9	Отказоустойчивость
Наводнения	7	Катастрофоустойчивость
Выход из строя техники	5	Отказоустойчивость
Персонал + Прочие	10	Политика безопасности

В результате, по данным Gartner Group, проблема защиты информации выделилась среди других проблем совершенствования информационных технологий и стала одной из приоритетных проблем развития отечественных компаний и предприятий (см. рис. 1.14).

...

Рис. 1.14. Текущие проблемы развития информационных технологий

Как эффективно подойти к решению проблемы защиты информации? По-видимому, сначала необходимо разработать действенную политику информационной безопасности компании.

1.3. Основные причины создания политик безопасности

Любую отечественную компанию можно сравнить с небольшим государством. И если в каждом государстве существует законодательство, регламентирующее деятельность граждан, то в компании роль законов выполняют политики безопасности. За нарушение законов государства граждане несут ответственность, нарушение политик безопасности сотрудниками компании также влечет за собой ответственность.

Политики информационной безопасности определяют стратегию и тактику построения корпоративной системы защиты информации. В российской терминологии документ, определяющий стратегию, часто называют концепцией, а документ определяющий тактику, – политикой. На Западе принято создавать единый документ, включающий в себя стратегию и тактику защиты. Политики безопасности компании являются основой для разработки целого

ряда документов по обеспечению безопасности: стандартов, руководств, процедур, практик, регламентов, должностных инструкций и пр.

Что должно мотивировать отечественные предприятия и компании разрабатывать политики информационной безопасности? К таким мотивам относятся:

выполнение требований руководства компании;

Как правило, руководство компании проявляет внимание к проблемам информационной безопасности под воздействием «фактора страха» или после нескольких серьезных инцидентов, повлекших за собой остановку или замедление работы компании. Например, в результате вирусной атаки или атаки «отказ в обслуживании», разглашения конфиденциальной информации или кражи компьютеров с ценной информацией.

выполнение требований российской нормативной базы в области защиты информации;

Каждая компания обладает информацией, представляющей некоторую ценность, и по понятным причинам она не желала бы ее разглашения. Политики информационной безопасности позволяют определить правила, в соответствии с которыми информация будет отнесена к категории коммерческой или служебной тайны. Это позволит компании юридически защитить информацию (ст. 139 Гражданского кодекса и Закон о коммерческой тайне). В зависимости от сферы действия компании она должна выполнять требования существующего законодательства, применимого к ее отрасли. Например, банки в соответствии со ст. 857 Гражданского кодекса должны гарантировать защиту банковской тайны клиентов. Страховые компании должны защищать тайну страхования (ст. 946 Гражданского кодекса) и т. д. Кроме этого, в соответствии с Указом

Президента РФ № 188 от 06.03.97 «Об утверждении перечня сведений конфиденциального характера» компании должны обеспечивать защиту персональных данных сотрудников.

В целом автоматизированные системы отечественных компаний должны удовлетворять требованиям российской нормативной базы в области защиты информации, нормативно-правовым документам (федеральным законам, указам Президента, постановлениям Правительства) и нормативно-техническим документам (государственным стандартам, руководящим документам Гостехкомиссии (ФСТЭК) России, отраслевым и ведомственным стандартам). При этом после принятия и вступления в силу Федерального закона «О техническом регулировании», а также ГОСТ Р ИСО/МЭК 15408 статус ряда нормативных документов (государственных стандартов, отраслевых стандартов, стандартов организаций и др.) изменился. Государственные стандарты Российской Федерации из основного инструмента технического регулирования стали трансформироваться в российские национальные стандарты, требования которых стали носить добровольный характер. Обязательные требования стали устанавливаться в технических регламентах.

выполнение требований клиентов и партнеров;

Клиенты и партнеры компании часто желают получить некоторые гарантии того, что их конфиденциальная информация защищена надлежащим образом и могут потребовать юридического подтверждения этого в контрактах. В этом случае политики информационной безопасности компании и являются доказательством предоставления подобных гарантий, так как в политиках безопасности декларируются намерения компании относительно качества обеспечения информационной безопасности. Интересно, что партнеров по бизнесу и клиентов компании, как правило, интересуют именно эти «намерения», а не технические средства, с помощью которых они могут быть достигнуты.

подготовка к сертификации по ISO 9001, ISO 15408 и ISO 17799;

Сертификация по одному из вышеперечисленных стандартов подтверждает необходимый уровень обеспечения информационной безопасности компании. В настоящее время фокус создания продуктов и услуг смещается в страны с дешевой рабочей силой, и одним из доказательств того, что компании этих стран смогут адекватно защитить передаваемую информацию производителей, является сертификация на соответствие

требованиям стандартов по информационной безопасности, например ISO 17799 (BS 7799-2). На сайте www.xisec.com ведется реестр компаний, подтвердивших свое соответствие требованиям этого стандарта. Список увеличивается примерно на 50-100 компаний ежемесячно, что показывает возросшее внимание к этой теме.

устранение замечаний аудиторов;

Любая внешняя аудиторская проверка обращает внимание на необходимость защищенности бизнес-процессов компании, в том числе особое внимание уделяется наличию политик информационной безопасности.

получение конкурентного преимущества на рынке;

Правильно разработанные и реализованные политики безопасности позволяют увеличить время доступности и коэффициент готовности сервисов компании. Таким образом увеличивается общая жизнеспособность компании и обеспечивается непрерывность бизнеса. По словам ведущих аналитиков Gartner Group, «обеспечение информационной безопасности является ключевым моментом устойчивости и непрерывности бизнеса».

демонстрация заинтересованности руководства компании;

Вовлечение руководства в организацию режима информационной безопасности компании значительно увеличивает приоритет безопасности, что положительно сказывается на общем уровне безопасности компании. Без демонстрации заинтересованности руководства компании сотрудники не станут воспринимать политики информационной безопасности всерьез. Цель любой политики безопасности – разъяснение и доведение позиции руководства в соответствии с принципами безопасности и бизнес-целями компании.

создание корпоративной культуры безопасности;

«Образно организацию режима информационной безопасности можно сравнить с цепью: рвется там, где самое тонкое звено цепи» (Б. Шнайер). Сотрудники являются как самым сильным, так одновременно и самым слабым звеном в обеспечении информационной безопасности. Необходимо донести до сотрудников мысль о том, что «обеспечение информационной безопасности – обязанность всех сотрудников». Это достигается путем введения процедуры ознакомления с требованиями политик безопасности и подписания соответствующего документа о том, что сотрудник ознакомлен, ему понятны все требования политик и он обязуется их выполнять. Политики безопасности позволяют ввести требования по поддержанию необходимого уровня безопасности в перечень обязанностей каждого сотрудника. В процессе выполнения трудовых обязанностей для сотрудников необходимо периодически проводить ознакомление с вопросами обеспечения информационной безопасности и обучение. Критически важным условием для успеха в области обеспечения информационной безопасности компании становится создание в компании атмосферы, благоприятной для создания и поддержания высокого приоритета информационной безопасности. Чем крупнее компания, тем более важной становится информационная поддержка сотрудников по вопросам безопасности.

уменьшение стоимости страхования;

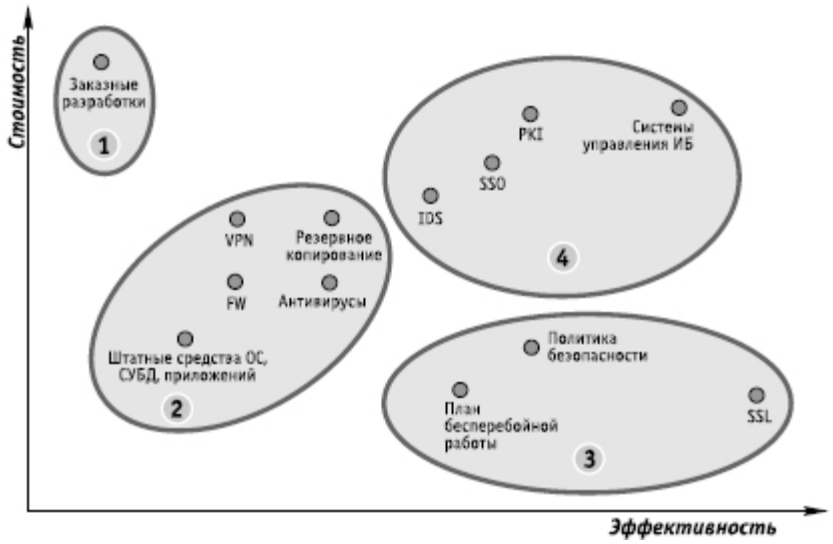
Страхование – важная составляющая управления информационными рисками. Наличие политик информационной безопасности является необходимым и обязательным условием страхования. В России уже появились фирмы, предлагающие страховать информационные риски, например «Ингосстрах» и «РОСНО». Стоимость страхования страховая компания определяет путем проведения аудита информационной безопасности независимой компанией, специализирующейся в этой области. Например, компания «Центр финансовых технологий» (интернет-проект Faktura.ru) заключила договор комплексного страхования информационных рисков с «Ингосстрахом». Сумма ответственности составила 500 тыс. долларов. Аудит проводила компания ОАО «Элвис+».

экономическая целесообразность;

По рекомендациям ведущих компаний в области безопасности, от 60 до 80 % всех усилий по обеспечению безопасности должны быть направлены на разработку политик безопасности и сопутствующих документов. Вы спросите, почему?

Как видно из диаграммы (рис. 1.15), разработанной Стивеном Россом (Delloitte & Touche), каждая политика безопасности может являться как самым дешевым, так и одновременно самым эффективным способом обеспечения информационной безопасности.

хорошая бизнес-практика.



...

Рис. 1.15. Оценка эффективности и цены решений в области защиты информации

Наличие политик информационной безопасности является правилом хорошего тона. В опросе, проведенном в Великобритании компанией PriceWaterhouseCoopers в 2002 году, 67 % компаний назвали именно эту причину создания политик информационной безопасности.

Даже такие высокотехнологичные компании, как Cisco, заявляют, что правильно сформулированная политика информационной безопасности лучше технических средств обеспечения информационной безопасности. Подход Cisco к проблемам создания защищенной инфраструктуры (рис. 1.16) показывает, что именно политики информационной безопасности являются краеугольным камнем, вокруг которого строится вся система обеспечения безопасности.

...

Рис. 1.16. Подход Cisco к созданию политик безопасности

Таким образом, политики обеспечения информационной безопасности необходимы для

успешной организации режима информационной безопасности любой отечественной компании. Политики безопасности минимизируют влияние «человеческого фактора» и недостатки существующих технологий защиты информации. Кроме того, политики безопасности дисциплинируют сотрудников компании и позволяют создать корпоративную культуру безопасности.

1.4. Как разработать политики безопасности?

Прежде чем мы начнем искать ответ на поставленный вопрос, поговорим немного о проблеме доверия.

1.4.1. Кому и что доверять

От правильного выбора уровня доверия к сотрудникам зависит успех или неудача реализации политики безопасности компании. При этом слишком большой уровень доверия может привести к возникновению проблем в области безопасности, а слишком малый – заметно затруднить работу сотрудника, вызвать у него недоверие и даже привести к увольнению. Насколько можно доверять сотрудникам компании? Обычно используют следующие модели доверия:

- *доверять всем и всегда* – самая простая модель доверия, но, к сожалению, непрактичная;
- *не доверять никому и никогда* – самая ограниченная модель доверия и также непрактичная;
- *доверять избранным на время* – модель доверия подразумевает определение разного уровня доверия на определенное время. При этом доступ к информационным ресурсам компании предоставляется по необходимости для выполнения служебных обязанностей, а средства контроля доступа используются для проверки уровня доверия к сотрудникам компании.

Вряд ли существует компания, в которой следуют модели доверия «доверять всем и всегда». В сегодняшнем мире это нереально. То же самое относится и ко второй модели – «не доверять никому и никогда». Поэтому самая реалистичная модель доверия – «доверять некоторым из сотрудников компании на время». 1.4.2. Трудности внедрения политик безопасности

Опыт создания политик безопасности авторами показывает, что внедрение политики безопасности часто приводит к возникновению напряженности во взаимоотношениях между сотрудниками компании. Это в основном связано с тем, что сотрудники часто стараются не следовать каким-либо правилам безопасности, так как не хотят себя ограничивать в своих действиях. Другая причина в том, что каждый сотрудник имеет свое представление (не обязательно солидарное с принятой в компании политикой безопасности) о необходимости и способах организации режима информационной безопасности в компании. Например, сотрудники контура сбыта заинтересованы в оперативном исполнении своих обязанностей без каких-либо задержек, связанных с применением средств защиты информации. Персонал службы поддержки часто заинтересован только в простоте эксплуатации администрируемых ими информационных систем. TOP-менеджмент компании заинтересован прежде всего в оптимизации затрат и уменьшении общей стоимости владения (TCO) корпоративной системы защиты информации. Получить одобрение всех положений политики безопасности у перечисленных групп сотрудников компании – трудная и практически неосуществимая задача. Поэтому лучше всего попробовать достигнуть некоторого компромисса.

1.4.3. Кто заинтересован в политиках безопасности?

Политики безопасности затрагивают практически каждого сотрудника компании. Сотрудники службы поддержки будут осуществлять и поддерживать правила безопасности компании. Менеджеры заинтересованы в обеспечении безопасности информации для достижения своих целей. Юристы компании и аудиторы заинтересованы в поддержании репутации компании и предоставлении определенных гарантий безопасности клиентам и

партнерам компании. Рядовых сотрудников компании политики безопасности затрагивают больше всего, поскольку правила безопасности накладывают ряд ограничений на поведение сотрудников и затрудняют выполнение работы.

1.4.4. Состав группы по разработке политик безопасности

Буклет SAGE «A Guide to Developing Computing Policy Documents» рекомендует следующий состав рабочей группы по разработке политик безопасности:

• член совета директоров;

• представитель руководства компании (CEO, финансовый директор, директор по развитию);

• СЮ (директор службы автоматизации);

• CISO (директор по информационной безопасности);

• аналитик службы безопасности;

• аналитик ИТ-службы;

• представитель юридического отдела;

• представитель от пользователей;

• технический писатель.

Численность группы по разработке политик безопасности будет зависеть от широты и глубины проработки политик безопасности. Например, разработка политик безопасности для офисной сети в 40–50 узлов может занять один человекомесяц. 1.4.5. Процесс разработки политик безопасности

Если это возможно, то о том, что разрабатывается новая политика информационной безопасности компании, необходимо уведомить сотрудников заранее. До начала внедрения новой политики безопасности желательно предоставить сотрудникам текст политики на одну-две недели для ознакомления и внесения поправок и комментариев. Также надо учитывать, что без прав нет обязанностей, то есть сотрудники, на которых распространяются правила безопасности, должны обладать всеми необходимыми полномочиями для того, чтобы выполнять эти правила.

1.4.6. Основные требования к политике безопасности

В идеале политика безопасности должна быть реалистичной и выполнимой, краткой и понятной, а также не приводить к существенному снижению общей производительности бизнес-подразделений компании. Политика безопасности должна содержать основные цели и задачи организации режима информационной безопасности, четкое описание области действия, а также указывать на ответственных и их обязанности. Например, по мнению специалистов Cisco, желательно, чтобы описание политики безопасности занимало не более двух (максимум пяти) страниц текста. При этом важно учитывать, как политика безопасности будет влиять на уже существующие информационные системы компании. Как только политика утверждена, она должна быть представлена сотрудникам компании для ознакомления. Наконец, политику безопасности необходимо пересматривать ежегодно, чтобы отражать текущие изменения в развитии бизнеса компании.

1.4.7. Уровень средств безопасности

Хорошо написанные политики безопасности компании должны позволять балансировать между достигаемым уровнем безопасности и получаемым уровнем производительности корпоративных информационных систем компании. Одна из основных целей политики безопасности состоит в том, чтобы обосновать и внедрить средства защиты информации, адекватные целям и задачам бизнеса. Выбор необходимых средств защиты информации для определенной политики безопасности не всегда понятен и легко определяем. Здесь решающую роль играют необходимость организации режима информационной безопасности, а также бизнес-культура компании. При этом если правила политики безопасности слишком ограничительны или слишком жестки, для того чтобы их внедрять и соответствовать им в дальнейшем, то либо они будут игнорироваться, либо сотрудники компании найдут способ обойти средства безопасности.

1.4.8. Примеры политик безопасности

В настоящее время ряд ведущих компаний в области безопасности выделяют следующие политики:

- допустимого шифрования,
- допустимого использования,
- аудита безопасности,
- оценки рисков,
- классификации данных,
- управления паролями,
- использования ноутбуков,
- построения демилитаризованной зоны (DMZ),
- построения экстранет,
- безопасности рабочих станций и серверов,
- антивирусной защиты,
- безопасности маршрутизаторов и коммутаторов,
- безопасности беспроводного доступа,
- организации удаленного доступа,
- построения виртуальных частных сетей (VPN) и пр.,
- безопасности периметра.

Политика допустимого использования информационных ресурсов компании определяет права и ответственность сотрудников компании за надлежащую защиту конфиденциальной информации компании. В частности, политика допустимого использования определяет, могут ли сотрудники компании читать и копировать файлы, владельцами которых они не являются, но к которым имеют доступ. Также эта политика устанавливает правила допустимого использования корпоративной электронной почты, служб новостей и процедур доступа к сети компании. Примерный текст из описания политики допустимого использования:

«Сотрудники несут личную ответственность за безопасность любой информации, используемой и/или сохраненной с применением их учетных записей в компании. Используйте руководство пользователя для получения рекомендаций по защите вашей учетной записи и информации с использованием стандартных методов безопасности на уровне операционной системы или при помощи программного обеспечения для шифрования типа PGP. Конфиденциальная информация компании или сторонних организаций не должна храниться (или быть переданной) на компьютерах, не принадлежащих компании».

«Сотрудники не должны пытаться получить доступ к любым данным или программам, находящимся на рабочих станциях и серверах компании, если они не имеют соответствующего разрешения или явного согласия владельца этих информационных ресурсов».

Политика организации удаленного доступа определяет допустимые способы удаленного соединения с корпоративной информационной системой. Представляет собой основной документ безопасности в крупных транснациональных компаниях с географически разветвленной сетью. Должна описывать все доступные способы удаленного доступа к внутренним информационным ресурсам компании: доступ по коммутируемым сетям (SLIP, PPP), доступ с использованием ISDN/Frame Relay, Telnet/SSH-доступ через Интернет, выделенную линию/VPN/DSL и пр. Примерный текст из описания политики организации удаленного доступа:

1. Сотрудники, менеджеры по продажам и выездные специалисты компании, обладающие удаленным доступом к корпоративной сети компании, несут такую же ответственность, как и в случае локального подключения к сети компании.

2. Для членов семьи сотрудника компании доступ к Интернету через сеть компании разрешается только в случае оплаты трафика самим сотрудником. При этом сотрудник компании несет личную ответственность за то, чтобы член его семьи не нарушил правила политик безопасности компании, не выполнил противозаконные действия и не использовал

удаленный доступ для собственных деловых интересов. Сотрудник компании также несет ответственность за последствия неправильного использования удаленного доступа.

3. При осуществлении удаленного доступа к корпоративной сети, пожалуйста, ознакомьтесь со следующими политиками безопасности:

а) политика допустимого шифрования,

б) политика организации виртуальных частных сетей,

в) политика безопасности беспроводного доступа,

г) политика допустимого использования.

4. Для получения дополнительной информации относительно удаленного доступа, включения и отключения услуги, поиска неисправностей и т. д., обращайтесь на Web-сайт службы организации удаленного доступа к информационным ресурсам компании».

Политика удаленного доступа определяет, кто из сотрудников может иметь высокоскоростной удаленный доступ ISDN, Frame Relay. При этом определяются ограничения по организации удаленного доступа. Пример требований политики удаленного доступа:

«Защищенный удаленный доступ должен строго контролироваться. Требуемый уровень безопасности обеспечивается с помощью использования однократных (one-time) паролей или инфраструктуры открытых ключей устойчивыми к взлому ключевыми фразами (passphrase). (Для получения информации по созданию устойчивых ко взлому ключевых фраз, см. описание политики управления паролями.) Сотрудник никому не должен передавать или посылать по электронной почте свой пароль на вход в систему, включая даже членов семьи.

Сотрудники, имеющие привилегию удаленного доступа, должны гарантировать, что их компьютеры, которые удаленно подключены к сети, не подключены в то же самое время ни в какую другую сеть, за исключением домашних сетей, которые находятся под полным управлением сотрудника.

Сотрудники, имеющие привилегию удаленного доступа к корпоративной сети, не должны использовать адреса электронной почты компании для ведения собственного бизнеса.

Маршрутизаторы для выделенных ISDN-линий, сконфигурированные для доступа к корпоративной сети, должны использовать для аутентификации, как минимум, CHAP».

Политика безопасности периметра описывает порядок и правила получения привилегированного доступа к системам безопасности периметра корпоративной сети компании. Кроме того, описывает процедуру инициации и обработки запросов на изменение конфигурации систем безопасности периметра сети, а также порядок и периодичность проверки этих конфигураций. Примерный текст из политики безопасности периметра:

«Доступ к информации о конфигурации систем безопасности периметра сети компании должен быть ограничен. Информация о конфигурации систем безопасности периметра никогда не должна храниться или передаваться по корпоративной сети и никогда не должна печататься и храниться в виде бумажной копии. Необходимо отслеживать все изменения конфигурации систем сетевой безопасности и периодически проводить аудит безопасности периметра сети».

Политика управления паролями определяет правила и порядок создания и изменения паролей сотрудников компании. Примерный текст из описания политики управления паролями:

«Все пароли системного уровня (например, root, enable, administrator в системе Windows, пароли администраторов приложений и т. д.) должны изменяться по крайней мере раз в квартал. Все пароли системного уровня должны быть частью глобальной базы данных управления паролями отдела защиты информации. Все пароли пользовательского уровня (например, доступа к электронной почте, к сети, к настольному компьютеру и т. д.) должны изменяться по крайней мере раз в шесть месяцев. Рекомендованный интервал изменения – раз в четыре месяца. Учетные записи сотрудников, которым предоставляется доступ к административным учетным записям на системах с помощью членства в группах

или программ sudo, должны иметь пароль, отличный от всех других паролей данного сотрудника».

Это только несколько примеров политик, которые могут быть использованы вашей компанией. С ними и другими политиками безопасности можно ознакомиться на Web-сайте американского института аудиторов и администраторов безопасности SANS (http://www.sans.org/newlook/resources/policies/policies.htm). 1.4.9. Процедуры безопасности

Процедуры безопасности так же важны, как и политики безопасности. Если политики безопасности определяют *что* должно быть защищено, то процедуры безопасности определяют *как* защитить информационные ресурсы компании. Приведем здесь примеры нескольких важных процедур безопасности.

Процедура управления конфигурацией обычно определяется на уровне отдела или на уровне компании. Но даже если есть процедура по управлению изменениями на уровне компании, индивидуальные группы могут иметь собственные процедуры. Процедура управления изменениями должна определять процесс документирования и запроса на изменения конфигурации всех масштабов (от простой инсталяции маршрутизатора до изменения списков контроля доступа на межсетевом экране). Идеально, если служба защиты информации проводит анализ изменений и контролирует запросы на изменения. Процесс управления изменениями важен по нескольким ключевым причинам:

• документированные изменения обеспечивают возможность проведения аудита безопасности;

• в случае возможного простоя из-за изменения проблема будет быстро определена;

• обеспечивается способ координирования изменений таким образом, чтобы одно изменение не влияло на другое изменение.

Процедуры резервного копирования информации и хранения резервных копий вне офиса могут потребоваться из-за требований клиентов и партнеров по бизнесу. Число сотрудников компании, имеющих доступ к резервным лентам за пределами компании, должно быть сведено к минимуму. Вы должны тестировать возможность восстановления информации из резервных носителей на регулярной основе для проверки целостности резервных копий. Часть процедуры резервного копирования может быть выполнена в виде программы или сценария, который автоматизирует процесс создания резервных копий. *Процедура обработки инцидентов* определяет порядок обработки и расследования инцидентов. Эта процедура должна осуществляться в любой компании. Невозможно определить порядок реагирования на все инциденты, но вы должны описать порядок реагирования на основные их типы. Вот некоторые из них: сканирование портов, атаки типа «отказ в обслуживании», взлом компьютеров, взлом пароля учетной записи и несоответствующее использование информационных систем. Необходимо назначить одного сотрудника, отвечающего за взаимодействие с правоохранительными органами.

1.5. Возможные постановки задачи

1.5.1. Металлургическая компания

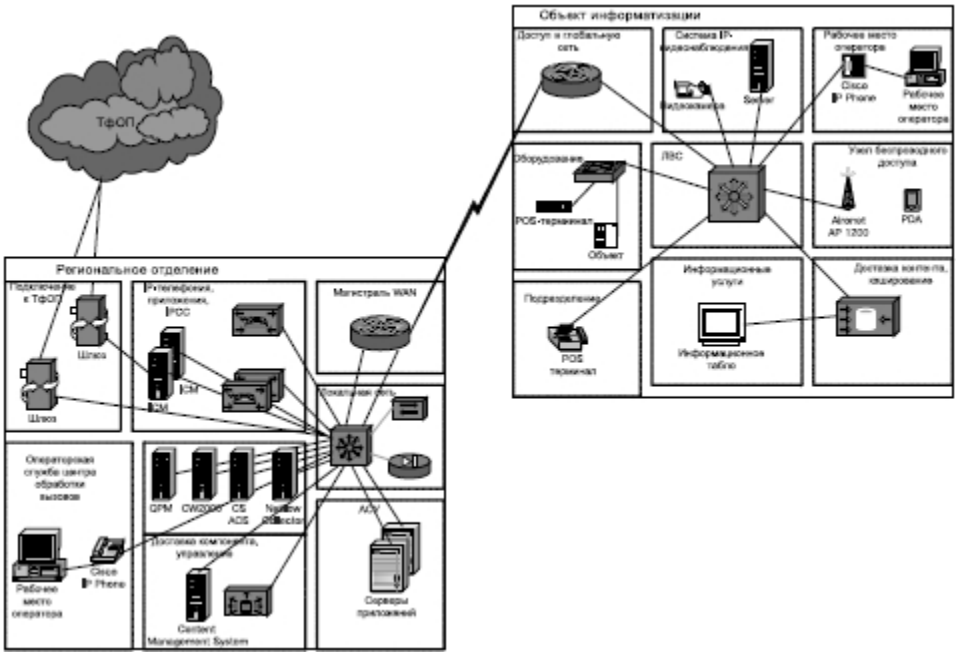
Задача: разработка политики информационной безопасности металлургической компании (далее – «компания»), см. рис. 1.17.

Основание: пункт «Разработка и реализация мероприятий по обеспечению информационной безопасности объектов информатизации компании» перечня мероприятий целевой программы компании «Информационная безопасность– 2005».

Сроки выполнения: начало работ по договору – после заключения договора по результатам конкурса. Окончание работ по договору – 1 декабря 2005 года.

Основные требования к составу работ. Разработка политики информационной безопасности объектов информатизации компании является первым этапом реализации мероприятия «Разработка и реализация мероприятий по обеспечению информационной безопасности объектов информатизации компании» раздела «Система обеспечения

информационной безопасности компании».



...

Рис. 1.17. Структура объекта информатизации металлургической компании

При разработке политики информационной безопасности объектов информатизации необходимо обеспечить:

• универсальность решений и полноту требований по информационной безопасности компании для мультипротокольных реализаций действующих информационных и коммуникационных систем объектов информатизации компании в соответствии с законодательными и нормативными актами Российской Федерации;

• формирование системы взглядов, требований и решений, обеспечивающих единство, интегрированность и совместимость реализации мероприятий раздела «Система обеспечения информационной безопасности компании» («Создание и развитие удостоверяющего центра, выдающего сертификаты ключей ЭЦП», «Разработка концепции программно-аппаратного комплекса мониторинга и защиты информационных ресурсов объектов информатизации компании от внешних и внутренних угроз информационной безопасности», «Создание и развитие защищенного центра резервного хранения данных информационных ресурсов компании»);

• формирование системы взглядов, требований и решений по информационной безопасности компании, необходимых для реализации проектов в области защиты информации.

При разработке политики информационной безопасности необходимо:

• разработать требования по обеспечению безопасности информационных ресурсов и систем компании;

• обследовать проекты, защищаемые объекты информатизации;

• разработать проект Технического задания на создание единой системы информационной безопасности компании;

• определить перечень первоочередных работ по защите программными и аппаратными способами информационных ресурсов и систем компании от несанкционированного доступа, искажения или потери;

• подготовить испытательный стенд для отработки типовых решений в области защиты информации;

• разработать технико-экономическое обоснование реализации базовых технологий по обеспечению информационной безопасности в рамках проектов планируемого года;

• подготовить и выпустить комплект необходимой документации, представить ее на экспертизу.

Решения, полученные в результате разработки политики информационной безопасности объектов информатизации компании, должны обеспечивать: • возможность создания единой системы информационной безопасности компании;

• единство принципов и интеграцию технологических решений по защите информации компании при реализации проектов в области защиты информации.

Требования к политике безопасности. Разработка политики информационной безопасности компании должна быть осуществлена с учетом: • существующих общих проблем и тенденций обеспечения информационной безопасности информационно-коммуникационных технологий на основе мирового и отечественного опыта;

• законодательной и нормативной основы обеспечения информационной безопасности информационно-коммуникационных технологий;

• особенностей обеспечения информационной безопасности объектов информатизации компании.

В результате разработки политики информационной безопасности компании должны быть рассмотрены: • потенциальные угрозы информационным ресурсам и системам, возможные последствия их реализации;

• требования и методы противодействия угрозам информационной безопасности;

• технологии обеспечения информационной безопасности защищаемых ресурсов и систем;

• функциональные подсистемы и организационные процедуры обеспечения информационной безопасности ресурсов и систем объектов информатизации компании;

• органы и процедуры управления деятельностью по обеспечению информационной безопасности;

• вопросы мониторинга и анализа состояния дел в сфере информационной безопасности.

В результате обследования должны быть оценены решения и разработаны типовые требования по обеспечению информационной безопасности компании. *Документирование проекта.* Отчетная документация оформляется в соответствии с общими требованиями к текстовым документам по ГОСТ 2.105-79.

В процессе выполнения работ Исполнителем разрабатывается следующая документация:

• Политика информационной безопасности компании;

• Итоговый научно-технический отчет;

• Предложения по реализации Концепции информационной безопасности компании на период 2005–2007 годов (по результатам обследования);

• Проект Технического задания на создание комплексной системы информационной безопасности объектов информатизации компании;

• Требования по обеспечению информационной безопасности объектов информатизации компании;

• Технико-экономическое обоснование реализации базовых технологий по обеспечению информационной безопасности компании.

Отчетные материалы оформляются на бумажном носителе формата А4 и магнитном носителе (CD-R) в двух экземплярах каждого вида и передаются Заказчику. Работы по объекту конкурса выполняются в один этап.

1.5.2. Коммерческий банк

Общее описание объекта информатизации (рис. 1.18):

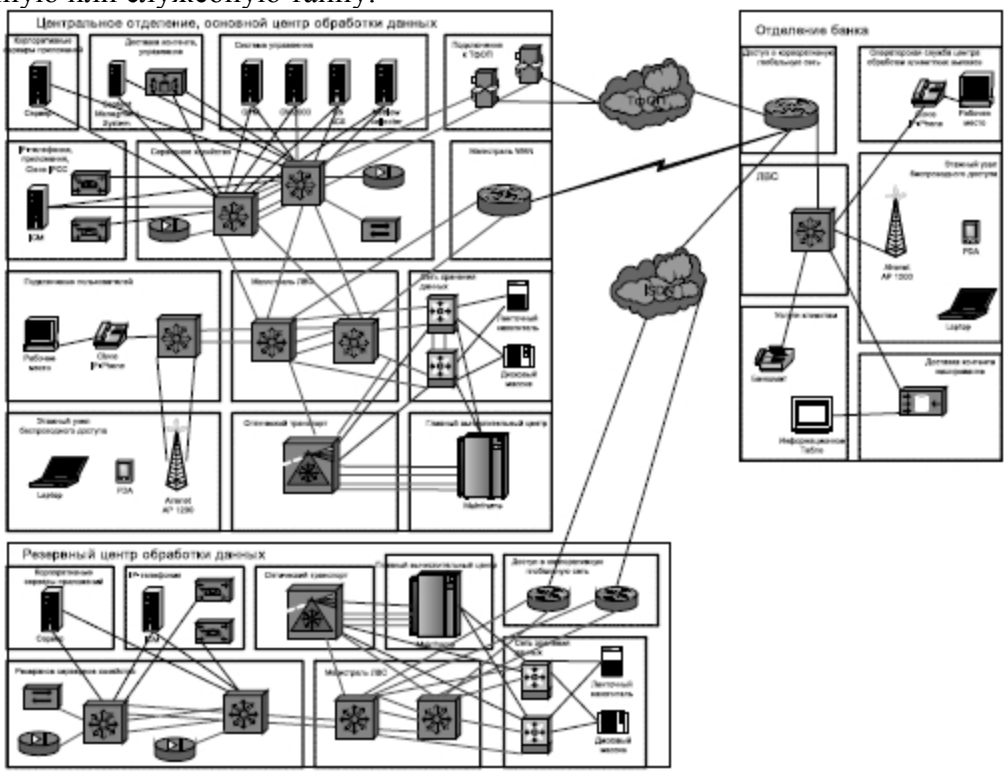
1. Документы, заказываемые Исполнителю, а именно проект концепции и эскизный проект по обеспечению информационной безопасности, согласованные и принятые Заказчиком, разрабатываются в целях обеспечения информационной безопасности объекта информатизации, которым является АС коммерческого банка (далее – «компания»),

2. Компания действует на основании Устава и предоставляет физическим и юридическим лицам банковские услуги.

3. Организационная структура компании имеет три основных уровня: центральное отделение банка, расположенное в г. Санкт-Петербурге; резервный центр обработки данных в г. Москве; отделения банка (около 100), расположенные в городах и других населенных пунктах районного значения на всей территории РФ.

4. Общая численность персонала компании составляет около 5 тыс. сотрудников.

5. Основной объем информации, вводимой, получаемой, передаваемой и обрабатываемой в процессе работы компании, – банковские данные, но в их составе также передается и обрабатывается дополнительная служебная информация. Помимо традиционных угроз возможного незаконного использования банковской информации, таких, как получение несанкционированного доступа к передаваемым или обрабатываемым данным, искажение передаваемой информации, нарушение целостности передаваемых или обрабатываемых данных, возможны угрозы доступа к сведениям, составляющим государственную или служебную тайну.



...

Рис. 1.18. Структура объектов информатизации банка

7. Взаимодействие компании осуществляется с клиентами и бизнес-партнерами, а также с Центральным банком России, МНС России, Государственным таможенным комитетом Российской Федерации и другими органами государственной власти.

8. Система защиты информации должна обеспечивать возможность организации процесса обмена данными и электронными документами между подразделениями компании на всех уровнях (центральное отделение – резервный центр обработки данных – городские и районные отделения банка), не накладывая ограничений на выбор системы передачи данных.

Кроме того, необходимо предусматривать возможность реализации удаленного доступа пользователей системы к информации, организации IP-телефонии, конференций и т. д.

9. Подразделения компании различного уровня могут размещаться в отдельных собственных или арендуемых зданиях (в том числе не в одном), собственных или арендуемых помещениях в зданиях (в том числе удаленных друг от друга). Организационная структура компании строится из отделов.

Таблица 1.3. Перечень разрабатываемых документов

№ пункта	№ подпункта	Наименование разрабатываемого документа
1	1.1	Концепция информационной безопасности компании
	1.2	Положение о системе защиты информации компании
	1.3	Положение о порядке организации и проведения работ по защите информации на объектах информатизации компании
	1.4	Положение о разрешительной системе допуска исполнителей к документам и сведениям компании конфиденциального характера
	1.5	Положение об организации пропускного и внутри-объектного режима в подразделениях компании
	1.6	Положение о порядке учета, обращения и хранения информации ограниченного распространения в подразделениях компании
	1.7	Положение об организации электронного документооборота компании
	1.8	Инструкция по организации контроля эффективности защиты информации в подразделениях компании
	1.9	Положение об отделе обеспечения безопасности информации
	1.10	Типовая инструкция сотрудников отдела обеспечения безопасности информации
	1.11	Типовая инструкция администратора безопасности
	1.12	Типовая инструкция администратора локально-вычислительной сети
	1.13	Типовая инструкция администратора баз данных
	1.14	Типовая инструкция пользователя автоматизированной системы
2	2.1	Эскизный проект по обеспечению информационной безопасности компании
	2.17	Требования по защите информации на объектах информатизации компании
	2.19	Методические рекомендации по разработке моделей угроз и потенциального нарушителя для объектов информатизации компании
3		Другие документы для нормативной базы Заказчика по обеспечению информационной безопасности, которые Исполнитель сочтет необходимым разработать в дополнение к руководящим и специальным документам, указанным в пунктах 1 и 2 настоящей таблицы

...

Примечание: Под сокращенным термином «концепция» понимается концепция информационной безопасности, под сокращенным термином «ЭП» понимается эскизный проект по обеспечению информационной безопасности. Участник в составе Технической части своей заявки может мотивированно предложить дополнить указанный выше перечень руководящих и специальных нормативных документов по обеспечению безопасности, подлежащих разработке в дополнение к концепции и ЭП. Данные предложения будут оцениваться в рамках оценки Технической части заявки по установленным критериям.

Иногда возможно размещение не связанных между собой отделов в одном помещении.

10. В территориальных подразделениях компании должны быть созданы отделы обеспечения безопасности информации для работы на местах.

11. Руководящие и специальные документы по обеспечению информационной безопасности должны разрабатываться с учетом возможных организационных и технологических изменений в работе компании.

Требования к документам. В результате проведенных работ Победитель конкурса должен сдать согласованную с Заказчиком окончательную редакцию проектов следующих

документов (см. табл. 1.3).

Все перечисленные отчетные документы должны быть подготовлены в соответствии с *нормативными документами,* приведенными ниже в табл. 1.4.

Таблица 1.4. Перечень нормативных документов

№	Тип документа	Название нормативного документа
1	Концепция	Конституция Российской федерации (принята на всенародном голосовании 12 декабря 1993 г.)
2	Федеральный закон	Федеральный закон «Об участии в международном информационном обмене» от 4 июля 1996 г. № 85-ФЗ
3	Федеральный закон	Федеральный закон «О связи» от 7 июля 2003 г. № 126-ФЗ
4	Кодекс	Гражданский кодекс Российской федерации (части первая, вторая и третья)
5	Закон	Закон РФ «Об авторском праве и смежных правах» от 9 июля 1993 г. № 5351-I
6	Федеральный закон	Федеральный закон «Об информации, информатизации и защите информации» от 20 февраля 1995 г. № 24-ФЗ
7	Концепция	Концепция национальной безопасности Российской Федерации (утверждена Указом Президента РФ от 17 декабря 1997 г. № 1300) (в редакции Указа Президента РФ от 10 января 2000 г. № 24)
8	Доктрина	Доктрина информационной безопасности Российской федерации от 9 сентября 2000 г. № ПР-1895
9	Закон	Закон РФ «О безопасности» от 5 марта 1992 г. № 2446-I
10	Федеральный закон	Федеральный закон «О техническом регулировании» от 27 декабря 2002 г. № 184-ФЗ
11	Закон	Закон РФ «О государственной тайне» от 21 июля 1993 г. № 5485-1
12	Федеральный закон	Федеральный закон «О коммерческой тайне» №98-ФЗ от 29 июля 2004 г.
13	Указ	Указ Президента РФ «Об утверждении перечня сведений, отнесенных к государственной тайне» от 30 ноября 1995 г. № 1203

Продолжение табл. 1.14

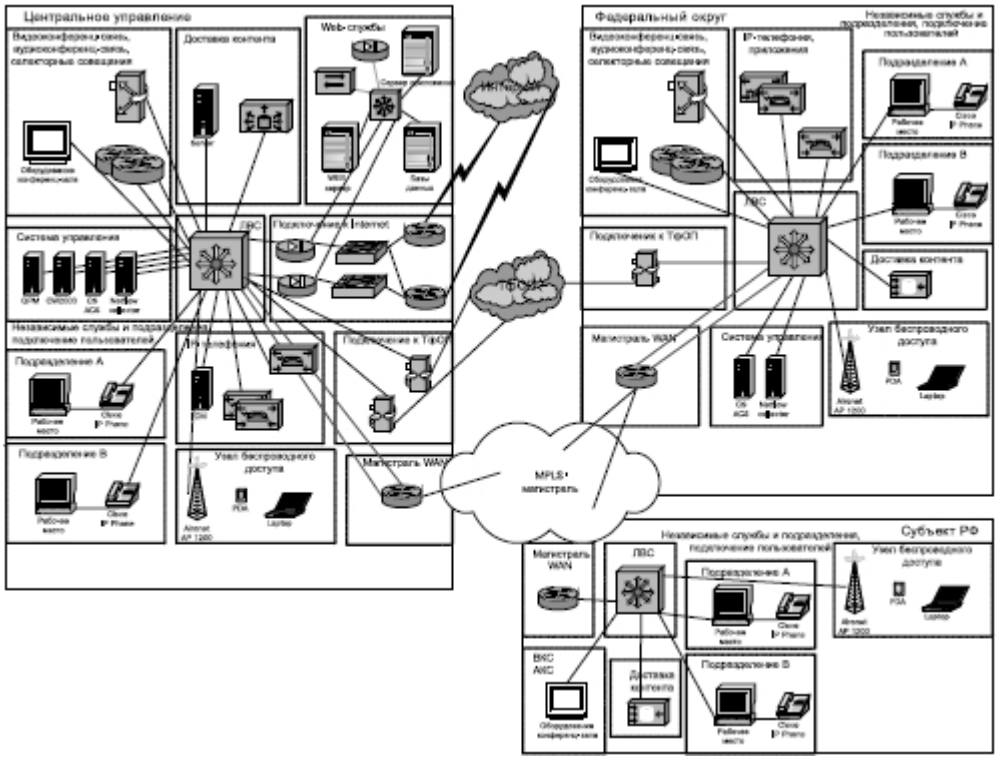
№	Тип документа	Название нормативного документа
14	Указ	Указ Президента РФ «Об утверждении перечня сведений конфиденциального характера» от 6 марта 1997 г. № 188
15	Указ	Указ Президента РФ «О мерах по обеспечению информационной безопасности Российской Федерации в сфере международного информационного обмена» от 12 мая 2004 г. №611
16	Постановление	Постановление Правительства Рф от 4 сентября 1995 г. № 870 «Об утверждении Правил отнесения сведений, составляющих государственную тайну, к различным степеням секретности»
17	Положение	Положение о лицензировании деятельности предприятий, учреждений и организаций по проведению работ, связанных с использованием сведений, составляющих государственную тайну, созданием средств защиты информации, а также с осуществлением мероприятий и (или) оказанием услуг по защите государственной тайны (утверждено постановлением Правительства Рф от 15 апреля 1995 г. № 333)
18	Постановление	Постановление Правительства РСФСР от 5 декабря 1991 г. № 35 «О перечне сведений, которые не могут составлять коммерческую тайну»
19	Постановление	Постановление Правительства Рф от 30 апреля 2002 г. № 290 «О лицензировании деятельности по технической защите конфиденциальной информации»
20	Постановление	Постановление Правительства Рф от 23 сентября 2002 г. № 691 «Об утверждении положений о лицензировании отдельных видов деятельности, связанных с шифровальными (криптографическими) средствами»
21	Постановление	Постановление Правительства Рф от 27 мая 2002 г. № 348 «Об утверждении Положения о лицензировании деятельности по разработке и (или) производству средств защиты конфиденциальной информации»
22	ГОСТ	ГОСТ Р 51624-2000 «Защита информации. Автоматизированные системы в защищенном исполнении. Общие требования»
23	ГОСТ	ГОСТ Р 50922-96 «Защита информации. Основные термины и определения»
24	ГОСТ	ГОСТ Р 50739-95 «Средства вычислительной техники. Защита от несанкционированного доступа к информации. Общие технические требования»
25	ГОСТ	ГОСТ Р 51583-2000 «Защита информации. Порядок создания автоматизированных систем в защищенном исполнении. Общие положения»
26	ГОСТ	ГОСТ Р 51241-98 «Средства и системы контроля и управления доступом. Классификация. Общие технические требования»
27	ГОСТ	ГОСТ Р 51275-99 «Защита информации. Объект информатизации. факторы, воздействующие на информацию. Общие положения»

Окончание табл. 1.14

№	Тип документа	Название нормативного документа
28	ГОСТ	ГОСТ 28806-90 «Качество программных средств. Термины и определения»
29	ГОСТ	ГОСТ 28195-89 «Оценка качества программных средств»
30	ГОСТ	ГОСТ Р ИСО/МЭК 9126-93 «Информационная технология. Оценка программной продукции. Характеристики качества и руководства по их применению»
31	ГОСТ	ГОСТ Р ИСО/МЭК 15408-2002 «Информационная технология. Методы и средства обеспечения безопасности. Критерии оценки безопасности информационных технологий (Часть 1. Введение и общая модель; Часть 2. функциональные требования безопасности; Часть 3. Требования доверия к безопасности)»
32	ГОСТ	ГОСТ Р 51188-98 «Защита информации. Испытания программных средств на наличие компьютерных вирусов. Типовое руководство»
33	ГОСТ	ГОСТ РВ 50600-93 «Защита секретной информации от технической разведки. Система документов. Общие положения»
34	Документы Гостехкомиссии России	РД. Концепция защиты средств вычислительной техники и автоматизированных систем от несанкционированного доступа к информации. Введена Решением Председателя Гостехкомиссии России от 30.03.92 г.
35	Документы Гостехкомиссии России	РД. Средства вычислительной техники. Защита от несанкционированного доступа к информации. Показатели защищенности от несанкционированного доступа к информации. 1992 г.
36	Документы Гостехкомиссии России	РД. Автоматизированные системы. Защита от несанкционированного доступа к информации. Классификация автоматизированных систем и требования по защите информации. 1992 г.
37	Документы Гостехкомиссии России	Документ Гостехкомиссии (ФСТЭК) России Специальные требования и рекомендации по технической защите конфиденциальной информации (СТР-К). 2002 г.
38	Стандарт Банка России	Стандарт Банка России «Обеспечение информационной безопасности организаций банковской системы Российской Федерации. Общие положения» Введен распоряжением от 18 ноября 2004 г. № Р-609 с 1 декабря 2004 г.

Субподрядчики для разработки конкретных документов по перечню, приводимому в табл. 1.3, будут приняты из Технической части победившей заявки; данные структуры, предлагаемые Участниками в составе Технической части своей заявки, должны соответствовать регламентирующим положениям нормативных документов, приведенных в табл. 1.4. 1.5.3. Субъект РФ

Концепция информационной безопасности субъекта РФ (далее – «Концепция») разрабатывается с учетом требований федеральных законов «Об электронной цифровой подписи», «Об информации, информатизации и защите информации» и имеющегося научно-технического задела (см. рис. 1.19).



...

Рис. 1.19. Структура объектов информатизации субъекта РФ

Цель разработки Концепции: определение политики безопасности АС субъекта РФ как совокупности целей, задач, нормативных актов, объектов обеспечения безопасности информации, технических и информационных ресурсов и технических решений по защите информации, основных путей и этапов реализации Концепции.

Результатом выполнения Концепции должно стать создание подсистемы обеспечения безопасности информации АС субъекта РФ, в полной мере отвечающей требованиям федеральных законов в области защиты информации. Концепция должна включать в себя следующие материалы:

• законодательные и нормативные акты Российской Федерации в области обеспечения безопасности информации, требованиям которых должна соответствовать АС субъекта РФ, в том числе перечень законодательных и нормативных документов, необходимых для реализации в АС субъекта РФ Федерального закона РФ «Об электронной цифровой подписи», рекомендации по совершенствованию существующей и разработке новой нормативно-правовой базы;

• результаты анализа АС субъекта РФ как объекта обеспечения безопасности информации, в том числе отличия существующей и усовершенствованной совокупностей информационно-телекоммуникационных средств, используемых для обработки информации в части категории обрабатываемой и хранящейся в ней информации, программно-технической среды, технологии обработки информации и информационных потоков, структуры связи и передачи данных, а также предложения по объемам информационных ресурсов, накапливаемых и хранящихся в АС различных уровней и относящихся исключительно к категории конфиденциальной информации; определение и обоснование принципов, целей и задач обеспечения безопасности информации;

• перечень объектов обеспечения безопасности информации, защищаемых технических и информационных ресурсов, возможных угроз защищаемым объектам, основных источников угроз и способов их реализации; описание моделей нарушителя с оценкой их

актуальности и соответствия существующим и перспективным угрозам;

• рекомендации по развитию структуры подсистемы обеспечения безопасности информации и АС субъекта РФ в целом с учетом требований законодательных и нормативных актов РФ в области обеспечения безопасности информации;

• описание и обоснование структуры подсистемы обеспечения безопасности информации АС субъекта РФ с учетом утвержденной модели нарушителя, угроз конфиденциальности, достоверности целостности, сохранности и доступности информации, технологии ее поиска, сбора, накопления, обработки, хранения и передачи по каналам связи, а также обоснование требуемой для обеспечения функционирования данной подсистемы численности персонала;

• описание структуры построения программно-технической среды АС субъекта РФ и требования к ней, реализация которых позволит обеспечить юридическую значимость создаваемых в ней электронных документов; перечень организационно-технических мероприятий, реализация которых необходима для обеспечения возможности обработки конфиденциальной информации и придания юридической силы документам, создаваемым в АС субъекта РФ;

• обоснование показателей надежности подсистемы обеспечения безопасности информации, подсистемы связи и передачи данных, в том числе их основных компонент, в условиях возможного компьютерного нападения или вирусного заражения, а также определение путей их повышения; анализ влияния надежности программно-технических средств и технологии функционирования составных частей АС субъекта РФ на показатели надежности подсистемы обеспечения безопасности информации;

• описание комплекса мероприятий по обоснованию достоверности получаемой с помощью АС субъекта РФ информации;

• анализ имеющихся лицензий и сертификатов на все программно-технические средства АС субъекта РФ, выданных органами по сертификации и лицензированию, на предмет их достаточности и соответствия модели нарушителя;

• требования к безопасности информации в АС субъекта РФ, включающие в себя требования к уровню защиты от несанкционированного доступа;

• распределение задач (функций) между встроенными средствами защиты информации операционной системы, СУБД, прикладными программами и специальными средствами защиты информации при их взаимодействии по обеспечению безопасности информации, а также их достаточности и непротиворечивости;

• описание основных путей и этапов реализации Концепции;

• технико-экономическую оценку работ по реализации Концепции;

• описание состава подсистем, обеспечивающих защиту информации от нарушения ее целостности и достоверности, а также штатное функционирование программно-технических средств сбора, обработки, накопления, хранения, поиска и передачи информации в АС субъекта РФ;

• требования по исключению влияния внешней среды на защищаемые ресурсы АС субъекта РФ.

1.6. Российская специфика разработки политик безопасности

Темпы развития современных информационных технологий значительно опережают темпы разработки рекомендательной и нормативно-правовой базы руководящих документов, действующих на территории России. Поэтому решение вопроса о разработке политики информационной безопасности на современном предприятии связано с проблемой выбора критериев и показателей защищенности, а также эффективности корпоративной системы защиты информации. Вследствие этого в дополнение к требованиям и рекомендациям стандартов [1] , Конституции и федеральным законам [2] , руководящим документам Гостехкомиссии (ФСТЭК) России приходится использовать ряд международных

рекомендаций. В том числе адаптировать к отечественным условиям и применять на практике в соответствии с рекомендациями Федерального закона № 184-ФЗ «О техническом регулировании» методики международных стандартов, таких, как ISO 17799 (BS 7799), ISO 9001, ISO 15408, ISO 13335, BSI, CobiT, ITIL [3] и др., а также использовать методики управления информационными рисками в совокупности с оценками экономической эффективности инвестиций в обеспечение защиты информации предприятия.

Современные методики управления рисками позволяют в рамках политик безопасности отечественных компаний поставить и решить ряд задач перспективного стратегического развития.

Во-первых, количественно оценить текущий уровень информационной безопасности предприятия, что потребует выявления рисков на правовом, организационно-управленческом, технологическом, а также техническом уровнях обеспечения защиты информации.

Во-вторых, разработать политику безопасности и планы совершенствования корпоративной системы защиты информации с целью достижения приемлемого уровня защищенности информационных активов компании. Для этого необходимо:

• обосновать и произвести расчет финансовых вложений в обеспечение безопасности на основе технологий анализа рисков, соотнести расходы на обеспечение безопасности с потенциальным ущербом и вероятностью его возникновения;

• выявить и провести первоочередное блокирование наиболее опасных уязвимостей до осуществления атак на уязвимые ресурсы;

• определить функциональные отношения и зоны ответственности при взаимодействии подразделений и должностных лиц по обеспечению информационной безопасности компании, создать необходимый пакет организационно-распорядительной документации;

• разработать и согласовать со службами организации, надзорными органами проект внедрения необходимых комплексов защиты, учитывающий современный уровень и тенденции развития информационных технологий;

• обеспечить поддержание внедренного комплекса защиты в соответствии с изменяющимися условиями работы организации, регулярными доработками организационно-распорядительной документации, модификацией технологических процессов и модернизацией технических средств защиты.

Решение названных задач политик безопасности открывает новые широкие возможности перед должностными лицами разного уровня. Руководителям верхнего звена это поможет объективно и независимо оценить текущей уровень информационной безопасности компании, обеспечить формирование единой стратегии безопасности, рассчитать, согласовать и обосновать затраты на защиту компании. На основе полученной оценки начальники отделов и служб смогут выработать и обосновать необходимые организационные меры (состав и структуру службы информационной безопасности, положение о коммерческой тайне, пакет должностных инструкций и инструкции по действиям в нештатных ситуациях). Менеджеры среднего звена смогут обоснованно выбрать средства защиты информации, а также адаптировать и использовать в своей работе количественные показатели оценки информационной безопасности, методики оценки и управления безопасностью с привязкой к экономической эффективности компании.

Практические рекомендации по нейтрализации и локализации выявленных уязвимостей системы, полученные в результате аналитических исследований, помогут в работе над проблемами информационной безопасности на разных уровнях и, что особенно важно, помогут определить основные зоны ответственности, в том числе материальной, за ненадлежащее использование информационных активов компании. При определении масштабов материальной ответственности за ущерб, причиненный работодателю, в том числе связанный с разглашением коммерческой тайны, следует руководствоваться положениями гл. 39 Трудового кодекса РФ.

В соответствии со ст. 20 Федерального закона «Об информации, информатизации и

защите информации» целями защиты информации являются в том числе: предотвращение утечки, хищения, утраты, искажения, подделки информации; предотвращение несанкционированных действий по уничтожению, модификации, искажению, копированию, блокированию информации; предотвращение других форм незаконного вмешательства в информационные ресурсы и информационные системы.

Поэтому главной целью политик безопасности отечественных компаний является обеспечение устойчивого функционирования предприятия: предотвращение угроз его безопасности, защита законных интересов владельца информации от противоправных посягательств, в том числе уголовно наказуемых деяний в рассматриваемой сфере отношений, предусмотренных Уголовным кодексом РФ [4] , обеспечение нормальной производственной деятельности всех подразделений объекта. Другая задача политик безопасности сводится к повышению качества предоставляемых услуг и гарантий безопасности имущественных прав и интересов клиентов [5] .

Для этого необходимо:

• отнести информацию к категории ограниченного доступа (коммерческой тайне) [6] ;

• прогнозировать и своевременно выявлять угрозы безопасности информационным ресурсам, причины и условия, способствующие нанесению финансового, материального и морального ущерба, нарушению нормального функционирования и развития ресурсов [7] ;

• создать условия функционирования с наименьшей вероятностью реализации угроз безопасности информационным ресурсам и нанесения различных видов ущерба [8] ;

• создать механизм и условия оперативного реагирования на угрозы информационной безопасности и проявления негативных тенденций в функционировании АС, а также пресечения посягательств на ресурсы на основе правовых, организационных и технических мер и средств обеспечения безопасности [9] ;

• создать условия для максимально возможного возмещения и локализации ущерба, наносимого неправомерными действиями физических и юридических лиц и тем самым ослабить негативное влияние последствий нарушения информационной безопасности [10] .

При разработке политики безопасности можно использовать следующую модель (рис. 1.20), основанную на адаптации Общих критериев (ISO 15408) и проведении анализа риска (ISO 17799). Эта модель соответствует специальным нормативным документам по обеспечению информационной безопасности, принятым в Российской Федерации, международному стандарту ISO/IEC 15408 «Информационная технология – методы защиты – критерии оценки информационной безопасности», стандарту ISO/IEC 17799 «Управление информационной безопасностью» и учитывает тенденции развития отечественной нормативной базы (в частности, документов Гостехкомиссии РФ) по вопросам защиты информации.

...

Рис. 1.20. Модель построения корпоративной системы защиты информации

Представленная модель – это совокупность объективных внешних и внутренних факторов и их влияние на состояние информационной безопасности на объекте и на сохранность материальных или информационных ресурсов.

Рассматриваются следующие объективные факторы:

• угрозы информационной безопасности, характеризующиеся вероятностью возникновения и вероятностью реализации;

• уязвимости информационной системы или системы контрмер (системы информационной безопасности), влияющие на вероятность реализации угрозы;

• риск – фактор, отражающий возможный ущерб организации в результате реализации угрозы информационной безопасности: утечки информации и ее неправомерного использования (риск в конечном итоге отражает вероятные финансовые потери – прямые или косвенные).

Таким образом, для создания эффективных политик безопасности отечественных компаний предлагается первоначально провести анализ рисков в области информационной безопасности. Затем определить оптимальный уровень риска для предприятия на основе заданного критерия. Политику безопасности и соответствующую корпоративную систему защиты информации предстоит построить таким образом, чтобы достичь заданного уровня риска. Предлагаемая методика разработки политики информационной безопасности современного предприятия позволяет полностью проанализировать и документально оформить требования, связанные с обеспечением информационной безопасности, избежать расходов на излишние меры безопасности, возможные при субъективной оценке рисков, оказать помощь в планировании и осуществлении защиты на всех стадиях жизненного цикла информационных систем, обеспечить проведение работ в сжатые сроки, представить обоснование для выбора мер противодействия, оценить эффективность контрмер, сравнить различные варианты контрмер.

В ходе работ должны быть установлены границы исследования. С этой целью необходимо выделить требующие оценки рисков ресурсы информационной системы. При этом предстоит разделить рассматриваемые ресурсы и внешние элементы, с которыми осуществляется взаимодействие. Ресурсами могут быть средства вычислительной техники,

программное обеспечение, данные, а также в соответствии со ст. 2 Федерального закона «Об информации, информатизации и защите информации» информационные ресурсы – отдельные документы и отдельные массивы документов, документы и массивы документов в информационных системах (библиотеках, архивах, фондах, банках данных, других информационных системах). Примерами внешних элементов являются сети связи (абз. 4 ст. 2 Федерального закона «О связи»), внешние сервисы и т. п.

При построении модели будут учитываться взаимосвязи между ресурсами. Например, выход из строя какого-либо оборудования может привести к потере данных или выходу из строя другого критически важного элемента системы. Подобные взаимосвязи определяют основу построения модели организации с точки зрения информационной безопасности.

Эта модель, в соответствии с предлагаемой методикой, строится следующим образом: для выделенных ресурсов определяется их ценность, как с точки зрения ассоциированных с ними возможных финансовых потерь, так и с точки зрения ущерба репутации организации, дезорганизации ее деятельности, нематериального ущерба от разглашения конфиденциальной информации и т. д. Затем описываются взаимосвязи ресурсов, определяются угрозы безопасности и оцениваются вероятности их реализации.

На основе построенной модели можно обоснованно выбрать систему контрмер, снижающих риски до допустимых уровней и обладающих наибольшей ценовой эффективностью. Частью системы контрмер будут рекомендации по проведению регулярных проверок эффективности системы защиты.

Обеспечение повышенных требований к информационной безопасности предполагает соответствующие мероприятия на всех этапах жизненного цикла информационных технологий. Планирование этих мероприятий производится по завершении этапа анализа рисков и выбора контрмер. Обязательной составной частью этих планов является периодическая проверка соответствия существующего режима информационной безопасности политике безопасности, сертификация информационной системы (технологии) на соответствие требованиям определенного стандарта безопасности.

По завершении работ можно будет определить меру гарантии безопасности информационной среды, основанную на оценке, с которой можно доверять информационной среде объекта. Данный подход предполагает, что большую гарантию дает применение больших усилий при проведении оценки безопасности. Адекватность оценки основана на вовлечении в процесс оценки большего числа элементов информационной среды объекта; глубине, достигаемой за счет использования при проектировании системы обеспечения безопасности большего числа проектов и описаний деталей выполнения; строгости, которая заключается в применении большего числа инструментов поиска и методов, направленных на обнаружение менее очевидных уязвимостей или на уменьшение вероятности их наличия.

Важно помнить, что прежде чем внедрять какие-либо решения по защите информации, необходимо разработать политики безопасности, адекватные целям и задачам современного предприятия. В частности, политики безопасности должны описывать порядок предоставления и использования прав доступа пользователей, а также требования отчетности пользователей за свои действия в вопросах безопасности. Система информационной безопасности окажется эффективной, если она будет надежно поддерживать выполнение правил политик безопасности, и наоборот. Этапы построения требуемых политик безопасности – это внесение в описание объекта автоматизации структуры ценностей, проведение анализа риска, определение правил для любого процесса пользования данным видом доступа к ресурсам объекта автоматизации. При этом политики безопасности желательно оформить в виде отдельных документов и утвердить у руководства компании.

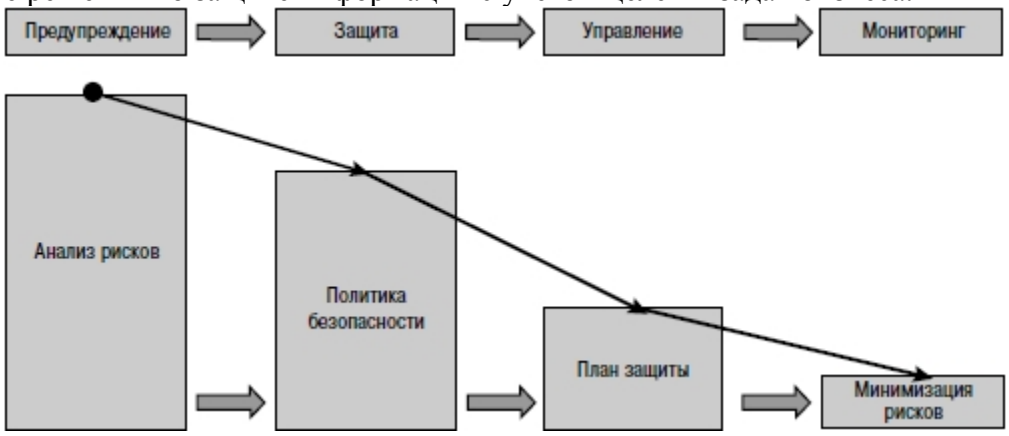
Глава 2 ЛУЧШИЕ ПРАКТИКИ СОЗДАНИЯ ПОЛИТИК БЕЗОПАСНОСТИ

В настоящее время сформировалась так называемая лучшая практика (best practices) политик информационной безопасности. Это прежде всего практика разработки политик,

процедур, стандартов и руководств безопасности таких признанных технологических лидеров, как IBM, Sun Microsystems, Cisco Systems, Microsoft, Symantec, SANS и пр. Насколько эти практики и рекомендации могут быть полезны для разработки политик безопасности в отечественных компаниях? В данной главе мы попробуем разобраться в этом.

2.1. Подход компании IBM

По мнению специалистов IBM, разработка корпоративных руководящих документов в области безопасности должна начинаться с создания политики информационной безопасности. При этом рекомендуется использовать международный стандарт ISO 17799:2005 и рассматривать политику безопасности компании как составную часть процесса управления информационными рисками (см. рис. 2.1). Считается, что разработка политики безопасности относится к стратегическим задачам менеджмента компании, который способен адекватно оценить стоимость ее информационных активов и принять обоснованные решения по защите информации с учетом целей и задач бизнеса.



...

Рис. 2.1. Процесс разработки политики безопасности компании

Компания IBM выделяет следующие основные этапы разработки политики безопасности:

• определение информационных рисков компании, способных нанести максимальный ущерб, для разработки в дальнейшем процедур и мер по предупреждению их возникновения;

• разработка политики безопасности, которая описывает меры защиты информационных активов, адекватные целям и задачам бизнеса;

• принятие планов действий в чрезвычайных ситуациях для уменьшения ущерба в случаях, когда выбранные меры защиты не смогли предотвратить инциденты в области безопасности;

• оценка остаточных информационных рисков и принятие решения о дополнительных инвестициях в средства и меры безопасности. Решение принимает руководство на основе анализа остаточных рисков.

2.1.1 Структура документов безопасности

Политика безопасности компании, с точки зрения IBM, должна содержать явный ответ на вопрос «Что требуется защитить?». Действительно, если руководство компании понимает, что необходимо защитить, какие информационные риски и угрозы информационным активам компании существуют, тогда можно приступать к созданию эффективной политики информационной безопасности. При этом политика безопасности является первым стратегическим документом, который необходимо создать и который содержит минимум технических деталей, будучи настолько статичным (неизменяемым), насколько возможно.

Предполагается, что политика безопасности компании будет содержать:

• определение информационной безопасности с описанием позиции и намерений руководства компании по ее обеспечению;

• описание требований по безопасности, в которые входит:

– соответствие требованиям законодательства и контрактных обязательств;

– обучение вопросам информационной безопасности;

– предупреждение и обнаружение вирусных атак;

– планирование непрерывности бизнеса;

– определение ролей и обязанностей по различным аспектам общей программы информационной безопасности;

– описание требований и процесса отчетности по инцидентам, связанным с информационной безопасностью;

– описание процесса поддержки политики безопасности.

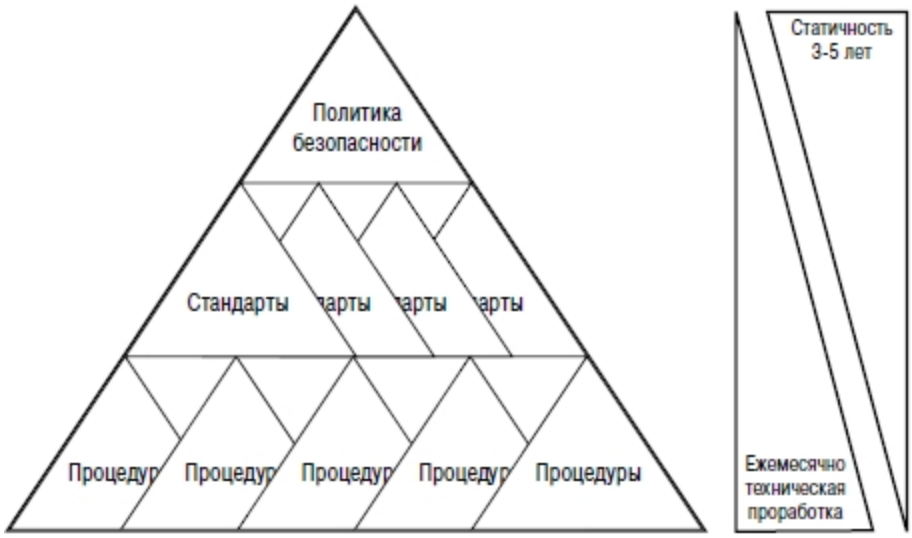
Компания IBM рекомендует выполнить следующие действия для разработки эффективной политики безопасности компании:

• анализ бизнес-стратегии компании и определение требований по информационной безопасности;

• анализ ИТ-стратегии, текущих проблем информационной безопасности и определение требований по информационной безопасности;

• создание политики безопасности, взаимно увязанной с бизнес– и ИТ-стратегиями.

В этом случае рекомендуемая структура руководящих документов по обеспечению информационной безопасности компании может быть представлена следующим образом (см. рис. 2.2).



...

Рис. 2.2. Структура руководящих документов безопасности

После создания корпоративной политики создается серия стандартов. Под стандартами IBM понимает документы, описывающие порядок применения корпоративной политики безопасности в терминах аутентификации, авторизации, идентификации, контроля доступа и т. д. Стандарты могут требовать частых изменений, так как на них оказывают влияние текущие угрозы и уязвимости информационных технологий.

В представлении IBM политики и стандарты безопасности создаются для:

• разработки правил и норм безопасности уровня компании;

• анализа информационных рисков и способов их уменьшения;

• формализации способов защиты, которые должны быть реализованы;

• определения ожиданий со стороны компании и сотрудников;

• четкого определения процедур безопасности, которым нужно следовать;

• обеспечения юридической поддержки в случае возникновения проблем в области безопасности.

Стандарты реализуются с помощью практик и/или процедур. Практики являются реализацией стандартов в операционных системах, приложениях и информационных системах. В них детализируются сервисы, устанавливаемые на операционных системах, порядок создания учетных записей и т. д. Процедуры документируют процессы запроса и подтверждения доступа к определенным сервисам, например VPN.

Рассмотрим особенности предлагаемого подхода IBM (рис. 2.3) на следующем примере: • проблемная ситуация – сотрудники загружают программное обеспечение из сети Интернет, что приводит к заражению вирусами, а в конечном счете к уменьшению производительности работы сотрудников компании;

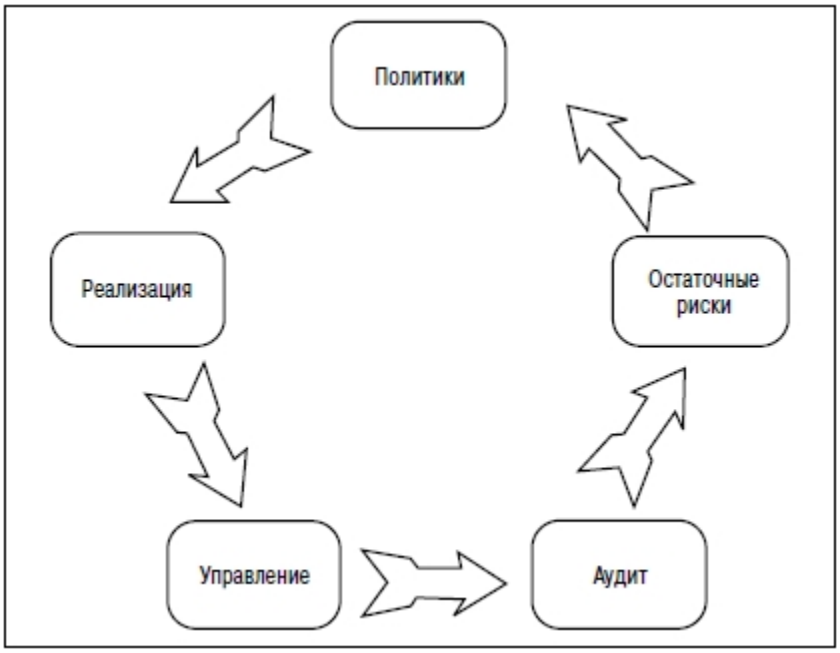
• в политику безопасности добавляется строка – «информационные ресурсы компании могут быть использованы только для выполнения служебных обязанностей». Политика безопасности доступна для ознакомления всем сотрудникам компании;

• создается стандарт безопасности, в котором описывается, какие сервисы и программное обеспечение разрешены для использования сотрудниками;

• практика безопасности описывает, как настроить операционную систему в соответствии с требованиями стандарта безопасности;

• процедура безопасности описывает процесс запроса и получения разрешения на использование дополнительных сервисов или установку дополнительного программного обеспечения сотрудниками;

• устанавливаются дополнительные сервисы для контроля выполнения требований политики безопасности.



...

Рис. 2.3. Подход IBM к разработке документов безопасности

2.1.2. Пример стандарта безопасности для ОС семейства UNIX

Цель и область действия стандарта: документ определяет требования по защите компьютеров, работающих под управлением ОС семейства UNIX.

Аудитория: персонал служб информационных технологий и информационной

безопасности.

Полномочия: отдел информационной безопасности наделяется всеми полномочиями для разрешения возможных проблем, связанных с безопасностью серверов информационной системы компании, и несет за это ответственность. Департамент управления информационными рисками утверждает все отклонения от требований данного стандарта.

Срок действия: с 1 января до 31 декабря … года.

Исключения: все отклонения от выполнения данного стандарта должны получить подтверждение в отделе информационной безопасности.

Поддержка: по всем вопросам, связанным с этим стандартом, обращаться в отдел информационной безопасности.

Пересмотр стандарта: стандарт пересматривается ежегодно.

СТАНДАРТ БЕЗОПАСНОСТИ ОС СЕМЕЙСТВА UNIX *УЧЕТНЫЕ ЗАПИСИ ПОЛЬЗОВАТЕЛЕЙ И ГРУПП*

Настройки по умолчанию. Операционная система и права доступа к файлам должны быть настроены в режиме защищенной конфигурации при использовании umask по умолчанию, что гарантирует надлежащие разрешения доступа. Все пароли, установленные вендорами по умолчанию, должны быть изменены перед промышленной эксплуатацией системы. Администрирование учетных записей пользователей и групп:

• учетные записи с привилегиями, равными привилегиям учетной записи root, запрещены;

• все идентификаторы групп и пользователей должны быть изменены таким образом, чтобы не было одинаковых учетных записей и владение учетной записью могло быть отслежено;

• выдача привилегированных учетных записей должна производиться с разрешения владельца системы;

• каждый пользователь системы должен иметь учетную запись с уникальным именем, идентификатором пользователя и паролем;

• все системные администраторы должны иметь свою собственную учетную запись;

• непосредственный доступ к учетной записи root для выполнения повседневных администраторских задач запрещен;

• только учетным записям администраторов предоставляется право повышения уровня привилегий;

• процесс регистрации в системе должен отображать данные о предыдущем входе в систему;

• неактивные учетные записи пользователей должны быть удалены;

• все пользовательские shell должны быть в списке легальных shell операционной системы;

• добавление нового shell осуществляется системными администраторами с разрешения владельца системы.

Профили пользователей. Все глобальные профили должны иметь значение umask, равное 0 2 3, то есть полный доступ – для владельца, доступ на чтение и выполнение – для членов группы владельцев и доступ на чтение – для всех остальных пользователей. Администраторы должны проверять индивидуальные профили для обеспечения целостности системы. Запрещено использовать текущую директорию в переменной shell PATH.*Политика использования паролей.* Пароли должны удовлетворять требованиям, описанным в Инструкции по использованию паролей.

Домашние директории. Домашние директории обязательны для любой учетной записи, если только это не требуется для какого-нибудь приложения.

Совместно используемые директории. Директории могут использоваться совместно несколькими учетными записями, принадлежащими к одной группе или объединенными общей функциональной потребностью. Членам такой группы разрешается доступ на запись в директорию. Группа (ее идентификатор) является собственником всех файлов и вложенных

директорий.

Совместно используемые учетные записи. Использование одной пользовательской учетной записи для совместной работы несколькими пользователями запрещено. Разрешается совместно использовать только специальные администраторские учетные записи или учетные записи для операций восстановления, при этом данные учетные записи не должны иметь права повышать свои привилегии.

Привилегированные учетные записи. Эти учетные записи имеют право повышать свои привилегии до уровня root. Совместное их использование строго запрещается. Обязательно журналирование таких учетных записей, и выданы они могут быть только системным администраторам и администраторам приложений.

Приветственное приглашение. При регистрации пользователя в системе должно появляться приветственное приглашение. Это сообщение должно иметь следующее содержание:

• эта система предназначена для использования только авторизованными пользователями;

• пользователи, использующие систему без авторизации или превысившие свои полномочия, являются нарушителями режима информационной безопасности, их действия в системе будут записаны и проанализированы системными администраторами;

• регистрация действий пользователей в системе может осуществляться при ненадлежащем использовании ими системы или при проведении регламентных работ;

• любое использование системы пользователями подтверждает правомерность мониторинга действий пользователей в системе, и, в случае нарушения режима информационной безопасности, системные администраторы вправе предоставлять записи действий пользователей в правоохранительные органы для проведения расследований.

СЕТЕВОЙ ДОСТУП УДАЛЕННЫЙ ДОСТУП

Команды удаленного управления. Удаленный доступ к системе с использованием r-команд семейства BSD для удаленного управления (rlogin, rexec) должен быть отключен, если только не существует другого способа управлять приложениями и системой. Если такой доступ необходим для выгрузки/загрузки файлов, то должна быть создана специальная учетная запись таким образом, чтобы нельзя было с ее помощью получить shell. Использование r-команд для удаленного управления запрещено. *Устройства удаленного доступа.* Установка и использование любых устройств удаленного доступа, за исключением специально предназначенных для этих целей систем, запрещены. Для указанных систем все действия регистрируются.

Удаленный доступ под учетной записью root. Непосредственный доступ в систему под учетной записью root запрещен. Администраторы должны регистрироваться в системе под своей персональной учетной записью и использовать команду su для повышения привилегий.

Удаленный доступ для привилегированных пользователей и администраторов. Все сетевые протоколы, передающие пароли в незашифрованном виде, запрещены для подключения. Такие протоколы могут быть подключены только в случае использования криптозащищенного туннеля.

Цепочка доверия. Цепочки доверия между компьютерами не должны включать системы, которые не удовлетворяют требованиям этого стандарта.

Сервис TFTP. Сервис TFTP не должен разрешать выгрузку файлов.

Сервис FTP. Запрещено использование скриптов для автоматической регистрации в FTP. Для анонимного доступа по FTP должна быть использована непривилегированная учетная запись. Разрешения на доступ к дереву каталога, используемого сервисом FTP, должны гарантировать целостность системы и запрещать неконтролируемую загрузку файлов. Если сервис доступен из Интернета, то для выгрузки файлов необходимо использовать отдельную файловую систему.

Сервис HTTP. Перед установкой Web-сереера обязательным является получение

разрешения у владельца системы. Web-приложения не должны нуждаться в административных привилегиях ни для администрирования, ни для функционирования.

Приветственное приглашение. При попытке пользователей войти в систему должно появляться приветственное приглашение. Приглашение должно отображать сообщение в формате, описанном выше. Там, где возможно, приглашение должно скрывать название операционной системы и ее версию.

ПРИЛОЖЕНИЯ

Учетные записи. Необходимо создавать учетные записи владельцев информационных ресурсов. Администраторы приложений должны иметь возможность повышения привилегий. При этом для таких учетных записей повышение привилегий до уровня root недопустимо, если только без этого приложение не будет работать. *Владение процессом сетевого сервиса.* Процессы, которые обеспечивают удаленный доступ к некоторым приложениям, не должны выполняться под привилегированными учетными записями и иметь возможность повышать привилегии учетной записи. Приложения, которые используют привилегированные порты, должны убрать такие привилегии до инициализации сетевого уровня.

Совместно используемые директории и файлы. Если файловая подсистема использует семантику BSD, то файлы и директории, совместно используемые несколькими приложениями и/или группами пользователей, должны принадлежать к определенной дополнительной группе, к которой принадлежат все авторизованные UID. Следует использовать настройки, предупреждающие неавторизованное удаление и кражу файлов. Должны быть использованы списки контроля доступа, если система предлагает расширенные механизмы безопасности из POSIX.

ЦЕЛОСТНОСТЬ СИСТЕМЫ

Сетевые сервисы. Все неиспользуемые сервисы должны быть отключены даже для локальных пользователей. Для «демонов» сетевых сервисов, которые не имеют возможности использовать списки контроля доступа, необходимо использовать TCP-упаковщики (wrappers) или подобные инструменты. Сервисы сетевого тестирования и отладки, включая echo, chargen, spray, должны быть отключены. Разрешения на доступ к файлам:

• минимальные разрешения на директории пользователей должны быть: read, write, execute – для владельца; read, execute – для группы, в которую входит пользователь; «нет доступа» – для всех остальных пользователей;

• разрешения по умолчанию не должны допускать доступа извне;

• разрешения на специальные файлы (fifos, AF_UNIX sockets, devices, memory) должны строго контролироваться;

• возможность изменять конфигурацию системы должны иметь только администраторы;

• любые файлы, которыми владеет неизвестный пользователь, должны быть удалены после проведения расследования.

Свойства монтирования файловой системы. Везде, где это возможно:

• файловые системы, выделенные для хранения данных и иерархии пользователей, должны быть смонтированы с опциями, эквивалентными nosuid и nodev;

• файловые системы, выделенные для временных областей тестирования, типа /tmp, где создание и запись файлов предоставлены всем, должны быть смонтированы с опциями, эквивалентными nosuid, nodev и noexec.

Файлы управления заданиями. Доступ к механизмам управления заданиями, таким, как at или cron, должен быть разрешен только системным администраторам или администраторам приложений. Повышение пользовательских привилегий:

• запрещено использование SUID/SGID-скриптовых shell;

• запрещено использование cheap fork/exec SUID-бинарников в качестве упаковщиков;

• повышение привилегий для упаковщиков должно использовать механизм SGID там, где это возможно;

• запрещены любые команды SUID/SGID, которые могут заканчиваться в shell escape;

• администраторы систем и приложений, обладающие возможностью повышения привилегий до уровня root, должны повышать их только с использованием упаковщиков shell, таких, как sudo, calife, super. Эти упаковщики необходимо устанавливать так, чтобы только администраторы могли выполнять набор разрешенных им команд. Должен быть организован тщательный анализ аргументов командной строки.

Журналирование. Журналы системной активности должны храниться минимум один месяц на локальных или внешних носителях информации. Для критичных журналов необходимо обеспечить маркировку и хранение за пределами предприятия. *Синхронизация времени.* Синхронизация времени должна происходить из доверенного источника.

КРИТИЧНЫЕ СИСТЕМЫ И СИСТЕМЫ, ДОСТУПНЫЕ ИЗ ИНТЕРНЕТА *УЧЕТНЫЕ ЗАПИСИ ГРУПП И ПОЛЬЗОВАТЕЛЕЙ*

Глобальные профили пользователей. Все глобальные профили пользователей должны использовать минимальную umask 0 2 7, то есть полный доступ – для владельца, read и execute – для владельца группы, «нет доступа» – для всех остальных пользователей. *Учетные записи конечных пользователей.* Учетные записи конечных пользователей запрещены. Должны быть доступны только учетные записи системных администраторов.

Обновление паролей. Все пароли должны обновляться в соответствии с политикой использования паролей.

Профили пользователей. После выхода из системы файлы, содержащие перечень введенных команд, должны быть очищены. Их содержание может быть перед этим скопировано в защищенную от доступа область для дальнейшего анализа.

УДАЛЕННЫЙ ДОСТУП

Использование r-команд BSD. Использование этих команд строго запрещено. *Удаленный доступ для привилегированных пользователей и администраторов.* Для организации такого доступа необходимо использовать механизмы шифрования. Все другие протоколы, передающие пароли открытым текстом, запрещены.

ПРИЛОЖЕНИЯ

Сетевые приложения. Сетевые приложения должны быть интегрированы и сконфигурированы таким образом, чтобы взлом приложения не привел к взлому самого сервера. *Совместно используемые директории и файлы.* Приложения должны иметь возможность осуществлять операции чтения и выполнения только над ограниченным списком файлов и директорий. Доступ на запись должен быть запрещен везде, где это возможно.

Уязвимости программного обеспечения. Системные администраторы и администраторы приложений отвечают за установку последних обновлений от производителей используемого программного обеспечения.

Инструменты разработки. Установка любых средств разработки и отладки, включая компиляторы и отладчики, запрещена.

ЦЕЛОСТНОСТЬ СИСТЕМЫ

Уменьшение поверхности атак. Все неиспользуемые сервисы должны быть отключены. *Файлы управления заданиями.* Все внешние команды в заданиях должны использовать абсолютные пути, а не относительные.

Безопасность критичных системных файлов и файлов данных:

• все критичные системные файлы и критичные файлы приложений должны регулярно проверяться по базе сигнатур (владелец, разрешения, дата последнего изменения, MD5-сумма);

• появление файлов дампов ядра должно быть немедленно обнаружено, и по этому поводу необходимо провести расследование;

• поиск, журналирование новых файлов и директорий, не представленных в базе данных, и создание отчетов о них должны быть автоматизированы и анализироваться администраторами;

• появление выполняемых или специальных файлов во временных директориях должно быть немедленно обнаружено, по этому поводу необходимо провести расследование.

Журналирование. Журналы активности приложений и системы должны храниться как минимум один месяц на локальных носителях информации и как минимум шесть месяцев на внешних. Журналы для систем типа серверов аутентификации удаленных пользователей должны храниться на внешних носителях информации в течение одного года.

Синхронизация времени. Системы должны использовать как минимум два надежных источника времени.

Свойства монтирования файловой системы. Файловые системы, используемые для /bin, /sbin, /usr, и любые другие каталоги, которые считаются статическими, должны быть смонтированы в режиме «только для чтения».

Сервисы каталогов. Использование непроверенных сервисов типа внешних DNS-серверов запрещено, если это может оказать негативное влияние на системы или сервисы.

Уязвимости программного обеспечения. Системные администраторы отвечают за установку последних обновлений от производителей используемого программного обеспечения для поддержания требуемого уровня безопасности системы.

2.2. Подход компании Sun Microsystems

Как считают в Sun, политика безопасности является необходимой для эффективной организации режима информационной безопасности компании. Здесь под политикой безопасности понимается стратегический документ, в котором ожидания и требования руководства компании к организации режима информационной безопасности выражаются в определенных измеримых и контролируемых целях и задачах. При этом Sun рекомендует реализовать подход «сверху-вниз», то есть сначала разработать политику безопасности, а затем приступать к построению соответствующей архитектуры корпоративной системы защиты информации. В противном случае политика безопасности будет создана сотрудниками службы автоматизации произвольно. При этом архитектура корпоративной системы защиты информации будет разрозненной, затратной и далеко не оптимальной.

Определение ролей и обязанностей. К разработке политики безопасности рекомендуется привлечь сотрудников таких подразделений компании, как:

• управление бизнесом,
• техническое управление,
• отдел защиты информации,
• департамент управления рисками,
• департамент системных операций,
• департамент разработки приложений,
• отдел сетевого администрирования,
• отдел системного администрирования,
• служба внутреннего аудита и качества,
• юридический отдел,
• отдел кадров.

2.2.1. Структура политики безопасности

Рекомендуемая структура документов политики безопасности:

• описание основных целей и задач защиты информации,
• определение отношения руководства компании к политике безопасности,
• обоснование путей реализации политики безопасности,
• определение ролей и обязанностей ответственных за организацию режима информационной безопасности в компании,
• определение требуемых правил и норм безопасности,
• определение ответственности за нарушение политики,

• определение порядка пересмотра и контроля положений политики безопасности.

Основное назначение политики безопасности. Основное назначение политики безопасности – информирование сотрудников и руководства компании о существующих требованиях по защите информационных активов компании. Политика также определяет механизмы и способы, используемые для достижения выполнения этих требований. Для этого в политике безопасности должны быть определены показатели и критерии защищенности активов компании, в соответствии с которыми будут приобретаться и настраиваться средства защиты. Политика также служит основой для последующей разработки стандартов, процедур, регламентов безопасности. *Связь со стандартами и процедурами безопасности.* Политика безопасности содержит ожидания руководства по обеспечению безопасности, цели и задачи организации режима информационной безопасности. Для того чтобы быть практичной и осуществимой, политика безопасности должна реализовываться в процедурах, руководствах и стандартах, обеспечивающих детальную интерпретацию положений политики безопасности для сотрудников, партнеров и клиентов компании. При этом рекомендуется начинать разработку стандартов, процедур и руководств безопасности после принятия политики безопасности и внедрения соответствующих механизмов контроля выполнения ее требований.

Основные идеи политики безопасности. К основным идеям политики безопасности относятся:

определение ценности информационных активов;

Разработка политики безопасности компании основана на необходимости защиты ценных информационных активов компании. Это означает, что нужно уделить пристальное внимание категорированию информационных ресурсов, определению их владельцев, определению критически важных для компании информационных потоков.

управление остаточными рисками;

Для создания реалистичной политики безопасности компании необходимо, чтобы она была адекватной целям и задачам развития бизнеса компании. Для этого нужно воспользоваться концепцией управления информационными рисками. В теории управления финансами категория риска определяется следующим образом:

$R = H \times P,$

где Н – денежная оценка ущерба в результате инцидента; Р – вероятность инцидента.

Представим, например, защиту источника питания хранилища данных некоторого коммерческого банка. Источник питания стоит 10 млн. долларов. Если принять вероятность полного разрушения источника питания, например в результате теракта, как 1:1 000 000 000, то риск будет равен произведению этих величин и составит всего 1 цент. Теперь представим персональный счет клиента, который защищен лишь 4-значным пин-кодом. Вероятность подбора такого кода равна 0,001. Если представить, что средняя сумма на балансе составляет 3 тыс. долларов, то риск составит 30 центов. То есть риск взлома банковского счета может быть в 30 раз выше риска потери источника питания стоимостью 10 млн. долларов.

Следует сказать, что задача управления рисками состоит не в том, чтобы определять риск исключительно количественно с высокой точностью и достоверностью. Здесь достаточно просто понимания природы риска и определения такой метрики риска, которая позволяет измерять, сравнивать, наблюдать и оптимизировать остаточные риски компании и тем самым устанавливать, насколько политика безопасности соответствует требованиям бизнеса.

управление информационной безопасностью;

Необходимо четко представлять, что только одна компонента корпоративной системы защиты информации (пусть даже самая важная) не обеспечит приемлемую безопасность информационных активов компании. Политики безопасности будут эффективны только в контексте целостной архитектуры безопасности, то есть все системы контроля доступа, межсетевые экраны, криптосистемы, системы управления ключами и другие средства защиты информации должны работать как единое целое.

обоснованное доверие.

Доверие – основа всех деклараций безопасности компании. Для доверия нужно понимать и принимать основные положения политики безопасности и обладать уверенностью в том, что они отвечают заявленным ожиданиям руководства компании. *Принципы безопасности.* Формулирование принципов обеспечения информационной безопасности является первым важным шагом при разработке политики безопасности, так как они определяют сущность организации режима информационной безопасности компании. К ним относятся принципы:

- *ответственности* – ответственность за обеспечение безопасности информационных систем компании должна быть явно определена;
- *ознакомления* – собственники информации, пользователи информационных систем, а также клиенты и партнеры по бизнесу должны быть проинформированы о правилах утвержденной политики безопасности компании, а также о степени ответственности при работе с конфиденциальной информацией компании;
- *этики* – обеспечение информационной безопасности компании должно осуществляться в соответствии со стандартами этики, применимыми к деятельности компании;
- *комплексности* – политики, стандарты, практики и процедуры безопасности должны охватывать все уровни обеспечения безопасности: нормативно-методический, экономический, технологический, технический и организационно-управленческий;
- *экономической оправданности* – обеспечение безопасности компании должно быть экономически оправданным;
- *интеграции* – политики, стандарты, практики и процедуры безопасности должны быть скоординированы и интегрированы между собой;
- *своевременности* – обеспечение безопасности компании должно позволять своевременно реагировать на угрозы безопасности и парировать их;
- *пересмотра* – регулирующие документы в области безопасности компании должны периодически пересматриваться и дополняться;
- *демократичности* – обеспечение безопасности информационных активов компании должно осуществляться в соответствии с принятыми нормами демократии;
- *сертификации и аккредитации* – информационные системы компании и компания в целом должны быть сертифицированы на соответствие требованиям безопасности. Сотрудники компании, ответственные за организацию режима информационной безопасности, должны быть сертифицированы и внутренними приказами руководства компании допущены к исполнению своих должностных обязанностей;
- *парирования злоумышленника* – стратегии и тактики обеспечения безопасности, а также соответствующие технические решения должны быть адекватны уровню нападения различного рода злоумышленников;
- *наименьших привилегий* – сотрудникам компании должны быть предоставлены привилегии, необходимые для выполнения служебных обязанностей, и не более того;
- *разделения привилегий* – привилегии сотрудников компании должны быть распределены таким образом, чтобы предупредить возможность нанесения ими умышленного или непреднамеренного ущерба критически важным информационным системам компании;
- *непрерывности* – должна быть обеспечена требуемая непрерывность бизнеса компании в случае чрезвычайных ситуаций;
- *простоты* – должно быть отдано предпочтение более простым средствам и технологиям обеспечения безопасности.

Простота политики безопасности. Ключ к успеху политики безопасности – ее простота. В связи с тем, что современные информационные технологии, программное обеспечение и оборудование быстро и постоянно совершенствуются и изменяются, политика безопасности должна быть независима от определенных программных и аппаратных

решений. В добавление к этому должны быть явно описаны механизмы изменения политики безопасности. *Доведение политики безопасности.* После создания политики безопасности она должна быть доведена до сведения сотрудников компании, ее партнеров и клиентов. При этом желательно доводить политику безопасности через подпись, подтверждающую сам факт ознакомления с политикой безопасности, а также означающую, что все требования политики безопасности понятны и их обязуются выполнять.

Пересмотр политики безопасности. Необходимо организовать процесс периодического пересмотра политики безопасности для того, чтобы ее положения не устаревали. В этот процесс должен быть включен механизм внесения изменений. Компания Sun рекомендует создать экспертную группу из сотрудников компании, которые будут нести ответственность за регулярный пересмотр политики безопасности, проверку положений политики безопасности на практике, а также, при необходимости, внесение изменений.

Реализация в информационных системах. После создания политики безопасности, а также соответствующих процедур безопасности эти процедуры могут быть реализованы в информационных системах компании. Например, в системах, основанных на технологии Java, некоторые требования политики безопасности могут обусловить необходимость установки дополнительных криптопровайдеров сторонних производителей, в то время как другие требования политики безопасности могут быть реализованы встроенной в Java библиотекой Security API. Следует подчеркнуть, что выполнение требований политики безопасности в системах обработки данных не является достаточным для поддержки доверия клиентов: нельзя гарантировать безопасность без правильной организации обработки данных.

Этапы разработки политики безопасности. Компания Sun рекомендует разрабатывать политику безопасности компании на основе лучших практик, описанных в известных стандартах безопасности, например ISO 17799:2005. При этом рекомендуются следующие этапы разработки политики безопасности:

определение основных целей и задач развития бизнеса компании;

Определение основных целей и задач развития бизнеса компании важно для определения области применения политики безопасности. Необходим соответствующий уровень согласия внутри компании, гарантирующий, что политика безопасности надлежащим образом отображает требования безопасности, адекватные целям и задачам развития бизнеса компании. Здесь важно понимать, кто будет определять политику безопасности компании и кто будет заниматься ее реализацией и поддержкой. Команда разработчиков политики безопасности должна быть представительной и, как минимум, включать сотрудников отдела защиты информации, юридического отдела, отдела кадров, отдела внутреннего аудита и качества, отдела системных операций и отдела программных разработок.

описание основных принципов безопасности;

Описание основных принципов обеспечения информационной безопасности компании позволяет простым и понятным языком, не вдаваясь в технические детали, сформулировать основные ценности компании и необходимость их защиты.

классификация и категорирование информационных ресурсов;

В основе любой политики безопасности лежит определение ценности информационных активов компании. Классификация и категорирование информационных ресурсов компании позволяет быстро и качественно принять решение о необходимой степени защищенности этих ресурсов.

анализ информационных потоков;

Цель анализа информационных потоков – определить все критичные точки обработки данных компании. Например, в системе обработки транзакций данные могут перемещаться через Web-браузеры, серверы данных и межсетевые экраны и могут храниться в базах данных, на магнитных носителях и на бумаге. Отслеживая информационные потоки, можно определить состав и структуру соответствующих средств защиты информации.

определение основных угроз и модели нарушителя;

Разработка модели угроз и модели нарушителя позволяет решить, какие типы угроз существуют в информационных системах компании, какова вероятность реализации угроз и каковы их последствия, а также стоимость восстановления.

определение сервисов безопасности;

Определение сервисов безопасности компании, например журналирования, авторизации, идентификации, аутентификации и пр., позволяет правильно выработать политику безопасности.

создание шаблона политики безопасности;

Структура политики безопасности может быть различна. Этот шаг используется для четкого определения разделов политики безопасности компании.

определение области действия политики безопасности.

Последний этап перед созданием первых черновых вариантов политики безопасности – определение всех областей, на которых фокусируется политика безопасности. Например, могут быть определены политики безопасности: – категорирования информационных ресурсов,

– доступа к информационным ресурсам,
– использования паролей,
– использования шифрования и управления ключами,
– сетевой безопасности,
– физической безопасности,
– работы с электронной почтой,
– реагирования на инциденты в области безопасности,
– мониторинга и аудита безопасности,
– межсетевого экранирования,
– антивирусной защиты,
– управления системами и сетями,
– контроля действий сотрудников,
– резервного копирования,
– допуска сторонних организаций,
– разработки и внедрения приложений,
– управления конфигурациями,
– обнаружения вторжений и пр.

Шаблон политики безопасности. Компания Sun рекомендует использовать следующий шаблон политики безопасности: • *разделы:* делается краткий обзор основных разделов политики безопасности;

• *заявление о назначении:* почему нужна политика безопасности;
• *область действия:* какова область действия политики безопасности;
• *заявление политики:* каковы специфические особенности политики безопасности;
• *обязанности:* кто и что должен делать;
• *аудитория:* на кого ориентирована политика безопасности;
• *внедрение:* кто отвечает за внедрение политики безопасности; кто отвечает за нарушения политики безопасности;
• *исключения:* описание возможных исключений;
• *другие соглашения:* описание дополнительных соглашений;
• *доведение:* кто отвечает за доведение политики безопасности до сотрудников; каков процесс доведения;
• *процесс пересмотра и обновления:* кто отвечает за пересмотр и обновление политики безопасности; что представляет собой процесс пересмотра; по каким причинам это происходит; периодичность пересмотра политики безопасности (например, ежегодно или при возникновении проблемы);
• *осуществление политики:* кто отвечает за осуществление политики безопасности; как

это выполняется;

• *мониторинг соответствия:* как выполняется мониторинг соответствия политики безопасности требованиям бизнеса.

2.2.2. Пример политики безопасности

Введение

...

Во введении должны быть описаны основные цели и задачи политики безопасности.

Основной целью настоящей политики безопасности является предоставление гарантий защиты информации на всех основных этапах жизненного цикла информационной системы компании. Политика безопасности применима ко всем компонентам информационной системы компании и содержит следующие разделы:

• Состав и структура информационных активов компании;
• Классификация и категорирование информационных активов;
• Определение владельцев информационных активов;
• Анализ угроз и информационных рисков;
• Выработка требований к защите конфиденциальной информации;
• Определение принципов, подходов и способов организации требуемого режима информационной безопасности;
• Создание требуемого режима информационной безопасности компании;
• Поддержка режима информационной безопасности компании.

...

Далее следует краткое изложение политики безопасности. Здесь важно показать позицию руководства компании по вопросу организации режима информационной безопасности.

Настоящая политика безопасности определяет общие цели и задачи компании по обеспечению информационной безопасности и управлению информационными рисками. Утверждается руководством компании и является обязательной для исполнения всеми сотрудниками, партнерами и клиентами компании. Вводная часть политики безопасности может быть описана следующим утверждением: «Доступ к конфиденциальной информации компании предоставляется только авторизованным сотрудникам и пользователям компании для выполнения своих служебных обязанностей».

Нарушение политики и ответственность

...

В этом пункте описывается, что является нарушением политики безопасности, а также степень ответственности за нарушения политики безопасности.

Нарушение настоящей политики безопасности может привести к тяжелым последствиям для компании, в частности к невозможности предоставлять услуги, поддерживать целостность, конфиденциальность и доступность данных и пр.

Преднамеренные действия сотрудников компании, которые привели к нарушению настоящей политики безопасности, влекут за собой дисциплинарные наказания. Преднамеренные или повторяющиеся нарушения политики безопасности, имеющие тяжелые последствия, могут быть приняты как основание к увольнению сотрудника или расторжению контракта, если нарушение произошло по вине клиента или вендора. Все сотрудники

компании обязаны строго выполнять требования настоящей политики безопасности.

Область действия политики безопасности

...

Область действия политики безопасности определяется руководством компании и описывает границы ее применимости.

Действие настоящей политики безопасности распространяется на:

- *сотрудников компании* с полной и частичной занятостью, обладающих правами доступа к конфиденциальным ресурсам компании;
- *вендоров,* обладающих правами доступа к конфиденциальным ресурсам компании;
- *клиентов и партнеров,* обладающих правами доступа к конфиденциальным ресурсам компании.

Использование информации

...

Кратко описывается порядок использования информации.

Все сотрудники компании, обладающие правами доступа к конфиденциальной информации компании, должны ее обрабатывать в соответствии с требованиями настоящей политики безопасности. Для надлежащей защиты информации должны быть использованы механизмы идентификации, аутентификации и авторизации.

Каждый сотрудник, ответственный за сохранение конфиденциальной информации компании, должен обеспечить надлежащую маркировку информации и использовать рекомендуемые средства защиты информации.

Передача информации

...

Кратко описывается порядок передачи информации по сети.

Передача данных по сети компании осуществляется в соответствии с требованиями настоящей политики безопасности.

Хранение информации

...

Описывается подход к хранению информации.

Хранение данных в сети компании осуществляется в соответствии с требованиями настоящей политики безопасности.

Уничтожение носителей информации

...

Описывается подход к уничтожению носителей информации.

Уничтожение носителей информации осуществляется в соответствии с процедурой отдела безопасности компании.

Утверждения политики безопасности

...

Этот пункт содержит детальное описание основных положений политики информационной безопасности компании.

Цели

...

Цели описывают административные задачи политики безопасности и почему она необходима.

Цели создания этой политики:

• разработать и довести до сотрудников компании требования по защите конфиденциальной информации компании;

• гарантировать безопасность, целостность и доступность конфиденциальных данных компании;

• установить базовый уровень защиты информации в компании.

Состав и структура информационной системы

...

Содержится описание состава и структуры информационной системы компании.

Обязанности по защите информации

...

Определение обязанностей компании по защите информации является важной задачей.

К названным обязанностям относятся следующие:

• все организационные бизнес-единицы и структуры компании должны гарантировать, что их сотрудники действуют в соответствии с настоящей политикой безопасности;

• отделы сетевых операций и системного администрирования должны гарантировать, что ведутся и надежно хранятся журналы и аудиторские записи о предоставлении доступа к конфиденциальной информации компании;

• отделы безопасности информации, сетевых операций и системного администрирования должны гарантировать выполнение всех необходимых механизмов обеспечения безопасности;

• отдел управления рисками отвечает за корректную классификацию информации для выполнения требований безопасности;

• отдел внутреннего аудита отвечает за регулярные проверки правильности классификации информации и защищенности компонент информационной системы компании.

Другие обязанности

...

Важно, чтобы политика безопасности детализировала обязанности отдельных отделов и/пли групп сотрудников.

К другим обязанностям относятся следующие:

• все партнеры компании, вендоры, провайдеры и сторонние организации, которые участвуют в процессе обработки конфиденциальной информации компании, должны руководствоваться четко документированной политикой безопасности для сторонних организаций;

• все партнеры компании, вендоры, провайдеры и сторонние организации, которые имеют доступ к конфиденциальной информации компании, должны подписать соглашение об обязательном исполнении настоящей политики безопасности.

Документирование

...

Документирование гарантирует, что политика безопасности принята к действию и соблюдается на рабочих местах в компании.

Политика безопасности компании требует разработки, внедрения и исполнения процедур безопасности. Должна быть разработана документация по управлению пользовательскими идентификаторами на рабочих станциях, по управлению списками контроля доступа на рабочих местах компании, по сбору и анализу системных журналов и журналов приложений, ведения отчетности по реагированию на инциденты и пр.

Пересмотр политики

...

Пересмотр политики безопасности должен выполняться как минимум ежегодно для поддержания ее актуальности.

Обязанность по периодическому пересмотру политики безопасности возлагается на службу безопасности. В связи с быстрым изменением информационных технологий политика безопасности должна пересматриваться не реже одного раза в год. В группу по пересмотру политики безопасности компании должны входить высшее руководство компании, сотрудники службы безопасности, отдела системного администрирования и юридического отдела.

Содержание информации

...

Далее описываются типы информации и как они могут быть использованы.

Содержание обрабатываемой в компании информации зависит от специфики ведения бизнеса компании. При этом, независимо от конкретного содержания информации, положения политики безопасности должны быть выполнены.

Классификация информации

...

Классификация информации – основа любой политики безопасности компании.

Служба безопасности отвечает за надлежащую классификацию информационных активов компании.

Вся обрабатываемая информация компании подразделяется на следующие виды:

• *информация открытого доступа или публичная информация;*

Информация, которая доступна как внутри компании, так и за ее пределами. Разглашение, использование или уничтожение такой информации не нанесет ущерба компании (пример: новости о компании, стоимость ее акций).

• *экономически ценная информация или собственность компании;*

Информация, не подлежащая разглашению за пределами компании, она защищается компанией по требованиям контрактов или законодательных актов. Если такая информация будет разглашена, то она потеряет свою экономическую ценность. Большая часть информации в компании должна попадать в эту категорию. Копирование и передача такой информации могут быть разрешены только определенному списку сотрудников внутри компании. Разглашение подобной информации за пределами компании должно осуществляться только с письменного разрешения лица, ответственного за надлежащее обращение с названной информацией (пример: политики компании, планы продаж, исходный код программы).

• *конфиденциальная информация;*

Информация, которая не должна быть разглашена независимо от ее экономической ценности. Разглашение, использование или уничтожение такой информации нанесет ущерб компании. Эта классификация применяется к информации, которая доступна только строго ограниченному списку сотрудников. Копирование такой информации и ее передача другому лицу разрешается только владельцем информации (пример: стратегические планы развития компании, ключи шифрования).

• *конфиденциальная информация клиентов и партнеров компании;*

Информация клиентов и партнеров, к которой имеет доступ только строго определенный список лиц. Разглашение, использование или уничтожение такой информации нанесет ущерб компании и ее отношениям с клиентами и партнерами. Информация этого типа может храниться в системах обработки информации компании, но при этом не иметь владельца (пример: банковские реквизиты клиента, ключи шифрования).

• *публичная информация клиентов и партнеров компании.*

Информация клиентов и партнеров, к которой имеют доступ как сотрудники компании, так и любые лица за пределами компании. Разглашение, использование или уничтожение такой информации не нанесет ущерба клиентам и партнерам или самой компании (пример: сообщения электронной почты, сертификат открытого ключа).

Определение собственника информации

...

Является необходимым шагом для корректной классификации информации компании.

Для корректной классификации информации необходимо определить ее владельца. Если владелец информации не может быть определен, то собственником и хранителем информации назначается служба безопасности компании.

Вся информация, не классифицированная ее владельцем, должна быть определена как конфиденциальная информация клиента или как собственность компании.

Служба безопасности компании отвечает за разработку, реализацию и поддержку процедуры по определению ценной информации компании и ее владельцев.

Соглашение о неразглашении конфиденциальной информации

...

Использование соглашения о неразглашении конфиденциальной информации компании необходимо для надлежащей защиты информационных активов компании. Использование названного соглашения зависит от действующего законодательства.

В случае необходимости передачи конфиденциальной информации компании за ее пределы, например при аудиторской проверке, должно быть подписано соответствующее соглашение о неразглашении конфиденциальной информации компании.

Декларация принципов безопасности

...

Декларация принципов безопасности позволяет концептуально определить основные цели и задачи организации режима информационной безопасности компании независимо от используемых информационных технологий и технологий защиты информации. Принципы безопасности зависят от целей и задач бизнеса конкретной компании.

Основные принципы безопасности компании могут быть описаны в терминах отчетности, авторизации и доступности.

2.3. Подход компании Cisco Systems

С точки зрения специалистов Cisco, отсутствие сетевой политики безопасности может привести к серьезным инцидентам в области безопасности. Разработку политики безопасности компании рекомендуется начинать с оценки рисков сети и создания рабочей группы по реагированию на инциденты.

2.3.1. Описание политики безопасности

Создание политик использования. Компания Cisco рекомендует создать политики использования, которые описывают роли и обязанности сотрудников компании для надлежащей защиты конфиденциальной информации. При этом можно начать с разработки главной политики безопасности, в которой четко прописать общие цели и задачи организации режима информационной безопасности компании.

Следующий шаг – создание политики допустимого использования для партнеров, чтобы проинформировать партнеров компании о том, какая информация им доступна. Следует четко описать любые действия, которые будут восприниматься как враждебные, а также возможные способы реагирования при обнаружении таких действий.

В заключение необходимо создать политику допустимого использования для администраторов, чтобы описать процедуры администрирования учетных записей сотрудников и проверки привилегий. При этом если компания имеет определенную политику относительно использования паролей или категорирования информации, то нужно ее здесь упомянуть. Далее необходимо проверить названные политики на непротиворечивость и полноту, а также убедиться в том, что сформулированные требования к администраторам нашли свое отображение в планах по обучению.

Проведение анализа рисков. Назначение анализа рисков состоит в том, чтобы категорировать информационные активы компании, определить наиболее значимые угрозы и уязвимости активов и обоснованно выбрать соответствующие контрмеры безопасности. Подразумевается, что это позволит найти и поддерживать приемлемый баланс между безопасностью и требуемым уровнем доступа к сети. Различают следующие уровни информационных рисков:

- *низкий уровень* – информационные системы и данные, будучи скомпрометированными (доступны для изучения неавторизованными лицами, повреждены или утеряны), не приведут к серьезному ущербу, финансовым проблемам или к проблемам с правоохранительными органами;
- *средний уровень* – информационные системы и данные, будучи скомпрометированными (доступны для изучения неавторизованными лицами, повреждены или утеряны), приведут к умеренному ущербу или к небольшим проблемам с правоохранительными органами, или к умеренным финансовым проблемам, а также к

получению дальнейшего доступа к другим системам. Затронутые системы и информация требуют умеренных усилий по восстановлению;

- *высокий уровень* – информационные системы и данные, будучи скомпрометированными (доступны для изучения неавторизованными лицами, повреждены или утеряны), приведут к значительному ущербу или к серьезным проблемам с правоохранительными органами, или к финансовым проблемам, нанесению ущерба здоровью и безопасности сотрудников. Системы и информация требуют существенных усилий по восстановлению.

Рекомендуется определить уровень риска для каждого из перечисленных устройств: сетевые устройства, устройства мониторинга сети, серверы аутентификации (TACACS+ и RADIUS), почтовые серверы, файловые серверы, серверы сетевых приложений (DNS и DHCP), серверы баз данных (Oracle, MS SQL Server), персональные компьютеры и другие устройства. При этом считается, что сетевое оборудование, такое, как коммутаторы, маршрутизаторы, DNS– и DHCP-серверы в случае компрометации могут быть использованы для дальнейшего проникновения в сеть и поэтому должны относиться к группе среднего или высокого риска. Возможное повреждение этих устройств может привести к прекращению работы всей сети. Такие инциденты наносят серьезный ущерб компании.

После определения уровней риска необходимо определить роли пользователей в этих системах. Рекомендуется выделять следующие пять наиболее общих типов пользователей:

- *администраторы* – внутренние пользователи, отвечающие за сетевые ресурсы;
- *привилегированные пользователи* – внутренние пользователи с необходимостью большего уровня доступа;
- *рядовые пользователи* – внутренние пользователи с обычным уровнем доступа;
- *партнеры* – внешние пользователи с необходимостью доступа к некоторым ресурсам;
- *другие* – внешние пользователи или клиенты.

Определение уровней риска и типов доступа, требуемых для каждой сети, позволяет сформировать некоторую матрицу безопасности (см. табл. 2.1). Эта матрица безопасности является стартовой точкой для дальнейших шагов по обеспечению безопасности, например таких, как создание соответствующей стратегии по ограничению доступа к сетевым ресурсам. Таблица 2.1. Матрица безопасности Cisco

Система	Описание	Уровень риска	Типы пользователей
АТМ-коммутаторы	Основные сетевые устройства	Высокий	Сетевые администраторы
Сетевые маршрутизаторы	Сетевые устройства распределения	Высокий	Сетевые администраторы
Коммутаторы доступа	Сетевые устройства доступа	Средний	Сетевые администраторы
ISDN- или dial up-серверы	Сетевые устройства доступа	Средний	Сетевые и системные администраторы
Межсетевые экраны	Сетевые устройства доступа	Высокий	Администраторы безопасности
Серверы DNS и DHCP	Сетевые приложения	Средний	Сетевые и системные администраторы
Внешние почтовые серверы	Сетевые приложения	Низкий	Администраторы и пользователи
Внутренние почтовые серверы	Сетевые приложения	Средний	Администраторы и пользователи
Серверы баз данных Oracle	Сетевые приложения	Средний или высокий	Администраторы баз данных и пользователи

Определение состава и структуры группы сетевой безопасности. Рекомендуется создать группу сетевой безопасности под руководством менеджера по безопасности с представителями из каждой значимой бизнес-единицы компании (минимум из представителей бизнес-единиц развития, исполнения и производства и/или продаж). Члены группы должны хорошо знать политику безопасности и технические аспекты защищаемых систем и сетей. Часто это требует дополнительного обучения сотрудников названной

группы. Группа безопасности должна принимать участие в разработке политики безопасности, организации режима информационной безопасности, а также своевременно реагировать на инциденты в области информационной безопасности компании. Процесс сопровождения политик безопасности заключается в контроле и, при необходимости, пересмотре политик безопасности компании. Необходим как минимум ежегодный пересмотр политики безопасности и проведение анализа рисков.

На практике группа сетевой безопасности должна проводить анализ рисков, подтверждать запросы на проведение изменений в системе безопасности, проводить мониторинг оповещений о появлении новых уязвимостей с использованием списков рассылок вендоров и независимых аналитических центров, например CERT или SANS, а также поддерживать соответствие требованиям политики безопасности с помощью определенных технических и организационных мер.

Так как нарушения безопасности часто обнаруживаются во время проведения мониторинга сети, то члены группы сетевой безопасности должны участвовать в расследовании инцидентов и предупреждении подобных нарушений в дальнейшем. Каждый член группы безопасности должен обладать хорошими знаниями в области прикладного, системного и сетевого программного и аппаратного обеспечения систем безопасности. При этом рекомендуется определить индивидуальные роли и обязанности каждого члена группы сетевой безопасности.

...

Предупреждение. Под предупреждением нарушений компания Cisco понимает подтверждение изменений в системах безопасности и мониторинг безопасности сети.

Подтверждение изменений в системах безопасности. Изменения в системах безопасности могут быть определены как изменения в сетевом оборудовании, которые способны оказать потенциальное воздействие на состояние безопасности сети. Политика безопасности компании должна определять специфические требования конфигурации безопасности и содержать минимум технических деталей. Другими словами, вместо такого определения требования, как «не разрешены внешние FTP-соединения во внутреннюю сеть», нужно определить это требование так – «внешние соединения не должны быть способны получать файлы из внутренней сети». При этом желательно стремиться к определению уникальных требований компании. Использование стандартных шаблонов обеспечения безопасности и настроек по умолчанию в подходе компании Cisco настоятельно не рекомендуется.

Группа сетевой безопасности просматривает описанные общедоступным языком требования и определяет соответствие технического дизайна и настроек элементов сети этим требованиям. Если выявляются несоответствия, группа безопасности создает требуемые изменения сетевой конфигурации для выполнения требований политики безопасности и применяет их в дальнейшем. При этом группой сетевой безопасности могут контролироваться не все изменения. Здесь важно просмотреть изменения, наиболее значимые и существенные для сети компании в плане безопасности. Например, к ним относятся изменения:

- в конфигурации межсетевых экранов,
- в списках контроля доступа,
- в конфигурации SNMP,
- версий программного обеспечения.

Компания Cisco рекомендует следовать следующим правилам: • регулярно изменять пароли на сетевых устройствах;

- ограничить доступ к сетевым устройствам согласно утвержденному списку сотрудников;

• гарантировать, что текущая версия программного обеспечения сетевого и серверного оборудования соответствует требованиям безопасности.

В добавление к этим правилам необходимо включить представителя группы сетевой безопасности в постоянно действующую комиссию компании по утверждению изменений для отслеживания всех изменений, происходящих в сети компании. Представитель группы безопасности может запретить реализацию любого изменения, связанного с безопасностью, до тех пор, пока это изменение не будет разрешено руководителем группы сетевой безопасности. *Мониторинг сетевой безопасности.* Мониторинг сетевой безопасности фокусируется на обнаружении изменений в сети, позволяющих определить нарушение безопасности. Отправной точкой мониторинга безопасности является определение понятия «нарушение безопасности». Анализ угроз и информационных рисков позволяет определить требуемый уровень полноты мониторинга безопасности сети компании. В дальнейшем при утверждении изменений безопасности каждый раз проверяется значимость выявленных угроз сети. Оценкой этих угроз определяется объект и частота мониторинга.

Например, в матрице анализа рисков межсетевой экран определен как устройство с высоким уровнем риска. Это означает, что мониторинг межсетевого экрана должен выполняться постоянно в режиме реального времени. Из раздела подтверждения изменений безопасности следует, что необходимо выявлять все изменения в настройках конфигурации межсетевого экрана. То есть SNMP-агент должен отслеживать такие события, как отвергнутые попытки регистрации, необычный трафик, изменения на межсетевом экране, предоставление доступа к межсетевому экрану и установление соединений через межсетевой экран.

Таким образом можно создать политику мониторинга для каждой компоненты сети, определенной при проведении анализа рисков. Рекомендуется проводить мониторинг компонент сети с низким уровнем риска – еженедельно, со средним уровнем риска – ежедневно, с высоким уровнем риска – раз в час. При этом если требуется более быстрое время реагирования, то необходимо уменьшить названные временные промежутки.

Важно также определить в политике безопасности порядок уведомления членов группы сетевой безопасности о нарушениях. Как правило, средства мониторинга безопасности сети будут первыми автономно обнаруживать нарушения. Должна быть предусмотрена возможность отправки по любым доступным каналам связи уведомлений в центр реагирования на инциденты в области безопасности для оперативного оповещения членов группы сетевой безопасности.

Реагирование на нарушения. Под реагированием на нарушения в безопасности здесь понимается определение нарушений безопасности, порядка восстановления и пересмотра правил безопасности.

Нарушения безопасности. При обнаружении нарушения безопасности важно своевременно отреагировать и оперативно восстановить нормальное функционирование сервисов сети. Здесь главное правило – своевременное оповещение группы сетевой безопасности после обнаружения нарушения. Если это правило не выполняется, то реагирование будет замедлено, а следовательно, вторжение и последствия более тяжелыми. Поэтому необходимо разработать соответствующую процедуру реагирования и оповещения, действенную 24 часа в день 7 дней в неделю.

Далее необходимо четко определить уровень привилегий по внесению изменений, а также порядок внесения изменений. Здесь возможны следующие корректирующие действия:

• реализация изменений для предупреждения дальнейшего распространения нарушения,

• изолирование поврежденных систем,

• взаимодействие с провайдером для отслеживания источника атаки,

• использование записывающих устройств для сбора доказательств,

• отключение поврежденных систем или источников атаки,

• обращение в правоохранительные органы или федеральные агентства,

• выключение поврежденных систем,

• восстановление систем в соответствии со списком приоритетности,

• уведомление руководства и юристов компании.

Необходимо детализировать любые изменения в политике безопасности, которые могут быть произведены без обязательного получения разрешения от руководства. Отметим, что существуют две основные причины для сбора и хранения информации об атаках: определение последствий реализации атаки и расследование и преследование злоумышленников. Тип информации, способ сбора и обработка информации обусловлены целями реагирования на нарушения безопасности.

Для определения последствий нарушения безопасности рекомендуется осуществить следующие шаги:

• зафиксировать инцидент с помощью записи сетевого трафика, снятия копий файлов журналов, активных учетных записей и сетевых подключений;

• ограничить дальнейшие нарушения путем отключения учетных записей, отсоединения сетевого оборудования от сети и от Интернета;

• провести резервное копирование скомпрометированных систем для проведения детального анализа повреждений и метода атаки;

• попытаться найти другие подтверждения компрометации. Часто при компрометации системы оказываются затронутыми другие системы и учетные записи;

• просматривать хранимые файлы журналов устройств безопасности и сетевого мониторинга, так как они часто являются ключом для определения метода атаки.

Если необходимо произвести юридические действия, следует уведомить руководство и привлечь юристов компании для сбора соответствующих доказательств. Если нарушение было внутренним, то потребуется привлечь сотрудников отдела кадров компании. *Восстановление.* Восстановление работоспособности сервисов сети компании является конечной целью процедуры реагирования на нарушения в области безопасности. Здесь необходимо определить порядок восстановления доступности сервисов, например с помощью процедур резервного копирования. При этом надо учитывать, что каждая система имеет свои собственные механизмы резервного копирования. Поэтому политика безопасности, являясь общей для всех элементов сети, при необходимости должна позволять детализировать условия восстановления конкретного элемента. Если требуется получить разрешение на восстановление, нужно описать порядок получения разрешения в политике безопасности.

Пересмотр политики безопасности. Пересмотр политики безопасности является заключительным этапом жизненного цикла политики безопасности. Здесь важно обратить внимание на следующее. Политика безопасности должна быть «жизнеспособным» документом, адаптированным к изменяющимся условиям. Сравнение существующей политики безопасности с лучшими практиками в этой области и последующий пересмотр политики должны поддерживать в актуальном состоянии защищенность активов сети. Необходимо регулярно обращаться на Web-сайты различных независимых аналитических центров, например CERT или SANS, за полезными советами и рекомендациями по обеспечению безопасности и учитывать их в поддерживаемой политике безопасности компании.

Также рекомендуется проводить аудит безопасности сети путем обращения в соответствующие консалтинговые компании, специализирующиеся на оказании подобных услуг. Для сетей с высокими требованиями к доступности информационных ресурсов рекомендуется проведение независимого аудита безопасности как минимум раз в год. Кроме того, достаточно эффективны и внутренние тренировки для отработки действий в чрезвычайных ситуациях.

2.3.2. Пример политики сетевой безопасности

Область действия политики. Как авторизованный пользователь корпоративной сети каждый сотрудник компании обладает доступом к информации с различным уровнем

конфиденциальности. Ознакомление и соблюдение политики сетевой безопасности компании (далее – «политика») является важной обязанностью каждого сотрудника для обеспечения конфиденциальности, целостности и доступности информационных активов компании. При этом компания следует принципу «знать только то, что необходимо знать для выполнения своих служебных обязанностей».

Целевая аудитория. Политика обязательна для следующих сотрудников компании:

• рядовых пользователей сети, выполняющих свои служебные обязанности на рабочих местах;

• специалистов ИТ-службы и службы безопасности, ответственных за эксплуатацию и сопровождение информационной системы, а также за соблюдение политики безопасности;

• менеджеров, ответственных за организацию режима информационной безопасности компании;

• руководства компании, которое стремится обеспечить целостность, конфиденциальность и доступность информационных активов компании в соответствии с целями и задачами бизнеса;

• юристов и аудиторов компании, которые обеспокоены сохранением репутации компании и ответственностью компании перед клиентами и партнерами.

Область действия. Политика является частью программы компании по обеспечению безопасности ее информационных активов. Политика определяет допустимые правила доступа сотрудников, клиентов, партнеров и вендоров к открытым и конфиденциальным информационным активам в сети компании. *Юридические права.* Совет директоров уполномочен акционерами компании создать, внедрить и поддерживать политику в соответствии с требованиями государственных органов, федерального и международного законодательства. Директор (начальник) службы информационной безопасности и главный юрист компании несут ответственность за реализацию этой политики.

Заинтересованные стороны. Следующий персонал компании несет личную ответственность за создание, поддержку и внедрение политики сетевой безопасности:

• директор по финансам,
• директор по развитию,
• директор службы продаж и маркетинга,
• исполнительный директор, CEO,
• директор информационной службы, CIO,
• директор службы информационной безопасности, CISO,
• директор по сетям и телекоммуникациям,
• главный менеджер по информационным системам,
• директор службы качества и внутреннего аудита,
• главный юрист компании,
• директор службы персонала,
• директор системной поддержки и сопровождения,
• директор службы разработки приложений.

Обязанности системного администратора. Системный администратор сетевого оборудования отвечает за выполнение следующих требований: • назначение учетной записи отдельным сотрудникам (не группам);

• обеспечение уникальности учетных записей сотрудников и оборудования внутри компании;

• установка обновлений безопасности и сервисных пакетов, рекомендованных отделом информационной безопасности, в соответствии с их уровнем критичности;

• осуществление управления учетными записями и паролями;

• отключение учетных записей при увольнении сотрудников;

• хранение файлов конфигураций сетевых устройств на защищенном TFTP-сервере. Защита конфигураций от разглашения. Использование керберизованного rcp между маршрутизаторами Cisco и сервером TFTP;

• ежедневное исследование файлов журналов. Немедленное оповещение отдела информационной безопасности об инцидентах, связанных с безопасностью. Еженедельная отправка отчетов о небольших нарушениях безопасности (типа многократных неудачных попыток регистрации) в отдел информационной безопасности;

• использование средств управления и контроля сетевой безопасности для поиска «слабых» паролей, сетевых уязвимостей и средств проверки целостности файлов и системных конфигураций (таких, как Cisco IDS, Cisco Netsys, Crack, COPS, Tiger, Tripwire) на постоянной основе.

Процедура поддержки политики безопасности. Заинтересованные стороны компании должны просматривать и обновлять политику не реже одного раза в год. Отдел информационных систем под руководством отдела информационной безопасности проводит аудит сети на регулярной основе и документирует результаты проверок. *Процедура реализации.* Директор по развитию сетей и телекоммуникаций должен определить точную сетевую топологию и сетевое оборудование компании, в рамках которых будет действовать настоящая политика безопасности.

Для проверки дееспособности политики безопасности проводится аудит после установки и подключения к сети нового сетевого оборудования и компьютеров.

Обучение сотрудников. Ознакомление с политикой осуществляется в ходе первичного инструктажа сотрудников. Сотрудники должны ежегодно перечитывать и подписывать политику допустимого использования как условие продолжения их работы.

Ознакомление сотрудников для предупреждения случаев социальной инженерии. Сотрудники обязаны соблюдать осторожность при общении с людьми, не являющимися сотрудниками компании. Перед началом дискуссии следует определить границы того, что можно сообщить постороннему человеку.

Политика допустимого использования. Политика допустимого использования определяет права и порядок доступа к информационным активам компании, порядок использования разрешенных аппаратно-программных средств, а также права и обязанности сотрудников согласно накладываемым ограничениям со стороны федеральных, законодательных актов и требований руководящих документов.

Допустимое использование сети. Сотрудникам запрещается делать и распространять копии конфигурации сетевого оборудования или серверов, если они не являются системными администраторами.

Сотрудникам запрещается получать или пытаться получить административный доступ к сетевому оборудованию и серверам, если они не являются системными администраторами или если это не входит в их служебные обязанности.

Требования по соответствию. Сотрудники обязаны выполнять все требования этой политики и любых последующих ее версий. Доступ к инфраструктуре компании и ее данным является привилегией, не правом. То есть компания может изменить привилегии доступа сотрудника любым способом в любое время. К сотруднику, нарушившему эту политику, могут быть применены дисциплинарные и административные меры, вплоть до увольнения.

Политика идентификации и аутентификации. Политика идентификации и аутентификации определяет процедурные и технические методы, используемые для идентификации и аутентификации.

Руководство по управлению паролями. Следующие принципы определяют правила выбора пароля:

• пароли, если возможно, должны использовать строчные и прописные буквы, знаки препинания и числа, должны иметь длину как минимум восемь символов;

• изменять пароли следует ежеквартально;

• нельзя записывать пароли;

• нельзя сообщать пароли кому бы то ни было.

Руководство по аутентификации. Компания должна использовать защищенную базу учетных записей на основе протокола TACACS+ для аутентификации. *Политика доступа в*

Интернет. Компания осознает важность доступа сотрудников в Интернет для ведения бизнеса и принимает возможные риски, связанные с этими подключениями.

Политику доступа в Интернет определяет Руководство по доступу в Интернет.

Допустимое использование. Исходящий доступ в Интернет может быть свободно использован сотрудниками для выполнения служебных обязанностей. Должно быть определено и реализовано разумное ограничение на общее время работы в Интернете.

Политика межсетевого экрана. Межсетевой экран, состоящий как минимум из пограничного маршрутизатора и защищенного компьютера, должен быть использован для защиты от несанкционированного доступа к внутренней сети компании из Интернета. Необходимо разработать правила фильтрации пакетов для управления доступом через периметр с регистрацией попыток нарушения доступа на сервере syslog.

Политика публичных сервисов. Входящий доступ из Интернета во внутреннюю сеть компании будет запрещен, если только не используется шифрование на сетевом уровне. Входящий доступ должен быть ограничен сервисами защищенного хоста, такими, как SMTP, HTTP, FTP, DNS.

Политика доступа во внутреннюю сеть компании. Политика доступа во внутреннюю сеть компании определяет процесс выдачи прав доступа сотруднику к ресурсам.

Доверительные отношения. Доступ к компьютерам внутренней сети разрешен для всех сотрудников компании на основе уровня доверия, определяемого руководителем сотрудника. Компания старается балансировать между прозрачным доступом сотрудника к ресурсам и безопасностью сети. Компания устанавливает пять уровней доверия. Каждый сотрудник получает определенный уровень доверия в соответствии с его служебными обязанностями. Для соблюдения требуемых уровней доверия должны быть реализованы соответствующие технические средства защиты.

Доступ к компьютерам внутренней сети сторонним организациям запрещен, если специально не разрешен отделом информационных технологий и соответствующим руководителем.

Безопасность сетевого оборудования. Административный доступ к сетевому оборудованию запрещен, за исключением сотрудников отдела информационных технологий, определяемых начальником этого отдела. Для защиты управляющего трафика между внутренними серверами используется шифрование на сетевом уровне.

Политика удаленного доступа. Сотрудники, получающие доступ во внутреннюю сеть компании с домашних компьютеров или через телефонные сети общего доступа, должны четко понимать и выполнять обязанности по защите ресурсов компании при получении такого доступа.

Поэтому сотрудники, получающие этот вид доступа, несут определенную ответственность. Компьютер, с которого сотрудник получает удаленный доступ в сеть, должен быть защищен паролем и сконфигурирован таким образом, чтобы не допустить доступ посторонних во внутреннюю сеть компании.

Аутентификация удаленного доступа должна происходить с использованием TACACS+ или токенов.

Мобильные компьютеры. Сотрудники компании, нуждающиеся в удаленном доступе в сеть компании с мобильных компьютеров, получают такой доступ через серверы сетевого доступа, находящиеся под управлением отдела информационных технологий. Сотрудники должны использовать компьютеры с операционными системами Windows 95, Windows 98, Windows 2000 или Apple Macintosh с программным обеспечением для организации удаленного доступа, утвержденным отделом информационных технологий.

Сотрудники компании и сторонние организации могут использовать телефонные сети общего доступа для получения доступа во внутреннюю сеть компании, при этом обязательно должны использоваться одноразовые (one-time) пароли.

Сотрудники, имеющие привилегию удаленного доступа по телефонным сетям общего пользования, несут ответственность за то, что никто кроме них не получит доступа в сеть

компании, используя их соединение.

Доступ из дома. Сотрудники компании, желающие организовать домашние офисы, могут использовать удаленный доступ к сети компании. По возможности, удаленные подключения должны использовать метод аутентификации CHAP.

Соглашение с сотрудниками, работающими вне офиса. Сотрудники, получающие привилегию удаленного доступа в сеть компании, подписывают документ, в котором определяется важность защиты информации компании от разглашения. Документ также должен определять их ответственность за выполнение всех политик безопасности компании.

Доступ филиалов. Для обеспечения безопасности внутренней сети компании доступ в нее филиалов определяется и разрешается отделом информационных технологий.

Доступ бизнес-партнеров. Для обеспечения безопасности внутренней сети компании порядок получения доступа в нее партнеров определяется и разрешается отделом информационных технологий. Для управления и защиты такого подключения должен быть использован межсетевой экран.

Политика шифрования. Для всех видов удаленного доступа необходимо использовать шифрование. Выбор алгоритма шифрования основывается на достижении баланса между конфиденциальностью передаваемых данных и требуемой скоростью передачи.

Процедура описания инцидентов. Все заинтересованные в выполнении данной политики лица совместно разрабатывают детальную и содержащую планы по обеспечению непрерывности бизнеса процедуру описания всех инцидентов, связанных с безопасностью. Процедура описания инцидентов должна представлять собой «книгу рецептов» на все случаи жизни, так, чтобы любой инцидент мог быть обработан определенным образом отделом информационных систем при выполнении ими своих повседневных обязанностей. В процедуре должны быть учтены все вопросы, затрагиваемые этой политикой.

Требования к системам обнаружения вторжений. Для получения важной и своевременной информации о состоянии защиты сетевого периметра должны быть внедрены системы обнаружения вторжений, такие, как Cisco IDS.

Системы обнаружения вторжений уровня предприятия, работающие в режиме реального времени, разработанные для обнаружения, журналирования и ограничения несанкционированной активности, должны обладать следующими возможностями:

• возможностью мониторинга демилитаризованной зоны и соответствующей производительностью для этого;

• возможностью быстрого и беспроблемного внедрения в растущую сеть (для этого системы обнаружения вторжений должны быть реализованы в виде многоуровневой архитектуры);

• возможностью удаленного администрирования системы обнаружения вторжений через интуитивно понятный графический интерфейс, интегрированный в систему управления сетью. Это гарантирует целостность внедрения политики безопасности на уровне компании;

• возможностью сохранять события в базе данных. Должна быть возможность сохранения информации об источнике, типе, цели и времени атаки для последующего детального исследования.

Процедура реагирования на инциденты. Начальник отдела информационных систем создает детальную процедуру реагирования на инциденты, и этот документ следует пересматривать и обновлять один раз в квартал или в течение одной недели после крупного инцидента. Вице-президент по информационным системам и начальник отдела информационной безопасности подписывают и утверждают данный документ. Процедура реагирования на инциденты должна определять реакцию компании при возникновении инцидента, так что в случае возникновения инцидента можно было бы сразу приступить к нейтрализации и уменьшению проблемы, а не решать, как с ней бороться. В процедуре реагирования на инциденты должны быть описаны следующие моменты: • *подготовка и планирование* – персонал отдела информационных систем должен минимум 16 часов

ежегодно обучаться обнаружению и нейтрализации инцидентов. Процедура определяет тип и длительность тренингов;

• *определение инцидентов* – системные администраторы должны проводить мониторинг системы обнаружения вторжений несколько раз в день. Системные журналы следует просматривать один раз в час и в конце рабочего дня. Дежурный старший системный администратор несет ответственность за обнаружение и реагирование на инцидент. Процедура реагирования на инциденты должна определять уровни приоритетов инцидентов так, как предлагается в RFC 2196, «Site Security Handbook»;

• *обработка инцидента* – процедура реагирования на инциденты определяет, как администратор будет обрабатывать инцидент. Ниже описаны шаги по обработке и документированию:

– определение типа и приоритета атаки;
– определение времени начала и окончания атаки;
– определение источника атаки;
– определение затронутых атакой компьютеров и сетевых устройств;
– журналирование атаки;
– попытка остановить атаку или уменьшить ее последствия;
– изолирование затронутых систем;
– уведомление соответствующих контактных лиц;
– защита доказательств атаки (файлов журналов);
– восстановление работоспособности сервисов;

• *документирование* – под руководством директора службы информационных технологий должен быть создан отчет об инциденте, в котором необходимо отразить следующие вопросы:

– инвентаризация ценности затронутых атакой систем;
– описание атаки;
– пересмотр политики сетевой безопасности (при необходимости);
– поиск и наказание злоумышленников.

Таблица 2.2. Члены команды по реагированию на инциденты

Контактное лицо	Роль
Дежурный старший системный администратор	Первая точка контакта по определению и реакции на инцидент Документирование инцидента в отчете
Главный менеджер по информационным системам	Первая точка контакта среди руководителей Определяет, как реагировать на инцидент Координирование действий системных администраторов в случае серьезных инцидентов Должен быть доступен 24 часа в сутки Контактирует со следующей персоной по командной цепочке
Начальник отдела информационной безопасности	Эскалация инцидента команде по реагированию на инциденты, такой, как CERT Подключение к работе правоохранительных органов
Вице-президент по информационным системам и начальник отдела информационных систем	Работают с руководством по взаимодействию внутри и за пределами компании Только они имеют полномочия по выступлению перед представителями прессы и внешними организациями Гарантируют, что реагирование на инцидент задокументировано и внесены соответствующие изменения в процедуры для недопущения повторения подобных инцидентов
Главный юрист	Координирует судебное преследование злоумышленников Рассматривает и подтверждает разрешение на общение с прессой и внешними организациями

2.4. Подход компании Microsoft

Компания Microsoft обладает сложной корпоративной инфраструктурой, которая состоит из 6 тыс. серверов Windows Server 2003 (из них 800 серверов приложений). В штате компании работает более 55 тыс. сотрудников. Сотрудники очень хорошо готовы технически, и 95 % из них имеют администраторские права на своих компьютерах. Более

чем 300 тыс. компьютеров компании расположены в 400 представительствах по всему миру, используется более 1,6 тыс. приложений.

В сеть компании ежедневно поступает приблизительно 8 млн. почтовых сообщений извне, и приблизительно 6,5 млн. почтовых сообщений циркулирует ежедневно в сети самой компании. В сеть компании имеют доступ 30 тыс. партнеров. Уникальная инфраструктура по разработке продуктов, тестированию и поддержке, исходный код продуктов требуют особой защиты. Ежемесячно на сеть компании осуществляется свыше 100 тыс. попыток вторжения. В почтовую систему ежемесячно поступает свыше 125 тыс. почтовых сообщений, зараженных вирусами (в день примерно 800 новых вирусов), и 2,4 млн. почтовых сообщений со спамом в день.

Обязанность по обеспечению информационной безопасности в компании Microsoft возложена на две группы – Corporate Security Group и Operations and Technology Group.

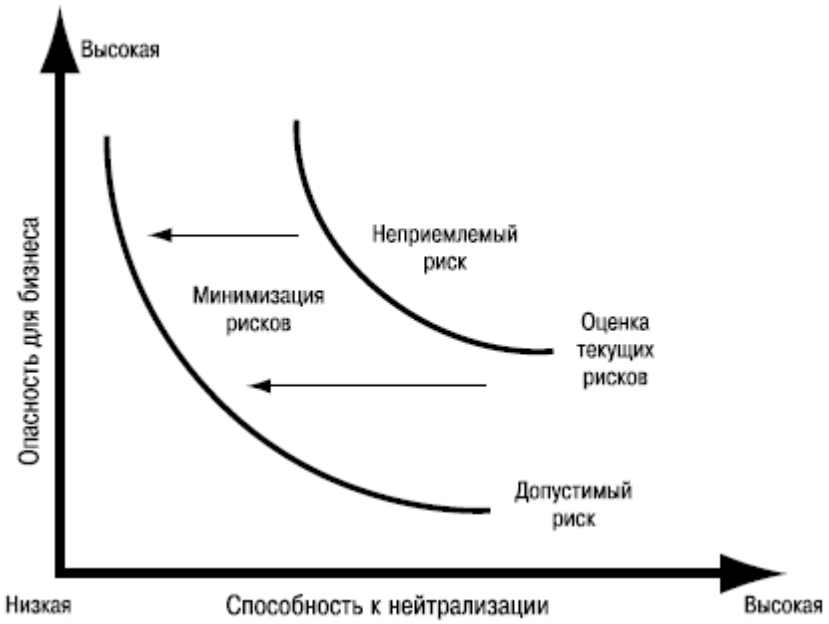
Компания Microsoft разработала стратегию безопасности, состоящую из 4 основных компонент:

- миссия корпоративной безопасности,
- принципы операционной безопасности,
- модель принятия решений, основанная на анализе рисков,
- тактическое определение приоритетности действий по уменьшению рисков.

Фундаментом для дизайна, разработки и нормального функционирования защищенных систем являются принципы безопасности, разделенные на несколько категорий (см. табл. 2.3). Таблица 2.3. Принципы безопасности защищенных систем

Категория	Принцип безопасности
Организационная Направлена на получение поддержки руководства по управлению рисками и ознакомление с вопросами безопасности	Управление рисками в соответствии с задачами бизнеса Определение ролей и обязанностей Инвестиции в дизайн защищенности Обеспечение безопасности операций
Пользователи и данные Включает аутентификацию, защиту данных пользователей, авторизацию	Управление принципом наименьших привилегий Классификация данных и их использование Внедрение защиты данных и идентичности пользователя Защита информации Гарантия целостности данных Мониторинг гарантии идентичности Доступность
Разработка приложений и систем Выделена для дизайна и разработки защищенных систем	Встраивание безопасности в жизненный цикл Дизайн «многоуровневой защиты» Уменьшение поверхности атаки Сохранение простоты использования
Операции и сопровождение Объединение людей, процессов и технологий для построения, поддержки и использования защищенных систем	План по поддержке систем Внедрение защищенных конфигураций Мониторинг и журналирование Практика реагирования на инциденты Проверка процедур восстановления в случае аварии

Для обеспечения информационной безопасности Corporate Security Group использует подход по управлению информационными рисками (рис. 2.4). Под управлением рисками здесь понимается процесс определения, оценки и уменьшения рисков на постоянной основе. Управление рисками безопасности позволяет найти разумный баланс между стоимостью средств и мер защиты и требованиями бизнеса. Модель управления рисками Corporate Security Group представляет собой комбинацию различных подходов, таких, как количественный анализ рисков, анализ возврата инвестиций в безопасность, качественный анализ рисков, а также подходы лучших практик.



...

Рис. 2.4. Модель управления рисками Corporate Security Group

Инвестирование в процесс управления рисками – с цельной структурой и определенными ролями и обязанностями – готовит организацию к определению приоритетов, планированию уменьшения угрозы и переходу к парированию или нейтрализации следующей угрозы или уязвимости. Для наилучшего управления рисками Corporate Security Group следует традиционному подходу по управлению рисками, состоящему из четырех этапов:

- *оценка информационных рисков* – выполнение методологии оценки риска для определения его величины;
- *разработка политики безопасности* – разработка политики безопасности по уменьшению, уклонению и предупреждению рисков;
- *внедрение средств защиты* – объединение сотрудников, процессов и технологий для уменьшения рисков, связанных с анализом соотношения «цена – качество»;
- *аудит безопасности и измерение текущей защищенности* – мониторинг, аудит безопасности и измерение защищенности информационных систем компании.

Как видно из рис. 2.5, разработка политики является одним из этапов по управлению информационными рисками. Методология, используемая при разработке политики, базируется на стандарте ISO 17799:2005 (BS 7799).

Рекомендуемая компанией Microsoft политика безопасности включает в себя:

- определение целей безопасности;
- важность обеспечения безопасности;

...

Рис. 2.5. Этапы управления информационными рисками

• определение требуемого уровня безопасности;
• стандарты безопасности, включая стратегии их мониторинга и аудита;
• роли и ответственность по обеспечению безопасности;
• цели и задачи офицера по безопасности;
• определение процессов по защите индивидуальных компонентов архитектуры;
• определение программ обучения вопросам безопасности.

Примерами декларируемых целей безопасности являются: • достижение максимально возможного уровня качества, надежности и конфиденциальности информации;
• сохранение репутации компании;
• недопущение повреждения или утери информации, процессов, собственности компании и обеспечение таким образом непрерывной работы компании;
• сохранение ценности информации, интеллектуальной собственности и технологических ресурсов.

Для разработки целей безопасности создается комитет по информационной безопасности. Комитет состоит из сотрудников с опытом работы в области безопасности, технических сотрудников и представителей других подразделений под руководством офицера по безопасности. Комитет решает следующие задачи: • разработка и управление жизненным циклом политики безопасности;
• создание процессов, обеспечивающих достижение целей безопасности;
• создание процессов и планов по реализации стандартов, описанных в политике;
• помощь в организации программ ознакомления с вопросами безопасности;
• консультирование персонала по вопросам безопасности;
• определение бюджета и требуемых ресурсов по обеспечению безопасности.

2.5. Подход компании Symantec

Руководящие документы в области безопасности (политики, стандарты, процедуры и метрики безопасности), как полагают в Symatec, являются основой любой успешной программы обеспечения информационной безопасности компании (см. рис. 2.6).

...

Рис. 2.6. Жизненный цикл обеспечения информационной безопасности организации

Наглядно проявления различий политик, стандартов и процедур безопасности представлены на рис. 2.7.

...

Рис. 2.7. Различия политики, стандартов и процедур безопасности

Политика информационной безопасности определяет, *почему* компания защищает свою информацию. Стандарты – *что* компания намерена предпринимать для реализации и управления безопасностью информации. Процедуры описывают, *как* компания будет выполнять требования, описанные в высокоуровневых документах (политике и руководствах). Руководства представляют собой *рекомендации,* которым сотрудникам желательно следовать.

2.5.1. Описание политики безопасности

Основные этапы разработки политики безопасности. Компания Symantec выделяет следующие основные этапы разработки политики безопасности:

- *определение и оценка информационных активов* – какие активы необходимо защищать и как их защищать с учетом целей и задач бизнеса;

• *определение угроз безопасности* – выявление потенциальных источников проблем в области безопасности компании. Оценка вероятности реализации угрозы и оценка возможного ущерба. При этом выделяют внешние и внутренние угрозы безопасности;

• *оценка информационных рисков* – представляет собой один из самых сложных этапов процесса разработки политики безопасности. На этом этапе необходимо определить вероятность реализации угроз и выделить те из них, что нанесут наибольший ущерб. Ущерб выражается не только количественно, например в денежном эквиваленте, но и качественно, для отражения ущерба, вызванного потерей имиджа компании, потерей конфиденциальности взаимоотношений с определенными стратегически важными клиентами и партнерами;

• *определение ответственности* – выбор команды разработчиков, способной определить потенциальные угрозы во всех областях деятельности компании. В идеале в процессе разработки политики безопасности должны принимать участие представители всех ключевых подразделений компании. Ключевые члены команды – представители руководства, отдела кадров, юридического отдела, отдела по связям с общественностью, сетевые администраторы, эксперты в области информационной безопасности;

• *создание комплексного документа* – создание политики со ссылками на такие дополнительные документы, как процедуры, руководства, стандарты и контракты сотрудников. Эти документы должны содержать требования к конкретным информационным системам, технологиям, а также определять степень ответственности сотрудников. В результате становится возможным производить изменения в документах, не затрагивая саму политику информационной безопасности. Политика информационной безопасности подписывается руководителем компании;

• *реализация* – политика безопасности должна четко определять ответственность за обеспечение информационной безопасности и ответственных за информационные системы и защиту информации. Компания может потребовать от сотрудников подписи в том, что они ознакомлены с политикой безопасности и обязуются соблюдать ее требования. Ответственность реализуется с помощью определения:

– процедуры соответствия – для определения ответственности за выполнение требований политики безопасности;

– состава и структуры подразделения офицеров безопасности – определяет сотрудников, которые несут ответственность за обеспечение режима информационной безопасности. Здесь необходимо предусмотреть проблемы, связанные с конфликтом интересов;

– процедуры выделения необходимых ресурсов – гарантирует выделение необходимых ресурсов для соответствия требованиям политики информационной безопасности;

• *управление программой безопасности* – определяет внутренние процедуры для реализации требований политики.

Рекомендуемый состав политики безопасности. Ключевыми аспектами политики информационной безопасности являются: • область применения,

• необходимость строгого соблюдения политики,

• основная часть политики,

• ответственность,

• последствия за несоответствие требованиям политики. Существенными утверждениями политики безопасности являются следующие:

• компания является собственником всех данных и систем;

• сотрудник обязуется не делать копий данных и программного обеспечения без получения соответствующего разрешения;

• сотрудник обязуется выполнять требования по парольной защите;

• сотрудник обязуется получать доступ к системам и информации только легальным способом, после авторизации;

• сотрудник подтверждает право компании осуществлять мониторинг его деятельности.

Рекомендуемый объем политики информационной безопасности не должен превышать

двух страниц.

Реализация политики достигается использованием стандартов, процедур, руководств.

Что принимается во внимание? Для эффективности политики безопасности необходимо, чтобы политика: • была простой для понимания,

• основывалась на требованиях бизнеса,

• была реализуемой,

• поддерживала баланс между безопасностью и производительностью,

• была доступна всем сотрудникам для ознакомления,

• не противоречила другим политикам компании,

• не противоречила требованиям законодательства,

• ясно определяла ответственность сотрудников за ее нарушение,

• была регулярно обновляемой.

Стандарты. Требования к стандартам: • каждый стандарт должен поддерживать выполнение бизнес-целей компании, соответствовать требованиям существующего законодательства и действующим в компании политикам;

• стандарт должен быть разработан для защиты информации, в то же время он не должен затруднять получение доступа к информации сотрудникам компании;

• стандарт должен разрабатываться совместными усилиями бизнес-менеджеров и технических экспертов;

• стандарт не должен противоречить требованиям политики информационной безопасности.

За основу при разработке стандартов компания Symantec рекомендует использовать стандарт ISO 17799:2005.

Процедуры. Следующим уровнем документов являются процедуры. Роль процедуры – определить, как реализуются и администрируются средства безопасности. Процедуры являются своего рода «библией» для сотрудников компании, их ежедневным руководством к действию. Процедуры, в отличие от политики и стандартов, являются часто изменяющимися документами, поэтому важно иметь в компании хорошую процедуру управления изменениями документов. Каждая процедура должна быть написана в соответствии с общим шаблоном, разработанным для процедур, быть доступной сотрудникам как в электронном, так и в бумажном виде. Так как некоторые процедуры могут содержать конфиденциальную информацию, то доступ к ним может быть ограничен, что регулируется отдельным стандартом. Рекомендуемыми элементами процедур безопасности являются:

цель процедуры:

– для соответствия какому стандарту она разработана;

– для чего нужна процедура;

область действия процедуры:

– к каким системам, сетям, приложениям, категориям персонала, помещениям применима процедура;

– какая роль необходима для выполнения процесса;

– что нужно знать для выполнения процесса;

определение процесса:

– введение в процесс(описание);

– детальное описание процесса (как, когда, что, критерии успеха, виды отчетов, взаимодействие с другими процессами);

контрольный список процесса;

• *проблемы процесса* (действия при возникновении проблем).

2.6. Подход SANS

2.6.1. Описание политики безопасности

Организация SANS выработала свой подход в понимании политики информационной

безопасности и ее составляющих. В терминологии SANS политика информационной безопасности – многоуровневый документированный план обеспечения информационной безопасности компании:

• верхний уровень – политики;
• средний уровень – стандарты и руководства;
• низший уровень – процедуры.

Далее документы разбиваются на следующие основные категории: • утверждение руководства о поддержке политики информационной безопасности;

• основные политики компании;
• функциональные политики;
• обязательные стандарты (базовые);
• рекомендуемые руководства;
• детализированные процедуры.

Стандарты детализируют различия по настройке безопасности в отдельных операционных системах, приложениях и базах данных. Руководства представляют из себя рекомендуемые, необязательные к выполнению действия по предупреждению проблем, связанных с различными аспектами информационной безопасности.

Процедуры – детальные пошаговые инструкции, которые сотрудники обязаны неукоснительно выполнять.

При разработке политик очень важным является корректное распределение ролей и обязанностей. Очень важно соблюдать принцип наименьших привилегий, принцип «знать только то, что необходимо для выполнения служебных обязанностей» и использовать разделение обязанностей на критичных системах.

Различают следующие типы политик безопасности:

• *направленные на решение конкретной проблемы* – примерами таких политик могут служить политика по найму персонала, политика использования паролей, политика использования Интернета;

• *программные* – высокоуровневые политики, определяющие общий подход компании к обеспечению режима информационной безопасности. Эти политики определяют направление разработки других политик и соответствие с требованиями законодательства и отраслевых стандартов;

• *применяемые к конкретной среде* – например, каждая операционная система требует отдельного стандарта по ее настройке.

Рекомендуемые компоненты политики безопасности:

• цель,
• область действия,
• утверждение политики,
• история документа,
• необходимость политики,
• какие политики отменяет,
• действия по выполнению политики,
• ответственность,
• исключения,
• порядок и периодичность пересмотра.

Организация SANS разработала ряд шаблонов политик безопасности: • политика допустимого шифрования,

• политика допустимого использования,
• руководство по антивирусной защите,
• политика аудита уязвимостей,
• политика хранения электронной почты,
• политика использования электронной почты компании,
• политика использования паролей,

• политика оценки рисков,
• политика безопасности маршрутизатора,
• политика обеспечения безопасности серверов,
• политика виртуальных частных сетей,
• политика беспроводного доступа в сеть компании,
• политика автоматического перенаправления электронной почты компании,
• политика классификации информации,
• политика в отношении паролей для доступа к базам данных,
• политика безопасности лаборатории демилитаризованной зоны,
• политика безопасности внутренней лаборатории,
• политика экстранет,
• политика этики,
• политика лаборатории антивирусной защиты.

2.6.2. Пример политики аудита безопасности [11]

Цель. Установить правила аудита безопасности информационных систем компании, выполняемого внутренними аудиторами. Аудиторы должны использовать утвержденный перечень средств поиска уязвимостей или сканеров безопасности при выполнении сканирования клиентских сетей и/или межсетевых экранов или любых других компонент информационных систем компании.

Аудит может быть проведен для:

• гарантии целостности, конфиденциальности и доступности информационных ресурсов компании;

• расследования возможных инцидентов в области безопасности компании;

• мониторинга деятельности сотрудников и активности информационной системы в целом.

Область действия. Политика охватывает все компоненты информационных систем компании. Аудиторы не будут проводить атаки класса «отказ в обслуживании». *Политика.* Аудиторам предоставляется доступ к информационной системе при выполнении аудита безопасности. Компания, таким образом, позволяет аудиторам проводить поиск уязвимостей в корпоративной сети и на оборудовании компании в соответствии с планом проведения аудита. Компания обеспечивает аудиторов всеми необходимыми документами для проведения аудита безопасности (технические проекты, карта сети, положения и инструкции и пр.).

Доступ к информационной системе включает:

• доступ на уровне пользователя или системный доступ к любому оборудованию системы;

• доступ к данным (в электронном виде, в виде бумажных копий и т. д.), которые создаются, передаются и хранятся в системе;

• доступ в помещения (лаборатории, офисы, серверные и т. д.);

• доступ к сетевому трафику.

Управление сетью. Если в компании доступ из корпоративной сети в Интернет обеспечивается сторонней организацией, то для проведения аудита безопасности требуется ее письменное разрешение. Подписывая такое соглашение, все заинтересованные стороны подтверждают, что они разрешают проведение аудиторами сканирования сети компании в определенный соглашением период времени. *Уменьшение производительности и/или недоступность сервиса.* Компания освобождает аудиторов от любой ответственности, связанной с уменьшением сетевой производительности или недоступностью сервисов, вызванных проведением сканирования, если только такие проблемы не возникли из-за некомпетентности аудиторов.

Контактные лица компании при проведении аудита. Компания должна определить и провести приказом список ответственных лиц, консультирующих аудиторов по всем вопросам, возникающим во время проведения аудита безопасности.

Период сканирования. Компания и аудиторы должны в письменном виде зафиксировать даты и время проведения аудита безопасности.

Процесс оценки рисков. Процесс оценки рисков описан в положении об оценивании и управлении информационными рисками компании.

Ответственность. К любому сотруднику компании, нарушившему эту политику, могут быть применены дисциплинарные меры, вплоть до увольнения.

Глава 3 РЕКОМЕНДАЦИИ МЕЖДУНАРОДНЫХ СТАНДАРТОВ ПО СОЗДАНИЮ ПОЛИТИК БЕЗОПАСНОСТИ

В последнее время в разных странах появилось новое поколение стандартов в области информационной безопасности, посвященных практическим вопросам обеспечения информационной безопасности в компаниях и организациях. Это, прежде всего, международные стандарты ISO/IEC 17799:2005 (BS 7799-1:2002), ISO/IEC 15408, ISO/IEC TR 13335, германский стандарт BSI IT Protection Manual, стандарты NIST США серии 800, стандарты и библиотеки CobiT, ITIL, SAC, COSO, SAS 78/94 и некоторые другие, аналогичные им. В соответствии с названными стандартами политики безопасности компании должны явно определять следующее:

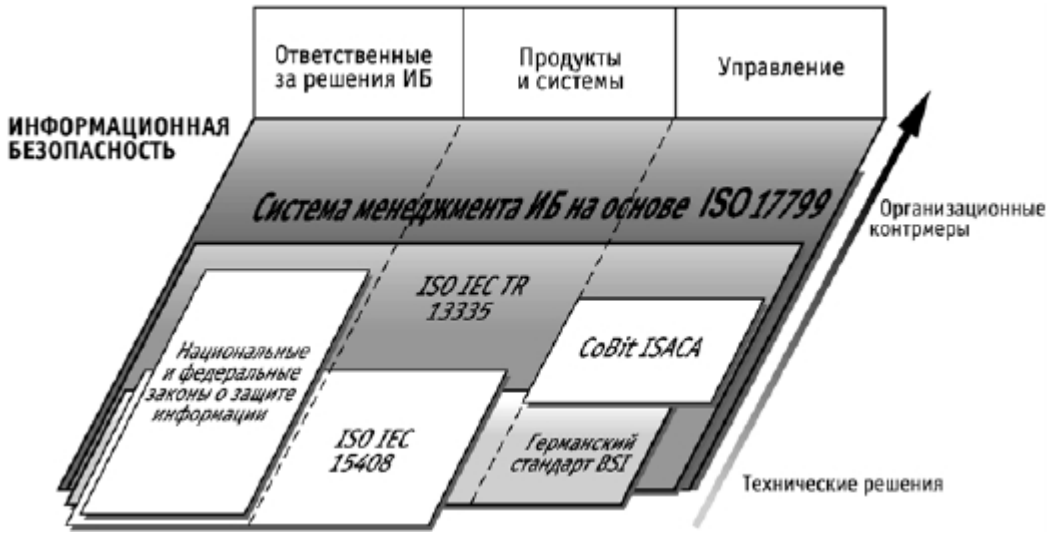
- предмет политики безопасности, основные цели и задачи политики безопасности;
- условия применения политики безопасности и возможные ограничения;
- описание позиции руководства компании по отношению к выполнению политики безопасности и организации режима информационной безопасности компании в целом;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

В этой главе нам предстоит рассмотреть, насколько рекомендации перечисленных стандартов безопасности могут быть полезны для разработки политик безопасности в отечественных компаниях.

3.1. Стандарты ISO/IEC 17799:2005 (BS 7799-1:2002)

В настоящее время международный стандарт ISO/IEC 17799:2005 (BS 7799-1:2002) «Управление информационной безопасностью – Информационные технологии» («Information Technology – Information Security Management») является наиболее известным стандартом в области защиты информации (см. рис. 3.1). Алгоритм применения стандарта ISO 17799 представлен на рис. 3.2. Данный стандарт был разработан на основе первой части британского стандарта BS 7799-1:1995 «Практические рекомендации по управлению информационной безопасностью» («Information Security Management – Part 1: Code of Practice for Information Security Management») и относится к новому поколению стандартов информационной безопасности компьютерных информационных систем. Текущая версия стандарта ISO/IEC 17799:2005 (BS 7799-1:2002) рассматривает следующие актуальные вопросы обеспечения информационной безопасности организаций и предприятий (см. рис. 3.3):

- необходимость обеспечения информационной безопасности;
- основные понятия и определения информационной безопасности;
- политика информационной безопасности компании;
- организация информационной безопасности на предприятии;
- классификация и управление корпоративными информационными ресурсами;
- вопросы безопасности, связанные с персоналом;



...

Рис. 3.1. Характеристика современных стандартов безопасности

...

Рис. 3.2. Алгоритм применения стандарта ISO 17799

...

Рис. 3.3. Основные области применения стандарта ISO 17799

• физическая безопасность;
• администрирование безопасности корпоративных информационных систем;
• управление доступом;
• требования по безопасности к корпоративным информационным системам в ходе их разработки, эксплуатации и сопровождения;
• управление бизнес-процессами компании с точки зрения информационной безопасности;
• внутренний аудит информационной безопасности компании;
• обеспечение непрерывности бизнеса;
• соответствие требованиям.

Вторая часть стандарта BS 7799-2:2002 «Спецификации систем управления информационной безопасностью» («Information Security Management – Part 2: Specification for Information Security Management Systems») определяет возможные функциональные спецификации корпоративных систем управления информационной безопасностью с точки зрения их проверки на соответствие требованиям первой части данного стандарта (см. рис. 3.4).

...

Рис. 3.4. Состав рабочей документации для сертификации по требованиям стандарта BS 7799-2

В соответствии с положениями этого стандарта также регламентируется процедура аудита безопасности информационных корпоративных систем (рис. 3.5).

...

Рис. 3.5. Рекомендуемые этапы проверки режима информационной безопасности компании

Стандарт ISO 17799 (BS 7799) позволяет задать правила безопасности и определить политики безопасности компании. Так, например, в табл. 3.1 представлены контрольные вопросы согласно стандарта BS 7799-2, позволяющие оценить систему управления информационной безопасностью компании и задать правила безопасности.

Дополнительные рекомендации по разработке корпоративных политик безопасности содержат руководства Британского института стандартов (British Standards Institution, BSI) (www.bsi-global.com). изданные в период 1995–2005 годов в виде следующей серии:

• «Введение в проблему управления информационной безопасностью» («Information Security Management: An Introduction»);

• «Возможности сертификации на соответствие требованиям стандарта BS 7799» («Preparing for BS 7799 Certification»);

• Подготовка к сертификации по требованиям стандарта BS 7799-2 («Preparing for BS 7799-2 Certification (PD3001:2002)»);

• «Руководство по оценке и управлению рисками в соответствии с требованиями BS 7799» («Guide to BS 7799 Risk Assessment and Risk Management»);

• «Готовы ли вы к аудиту на соответствие требованиям стандарта BS 7799» («Are You Ready for a BS 7799 Audit»);

• «Руководство для проведения аудита на соответствие требованиям стандарта BS 7799» («Guide to BS 7799 Auditing»);

• «Руководство по внедрению средств обеспечения информационной безопасности и их аудиту на соответствие BS 7799», («Guide to the Implementation and Auditing of BS 7799 Controls (PD3004:2002)»);

• «Руководство по выбору средств обеспечения информационной безопасности в соответствии с BS 7799-2» («Guide on the Selection of BS 7799 Part 2 Controls (PD3005:2002)»);

• «Практические рекомендации по управлению безопасностью информационных технологий» («Code of Practice for IT Security Management»).

Таблица 3.1. Примеры контрольных вопросов согласно стандарта BS 7799-2 для

задания правил безопасности

Сообщение		Область аудита, цель и вопросы		Результаты
Требования	*Пункт стандарта*	*Область управления ИБ*	*Вопрос аудита безопасности*	*Выполнение Шкала от 1 до 5*
Политика информационной безопасности (ПИБ)				
1.1	3.1	Политика информационной безопасности		
1.1.1	3.1.1	ПИБ	Существует ли политика информационной безопасности, которая подписана руководством, издана ли она и имеют ли все сотрудники доступ к ней	4

Продолжение табл. 3.1

Сообщение		Область аудита, цель и вопросы		Результаты
Требования	*Пункт стандарта*	*Область управления ИБ*	*Вопрос аудита безопасности*	*Выполнение Шкала от 1 до 5*
1.1.2	3.1.2	Пересмотр и оценка	Имеет ли ПИБ владельца, который несет ответственность за поддержание ПИБ в актуальном состоянии Гарантирует ли процесс, что пересмотр будет осуществлен в ответ на любые изменения, воздействующие на первоначальную оценку, пример: серьезные инциденты безопасности, новые уязвимости, изменения организационной или технической инфраструктуры	4
Организационная безопасность				
2.1	4.1	Инфраструктура информационной безопасности		
2.1.1	4.1.1	Отдел безопасности	Может ли отдел безопасности и экспертная комиссия гарантировать, что существуют четкое управление и видимая поддержка руководства ИБ в компании	4
2.1.2	4.1.2	Координация усилий по информационной безопасности	Существует ли комитет из представителей руководства по различным направлениям по координации выполнения требований информационной безопасности	5
2.1.3	4.1.3	Определение ответственности за информационную безопасность	Выделены ли ответственные за безопасность каждого актива и выполняются ли по отношению к ним специальные процедуры безопасности	3
2.1.4	4.1.4	Процесс авторизации средств обработки информации	Существует ли процесс авторизации для любых новых средств обработки информации. Он должен включать все новые средства (ПО и АО)	4

Продолжение табл. 3.1

Сообщение		Область аудита, цель и вопросы		Результаты
Требования	*Пункт стандарта*	*Область управления ИБ*	*Вопрос аудита безопасности*	*Выполнение Шкала от 1 до 5*
2.1.5	4.1.5	Консультации по вопросам информационной безопасности	Доступен ли консультант по информационной безопасности, когда требуется квалифицированный совет Может ли быть выделен внешний консультант для обеспечения помощи по вопросам информационной безопасности	4
2.1.6	4.1.6	Сотрудничество между организациями	Были ли соответствующие контакты с представителями властей, регулирующими органами, поставщиками информационных сервисов и телекоммуникационными операторами для гарантии того, что в случае возникновения инцидента безопасности соответствующие действия могут быть быстро выполнены и получена консультация	3
2.1.7	4.1.7	Независимый аудит информационной безопасности	Проводится ли независимый аудит ПИБ. Для гарантии того, что практика компании должным образом отражает политику, что она реальна и эффективна	2
2.2	4.2	Защита доступа сторонних организаций		
2.2.1	4.2.1	Идентификация рисков доступа сторонних организаций	Идентифицированы ли риски, связанные с доступом сторонних организаций, и реализованы ли соответствующие меры безопасности Могут ли типы доступа быть идентифицированы и классифицированы, доказана ли необходимость получения доступа Могут ли риски работников сторонних организаций, работающих по контракту на территории компании, быть идентифицированы и реализованы ли соответствующие меры безопасности	2

Продолжение табл. 3.1

Сообщение		Область аудита, цель и вопросы		Результаты
Требования	*Пункт стандарта*	*Область управления ИБ*	*Вопрос аудита безопасности*	*Выполнение Шкала от 1 до 5*
2.2.2	4.2.2.	Требования безопасности в контрактах со сторонними организациями	Содержат ли формальные контракты (или ссылаются) все требования безопасности для обеспечения соответствия с ПИБ и стандартами компании	2
2.3	4.3	Аутсорсинг		
2.3.1	4.3.1	Требования безопасности в контрактах по аутсорсингу	Внесены ли требования по безопасности в контракты со сторонними организациями, когда у компании есть ресурсы, управление и контроль над которыми осуществляют сторонние организации	3
Классификация и управление активами				
3.1	5.1	Возможность идентификации активов		
3.1.1	5.1.1	Инвентаризация активов	Поддерживается ли база инвентаризации или реестр важных активов, ассоциированных с любой информационной системой	3
3.2	5.2	Классификация информации		
3.2.1	5.2.1	Руководство по классификации	Существует ли схема или руководство по классификации информации, которые помогают определить, какая информация должна быть маркирована и подлежит защите	4
3.2.2	5.2.2	Маркировка и обработка информации	Определен ли набор процедур по маркировке и обработке информации в соответствии со схемой классификации, принятой в компании	5

Продолжение табл. 3.1

Сообщение		Область аудита, цель и вопросы		Результаты
Требования	*Пункт стандарта*	*Область управления ИБ*	*Вопрос аудита безопасности*	*Выполнение Шкала от 1 до 5*
Защита персонала				
4.1	6.1	Обязанности по защите информации в должностных инструкциях		
4.1.1	6.1.1	Включение обязанностей по защите информации в должностные инструкции	Определены ли в ПИБ роли по обеспечению безопасности и ответственность. ПИБ должна включать общие обязанности по обеспечению и поддержанию ПИБ, так же как специфические обязанности по защите конкретных активов	4
4.1.2	6.1.2	Проверка персонала и кадровая политика	Осуществляется ли проверка сотрудников в процессе найма на работу Она должна включать подтверждение профессиональной квалификации, реальности представленного резюме и независимую проверку личности	3
4.1.3	6.1.3	Соглашение о конфиденциальности	Требуют ли от сотрудников подписать соглашение о неразглашении или о конфиденциальности как обязательное условие принятия их на работу Охватывает ли это соглашение защиту информации, средств ее обработки и активов компании	4
4.1.4	6.1.4	Термины и условия найма	Предусматривают ли термины и условия найма ответственность сотрудников по информационной безопасности. Эти обязанности могут быть продлены на определенный период после увольнения	4
4.2	6.2	Обучение пользователей		
4.2.1	6.2.1	Обучение и тренинг по вопросам информационной безопасности	Обучаются ли все сотрудники компании и сторонние работники вопросам информационной безопасности и получают ли они регулярные обновления политик и процедур компании	2

Продолжение табл. 3.1

Сообщение		Область аудита, цель и вопросы		Результаты
Требования	*Пункт стандарта*	*Область управления ИБ*	*Вопрос аудита безопасности*	*Выполнение Шкала от 1 до 5*
4.3	6.3	Реагирование на инциденты безопасности		
4.3.1	6.3.1	Отчет по инцидентам безопасности	Существует ли формальная процедура уведомления руководства об инцидентах безопасности с помощью соответствующих каналов	2
4.3.2	6.3.2	Отчет о слабых местах в безопасности	Существует ли формализованная процедура или руководство для пользователей по действиям в случае обнаружения слабых мест в защите систем или сервисов	2
4.3.3	6.3.3	Реагирование на сбои ПО	Введена ли процедура отчетности о любых сбоях ПО	2
4.3.4	6.3.4	Анализ инцидента	Существует ли механизм измерения и анализа типов, масштабов и стоимости инцидентов и сбоев	2
4.3.5	6.3.5	Процесс дисциплинарных наказаний	Существует ли формализованная процедура наказания служащих, которые нарушили ПИБ и процедуры безопасности. Такой процесс может выполнять функцию устрашения сотрудников, склонных к нарушению ПИБ	2
Физическая защита и защита среды				
5.1	7.1	Защита помещений		
5.1.1	7.1.1	Физическая защита периметра	Какие физические устройства безопасности периметра осуществляют защиту средств обработки информации Примеры таких устройств безопасности — шлюзы, стены, охрана	4
5.1.2	7.1.2	Физические средства контроля доступа	Какие физические средства контроля доступа позволяют только авторизованному персоналу находиться внутри компании	4

Продолжение табл. 3.1

Сообщение		Область аудита, цель и вопросы		Результаты
Требования	*Пункт стандарта*	*Область управления ИБ*	*Вопрос аудита безопасности*	*Выполнение Шкала от 1 до 5*
5.1.3	7.1.3	Защита офисов, комнат и зданий	Заперты ли комнаты, в которых размещаются средства обработки информации, имеют ли они закрываемые на ключ шкафы или сейфы Имеют ли средства обработки информации защиту от естественных и искусственных бедствий Существуют ли угрозы, исходящие от смежных помещений	2
5.1.4	7.1.4	Работа в защищенных помещениях	Существуют ли средства защиты от действий сотрудников сторонних организаций, работающих на защищенной территории	3
5.1.5	7.1.5	Изоляция помещений для доставки от помещений для загрузки	Изолированы ли области доставки и области обработки и загрузки информации друг от друга во избежание несанкционированных действий Введена ли оценка рисков для определения безопасности таких помещений.	3
5.2	7.2	Безопасность оборудования		
5.2.1	7.2.1	Защита помещения с оборудованием	Находится ли оборудование в помещении с ограниченным доступом Изолировано ли оборудование, требующее специальной защиты, в отдельную зону, для снижения общего уровня требований по безопасности Применены ли средства защиты для минимизации рисков от таких потенциальных угроз, как кража, пожар, взрыв, дым, вода, вибрации, химические элементы, электромагнитное излучение, наводнение Существует ли политика, запрещающая принятие пищи, питье и курение рядом со средствами обработки информации	3

Продолжение табл. 3.1

Сообщение		Область аудита, цель и вопросы		Результаты
Требования	*Пункт стандарта*	*Область управления ИБ*	*Вопрос аудита безопасности*	*Выполнение Шкала от 1 до 5*
			Анализируются ли условия окружающей среды, которые неблагоприятно воздействуют на средства обработки информации	
5.2.2	7.2.2	Источники питания	Защищено ли оборудование от аварий с помощью источников бесперебойного питания, запасных генераторов	2
5.2.3	7.2.3	Защита кабелей	Защищены ли кабели телекоммуникаций и питания, переносящие данные и вспомогательную информацию от перехвата или повреждений Существуют ли дополнительные средства защиты для чувствительной или критичной информации	3
5.2.4	7.2.4	Техническая поддержка оборудования	Проводится ли профилактическое обслуживание оборудования через рекомендованные производителем интервалы времени и согласно спецификациям Осуществляется ли текущее обслуживание только авторизованным персоналом Существует ли система регистрации всех предполагаемых и действительных сбоев и всех реализованных профилактических и корректирующих мер Используются ли адекватные меры защиты при отправке оборудования за пределы компании Если оборудование застраховано, выполняются ли требования страховщиков	2
5.2.5	7.2.5	Защита оборудования за пределами компании	Нужно ли получать разрешение руководства для использования оборудования за пределами компании Должен ли быть уровень защиты оборудования, используемого за пределами компании, выше по сравнению с уровнем защиты внутри помещения компании	3

Сообщение		Область аудита, цель и вопросы		Результаты
Требования	*Пункт стандарта*	*Область управления ИБ*	*Вопрос аудита безопасности*	*Выполнение Шкала от 1 до 5*
5.2.6	7.2.6	Требования при повторном использовании или уничтожении оборудования	Ликвидируются ли физически, надежно ли стираются устройства хранения, содержащие критичную информацию	3
5.3	7.3	Общие средства безопасности		
5.3.1	7.3.1	Требования «чистого стола» и «чистого экрана»	Активирована ли функция автоматической блокировки экрана. Она должна блокировать экран, если компьютер оставлен на время без присмотра Знают ли сотрудники о требовании закрывать конфиденциальную информацию в форме бумажных документов в сейф или шкаф, если им необходимо отойти от своего рабочего места	2
5.3.2	7.3.2	Перемещение собственности компании за ее пределы	Может ли кто-то вынести оборудование, информацию или ПО за пределы компании без получения разрешения Проводится ли регулярный аудит по обнаружению попыток несанкционированного выноса собственности компании Осведомлены ли сотрудники о проведении такого аудита	4
Управление деятельностью и соединениями				
6.1	8.1	Операционные процедуры и ответственность		
6.1.1	8.1.1	Документирование операционных процедур	Определены ли в ПИБ такие операционные процедуры, как резервирование, обслуживание оборудования и т.д. Оформлены ли такие процедуры в виде документов и используются ли они	3

Продолжение табл. 3.1

Продолжение табл. 3.1

Сообщение		Область аудита, цель и вопросы		Результаты
Требования	*Пункт стандарта*	*Область управления ИБ*	*Вопрос аудита безопасности*	*Выполнение Шкала от 1 до 5*
6.1.2	8.1.2	Управление изменениями	Проходят ли все программы, запущенные в системе, строгий контроль изменений, то есть все изменения в этих программах должны пройти через авторизацию управления изменениями Ведутся ли журналы изменений в программах	2
6.1.3	8.1.3	Процедуры управления инцидентами	Существует ли процедура управления инцидентами для обработки инцидентов безопасности Содержат ли процедуры описание обязанностей по управлению инцидентами, порядка и скорости реакции на инциденты безопасности Определены ли в процедуре разные типы инцидентов, начиная от отказа в обслуживании до нарушения конфиденциальности, и способы реагирования на них Обрабатываются ли журналы аудита и регистрации, относящиеся к инциденту, и осуществляется ли профилактика повторения инцидента	2
6.1.4	8.1.4	Разделение обязанностей	Существует ли разделение обязанностей для того, чтобы сократить возможность несанкционированных модификаций и злоупотреблений по отношению к информации и сервисам	2
6.1.5	8.1.5	Разделение областей разработки и производства	Изолированы ли области тестирования и производства друг от друга. Например, ПО тестирования не должно находиться на том же компьютере, что и ПО производства Необходимо, чтобы сети тестирования и производства были разделены	1
6.1.6	8.1.6	Управление внешними помещениями	Могут ли помещения обработки информации находиться под управлением внешних компаний или третьих лиц	3

Продолжение табл. 3.1

Сообщение		Область аудита, цель и вопросы		Результаты
Требования	*Пункт стандарта*	*Область управления ИБ*	*Вопрос аудита безопасности*	*Выполнение Шкала от 1 до 5*
6.2	8.2	Планирование мощности систем и принятие систем		
6.2.1	8.2.1	Планирование мощности	Анализируются ли требования по требуемым ресурсам и создаются ли проекты по увеличению мощности. Это гарантирует адекватную мощность по обработке и хранению информации. Например, мониторинг места на жестком диске, оперативной памяти, процессора в критичных сервисах	3
6.2.2	8.2.2	Система приема	Введены ли критерии для внедрения новых информационных систем, обновлений и новых версий Проводятся ли соответствующие тесты перед приемом	2
6.3	8.3	Защита от зловредного кода		
6.3.1	8.3.1	Защита от зловредного кода	Существуют ли средства защиты от зловредного кода Имеет ли ПИБ требования по использованию только лицензионного ПО и запрещению использования неавторизованного ПО Существуют ли процедуры для проверки того, насколько все оповещения аккуратны и информативны в отношении использования зловредного кода Установлены ли антивирусные программы на компьютерах для проверки, изоляции или удаления вирусов Осуществляется ли регулярное обновление вирусных баз Проверяется ли весь трафик компании. Например, проводится ли проверка на вирусы электронной почты, прикрепленных файлов электронной почты и сети, FTP-трафик	3

Сообщение		Область аудита, цель и вопросы		Результаты
Требования	*Пункт стандарта*	*Область управления ИБ*	*Вопрос аудита безопасности*	*Выполнение Шкала от 1 до 5*
6.4	8.4	Работа вне офиса		
6.4.1	8.4.1	Резервирование информации	Регулярно ли осуществляется резервирование важной информации. Пример: Пн — Чт: инкрементальное резервирование и Пт — полное резервирование Хранятся ли резервные копии вместе с процедурами по восстановлению безопасным образом за пределами здания Регулярно ли тестируются резервные копии, чтобы убедиться, что они могут быть восстановлены в течение выделенного интервала времени с использованием процедуры восстановления	3
6.4.2	8.4.2	Журналы операций	Сохраняет ли операционный персонал журнал своих действий, в котором зафиксированы имя пользователя, ошибки, действия по коррекции Проверяются ли такие журналы на регулярной основе в соответствии с операционными процедурами	3
6.4.3	8.4.3	Журналирование сбоев	Описаны и контролируемы ли сбои. Это включает корректирующие действия, аудит сбоев и проверку предпринятых действий	3
6.5	8.5	Сетевое управление		
6.5.1	8.5.1	Управление сетью	Осуществляется ли эффективное операционное управление, такое, как создание выделенных сетей и устройств системного администрирования, там, где это необходимо Определены ли обязанности и процедуры управления для оборудования, расположенного за пределами территории компании, включая оборудование пользователей систем Существуют ли специальные средства защиты, гарантирующие	3

Продолжение табл. 3.1

Продолжение табл. 3.1

Сообщение		Область аудита, цель и вопросы		Результаты
Требования	*Пункт стандарта*	*Область управления ИБ*	*Вопрос аудита безопасности*	*Выполнение Шкала от 1 до 5*
			конфиденциальность и целостность данных при их передаче через внешние сети, защиту подключаемых систем. Например: VPN, шифрование и механизмы хеширования	
6.6.	8.6	Маркировка и безопасность носителей информации		
6.6.1	8.6.1	Управление перемещаемыми носителями информации	Существует ли процедура управления перемещаемыми носителями информации, такими, как магнитные ленты, жесткие диски, кассеты, карты памяти и отчеты	2
6.6.2	8.6.2	Уничтожение носителей информации	Осуществляется ли уничтожение носителей информации, при возникновении необходимости, надежным способом Регистрируется ли уничтожение носителей информации, при возникновении необходимости, для обеспечения возможности проведения аудита	3
6.6.3	8.6.3	Процедура маркировки информации	Существует ли процедура маркировки информации Освещены ли в этой процедуре вопросы защиты информации от несанкционированного разглашения или неправильного использования	3
6.6.4	8.6.4	Защита системной документации	Защищена ли системная документация от несанкционированного доступа Содержит ли список доступа к системной документации минимальное число сотрудников и утвержден ли он владельцем приложения. Например, системная документация, находящаяся на совместно используемом сетевом ресурсе, должна иметь список контроля доступа, чтобы быть доступной только ограниченному числу сотрудников	2

Продолжение табл. 3.1

Сообщение		Область аудита, цель и вопросы		Результаты
Требования	*Пункт стандарта*	*Область управления ИБ*	*Вопрос аудита безопасности*	*Выполнение Шкала от 1 до 5*
6.7	8.7	Обмен информацией и ПО		
6.7.1	8.7.1	Соглашение об обмене информацией и ПО	Существует ли формальное или неформальное соглашение между организациями при обмене информацией и ПО Ссылается ли соглашение на требования безопасности, базирующиеся на критичности информации	3
6.7.2	8.7.2	Защита носителей информации во время транспортировки	Осуществляется ли защита носителей информации во время транспортировки Хорошо ли защищены носители информации от несанкционированного доступа, неправильного использования и искажения	3
6.7.3	8.7.3	Безопасность электронной коммерции	Защищена ли электронная коммерция от мошенничества, сомнительных контрактов, разглашения или модификации информации Включает ли электронная коммерция такие средства обеспечения безопасности, как аутентификация и авторизация Урегулирован ли вопрос с торговыми партнерами, включая соглашения, которые описывают торговые операции между ними, в том числе требования по безопасности	4
6.7.4	8.7.4	Безопасность электронной почты	Существует ли политика, разрешающая использование электронной почты, и уделено ли внимание в ПИБ использованию электронной почты Реализованы ли такие средства безопасности, как антивирусная проверка, изолирование потенциально опасных прикрепленных файлов, защита от спама, для уменьшения риска, связанного с использованием электронной почты	3

Продолжение табл. 3.1

Сообщение		Область аудита, цель и вопросы		Результаты
Требования	*Пункт стандарта*	*Область управления ИБ*	*Вопрос аудита безопасности*	*Выполнение Шкала от 1 до 5*
6.7.5	8.7.5	Безопасность систем электронного офиса	Определена ли политика допустимого использования систем электронного офиса Существует ли руководство по эффективной защите от рисков, связанных с использованием систем электронного офиса	3
6.7.6	8.7.6	Публично доступные системы	Существует ли формализованный процесс авторизации для информации, которую необходимо сделать доступной общественности. Например, одобрение, в соответствии с политикой управления изменениями, собственниками информации или приложения Существуют ли средства безопасности для обеспечения целостности информации, предназначенной для общего доступа, от несанкционированного доступа. Они могут включать такие средства безопасности, как межсетевые экраны, защита ОС, средства обнаружения вторжений и т.д.	3
6.7.7	8.7.7	Другие формы обмена информацией	Есть ли политики, процедуры или средства защиты безопасности информации при ее передаче посредством голоса, факса и видео Уведомлен ли персонал о необходимости защиты конфиденциальной информации при использовании таких методов обмена	3
Управление доступом				
7.1	9.1	Бизнес-требования по управлению доступом		
7.1.1	9.1.1	Политика управления доступом	Определены ли и задокументированы бизнес-требования по управлению доступом Имеет ли политика управления доступом разработанные правила и права для каждого пользователя или группы пользователей Имеют ли пользователи и поставщики сервисов ясное понимание бизнес-требований по управлению доступом	2

Продолжение табл. 3.1

Сообщение		Область аудита, цель и вопросы		Результаты
Требования	*Пункт стандарта*	*Область управления ИБ*	*Вопрос аудита безопасности*	*Выполнение Шкала от 1 до 5*
7.2	9.2	Управление доступом сотрудников		
7.2.1	9.2.1	Регистрация сотрудников	Существует ли формальная процедура регистрации и отмены регистрации сотрудников, учитывая многопользовательские информационные системы и сервисы	2
7.2.2	9.2.2	Управление привилегиями	Ограничено и контролируемо ли выделение и использование привилегий в многопользовательских информационных системах, то есть выдаются ли привилегии только на основе принципа «необходимости использования» или только после формализованного процесса авторизации	3
7.2.3	9.2.3	Управление паролями пользователей	Размещение и удаление паролей должно контролироваться формальным процессом управления Осведомлены ли пользователи о необходимости сохранения пароля в тайне	3
7.2.4	9.2.4	Аудит используемых прав доступа	Существует ли процесс аудита прав доступа пользователей через определенные промежутки времени. Например, специальные привилегии просматриваются раз в 3 месяца, обычные — каждые 6 месяцев	4
7.3.	9.3	Ответственность сотрудников		
7.3.1	9.3.1	Использование паролей	Существует ли руководство пользователя по выбору и хранению паролей	5
7.3.2	9.3.2	Оборудование, работающее в автономном режиме	Знают ли сотрудники и контрактники требования и процедуры по защите оборудования, работающего в автономном режиме, так же как и об их ответственности за обеспечение такой безопасности. Например, выход из системы после окончания сессии или настройка автоматического выхода из системы	3

Продолжение табл. 3.1

Сообщение		Область аудита, цель и вопросы		Результаты
Требования	*Пункт стандарта*	*Область управления ИБ*	*Вопрос аудита безопасности*	*Выполнение Шкала от 1 до 5*
7.4	9.4	Управление сетевым доступом		
7.4.1	9.4.1	Политика использования сетевых сервисов	Существует ли политика, которая освещает проблемы, связанные с сетью и сетевыми сервисами, такими, как: части сети, разрешенные для доступа; сервисы авторизации, определяющие, кто и что может делать; процедуры защиты доступа к сетевым подключениям и сетевым сервисам	2
7.4.2	9.4.2	Обязательный маршрут	Существует ли какое-либо средство защиты, ограничивающее маршрут между пользовательским терминалом и определенными сервисами на компьютере, к которым необходимо получить доступ, например обязательный маршрут для уменьшения риска	3
7.4.3	9.4.3	Аутентификация сотрудников для доступа за пределы сети компании	Существует ли какой-нибудь механизм аутентификации для доступа за пределы сети компании. Например: техника, основанная на криптографии, аппаратное средство идентификации, программное средство идентификации, протокол, основанный на механизме запрос/отклик	3
7.4.4	9.4.4	Аутентификация узлов	Аутентифицированы ли подключения к удаленным компьютерным системам, которые находятся вне пределов управления безопасностью компании. Аутентификация узлов может служить альтернативным способом аутентификации групп удаленных пользователей, когда они подключаются к защищенным совместно используемым компьютерным устройствам	3

Сообщение		Область аудита, цель и вопросы		Результаты
Требования	*Пункт стандарта*	*Область управления ИБ*	*Вопрос аудита безопасности*	*Выполнение Шкала от 1 до 5*
7.4.5	9.4.5	Безопасность портов удаленной диагностики	Контролируется ли доступ к портам удаленной диагностики, защищен ли он средствами безопасности	2
7.4.6	9.4.6	Разделение сетей	Разделена ли сеть, к которой нужен доступ партнерам и сторонним организациям, с использованием таких механизмов безопасности, как межсетевые экраны	2
7.4.7	9.4.7	Протоколы сетевых соединений	Существует ли какое-либо средство управления сетевыми соединениями для общих сетей, которые расположены за пределами компании. Например, электронная почта, Web-доступ, FTP-доступ	3
7.4.8	9.4.8	Управление сетевой маршрутизацией	Существуют ли средства защиты сети, которые гарантируют, что соединения и информационные потоки не нарушают политику контроля доступа бизнес-приложений. Это часто необходимо для сетей, используемых несколькими организациями одновременно Базируется ли управление маршрутизацией на механизмах идентификации источника и отправителя. Например, трансляция адресов (NAT).	3
7.4.9	9.4.9	Безопасность сетевых сервисов	Уверены ли компании, использующие общие или частные сетевые сервисы, что обеспечено четкое описание требований безопасности ко всем сервисам	3

Продолжение табл. 3.1

Продолжение табл. 3.1

Сообщение		Область аудита, цель и вопросы		Результаты
Требования	*Пункт стандарта*	*Область управления ИБ*	*Вопрос аудита безопасности*	*Выполнение Шкала от 1 до 5*
7.5	9.5	Управление доступом в ОС		
7.5.1	9.5.1	Автоматическая идентификация терминалов	Используется ли автоматический механизм идентификации терминалов для аутентификации соединений	4
7.5.2	9.5.2	Процедуры регистрации на терминале	Возможен ли доступ к информационной системе только через защищенный процесс регистрации Существует ли процедура регистрации в информационной системе. Необходимо для минимизации возможности несанкционированного доступа	4
7.5.3	9.5.3	Идентификация и авторизация пользователя	Предоставлены ли уникальные идентификаторы всем пользователям, таким, как операторы, системные администраторы, и всем остальным допущенным специалистам Общая учетная запись может быть использована только в случае исключительных обстоятельств, когда это является бизнес-преимуществом. Дополнительные средства защиты могут быть необходимы для обеспечения возможности журналирования Реализует ли используемый метод аутентификации требуемую идентификацию пользователя. Общий используемый метод: пароль, который знает только пользователь	3
7.5.4	9.5.4	Система управления паролями	Существует ли система управления паролями, которая приводит в действие разные средства управления паролями, такие, как: индивидуальный пароль, принудительная смена пароля, хранение пароля в зашифрованном виде, отключение показа пароля на экране	2

Продолжение табл. 3.1

Сообщение		Область аудита, цель и вопросы		Результаты
Требования	*Пункт стандарта*	*Область управления ИБ*	*Вопрос аудита безопасности*	*Выполнение Шкала от 1 до 5*
7.5.5	9.5.5	Использование системных утилит	Контролируется ли доступ к системным утилитам, которые поставляются с операционной системой и имеют возможность изменения системы и приложений	2
7.5.6	9.5.6	Принудительная аварийная сигнализация для пользователей	Рассмотрено ли обеспечение аварийного сигнала для пользователей	1
7.5.7	9.5.7	Тайм-аут для терминала	Сконфигурирован ли терминал для очистки экрана или автоматического закрытия после определенного периода бездействия	2
7.5.8	9.5.8	Ограничение времени соединения	Существует ли ограничение на время соединения для критичных приложений. Эта установка должна быть рассмотрена для использования в критичных приложениях	3
7.6	9.6	Управление доступом в приложениях		
7.6.1	9.6.1	Ограничение доступа к информации	Определен ли доступ к приложениям для разных групп и индивидуальных пользователей компании в политике управления доступом согласно требованиям конкретного бизнес-приложения и не нарушает ли он требований политики доступа к информации	2
7.6.2	9.6.2	Изолирование критичных систем	Обеспечены ли критичные системы выделенным компьютерным оборудованием, таким, как специальный сервер; совместное использование ресурсов возможно только с доверенными приложениями	2
7.7	9.7	Мониторинг доступа к системам и использования систем		
7.7.1	9.7.1	Журналирование событий	Происходит ли журналирование важных событий, в том числе и по безопасности, для обеспечения	2

Продолжение табл. 3.1

Сообщение		Область аудита, цель и вопросы		Результаты
Требования	*Пункт стандарта*	*Область управления ИБ*	*Вопрос аудита безопасности*	*Выполнение Шкала от 1 до 5*
			проведения расследований и для мониторинга контроля доступа	
7.7.2	9.7.2	Мониторинг использования систем	Установлены ли процедуры по мониторингу использования информационных систем Процедуры должны гарантировать, что пользователи исполняют только те действия, которые авторизованы Проверяются ли результаты мониторинга регулярно	2
7.7.3	9.7.3	Синхронизация времени	Согласовано ли время компьютера или устройства с единым внешним или внутренним источником времени. Правильная установка времени важна для обеспечения правильности аудита журналов	4
7.8	9.8	Работа вне офиса и мобильные пользователи		
7.8.1	9.8.1	Портативные компьютеры	Учитывает ли политика риски, связанные с работой на ноутбуках, персональных цифровых ассистентах, особенно в незащищенных областях Проводится ли обучение персонала по использованию портативных компьютерных устройств для повышения осведомленности о дополнительных рисках, связанных с такой работой, и средствах защиты, которые необходимо реализовать для уменьшения риска	2
7.8.2	9.8.2	Работа вне офиса	Существуют ли политика, процедура или стандарт, регламентирующие порядок работы вне офиса, и согласованы ли они с ПИБ компании Предусмотрены ли соответствующие средства защиты от таких угроз, как кража оборудования, несанкционированное разглашение информации	3

Продолжение табл. 3.1

Сообщение		Область аудита, цель и вопросы		Результаты
Требования	*Пункт стандарта*	*Область управления ИБ*	*Вопрос аудита безопасности*	*Выполнение Шкала от 1 до 5*
Разработка и поддержка систем				
8.1	10.1	Требования безопасности в отношении систем		
8.1.1	10.1.1	Анализ и спецификация требований по безопасности	Оформлены ли требования безопасности как часть бизнес-требований для новых систем или при расширении имеющихся систем Требования и средства безопасности должны отражать ценность для бизнеса информационных активов и последствия несоблюдения требований безопасности Была ли проведена оценка рисков перед принятием решения о разработке системы	2
8.2	10.2	Безопасность в приложениях		
8.2.1	10.2.1	Проверка вводимой информации	Осуществляется ли проверка вводимой информации на предмет корректности и достоверности Реализованы ли такие средства защиты, как различные виды проверки для анализа сообщений об ошибках, процедуры реагирования на ошибки, определенные обязанности всех персон, связанных с процессом введения данных	2
8.2.2	10.2.2	Средства защиты при обработке информации	Определены ли риски, относящиеся к циклу обработки информации и проверке ошибок. В некоторых случаях, данные, которые были корректно введены, могут быть искажены в результате ошибок при обработке или умышленных действий Определены ли соответствующие средства защиты для приложений по уменьшению рисков, связанных с внутренней обработкой информации. Средства защиты будут зависеть от природы приложения и бизнес-воздействия в случае повреждения информации.	2

Продолжение табл. 3.1

Сообщение		Область аудита, цель и вопросы		Результаты
Требования	*Пункт стандарта*	*Область управления ИБ*	*Вопрос аудита безопасности*	*Выполнение Шкала от 1 до 5*
8.2.3	10.2.3	Аутентификация сообщений	Была ли выполнена оценка рисков безопасности по определению необходимости аутентификации сообщений; по определению наиболее подходящего метода реализации. Аутентификация сообщений — техника, используемая для определения несанкционированных изменений или искажений содержания передаваемых электронных сообщений	3
8.2.4	10.2.4	Проверка выходных данных	Проверяются ли результаты работы приложения для обеспечения корректности и соответствия обстоятельствам процесса обработки информации	2
8.3	10.3	Криптографические средства		
8.3.1	10.3.1	Политика использования криптографических средств защиты	Существует ли политика использования криптографических средств защиты для обеспечения безопасности информации Выполнена ли оценка рисков для определения требуемого уровня безопасности информации	3
8.3.2	10.3.2	Шифрование	Используются ли технологии шифрования для обеспечения безопасности информации Проведен ли анализ критичности информации и определен ли требуемый уровень безопасности	2
8.3.3	10.3.3	Электронная цифровая подпись	Используется ли электронная цифровая подпись для защиты аутентичности и целостности электронного документа	3
8.3.4	10.3.4	Сервисы неотказуемости	Используются ли там, где это необходимо, сервисы неотказуемости для разрешения конфликтных ситуаций по определению, было ли действие или нет. Пример: конфликтная ситуация, включающая использование электронной подписи в электронных платежах и контрактах	2

Продолжение табл. 3.1

Сообщение		Область аудита, цель и вопросы		Результаты
Требования	*Пункт стандарта*	*Область управления ИБ*	*Вопрос аудита безопасности*	*Выполнение Шкала от 1 до 5*
8.3.5	10.3.5	Управление ключами	Существует ли в компании система управления по поддержке симметричного и асимметричного шифрования Базируется ли система управления ключами на согласованных стандартах, процедурах и методах безопасности	2
8.4.	10.4	Защита системных файлов		
8.4.1	10.4.1	Защита ОС	Существуют ли средства безопасности на уровне ОС. Это минимизирует риск нарушения работы информационных систем	3
8.4.2	10.4.2	Защита тестовой системной информации	Защищена и контролируема ли тестовая системная информация. Запрещается использовать БД, содержащую персональные данные, для целей тестирования. Если такую информацию надо использовать, данные должны перед этим быть обезличены	2
8.4.3	10.4.3	Управление доступом к библиотекам исходных кодов программ	Существует ли строгий контроль доступа к библиотекам исходных кодов программ. Это снижает риски по потенциальному искажению компьютерных программ	2
8.5	10.5	Защита процессов разработки и поддержки		
8.5.1	10.5.1	Процедуры управления изменениями	Существуют ли процедуры строгого контроля за изменениями в информационных системах. Это минимизирует риски по искажению информационной системы	2
8.5.2	10.5.2	Технический аудит изменений в ОС	Существует ли процесс или процедура, гарантирующие, что приложения проверены и протестированы после внесения изменений в ОС. Периодически необходимо обновлять ОС, инсталлировать служебные программы, обновления для приложений	2

Продолжение табл. 3.1

Сообщение		Область аудита, цель и вопросы		Результаты
Требования	*Пункт стандарта*	*Область управления ИБ*	*Вопрос аудита безопасности*	*Выполнение Шкала от 1 до 5*
8.5.3	10.5.3	Ограничения на изменения в программных пакетах	Существует ли ограничение по изменению пакетов ПО. Насколько это возможно, пакет ПО должен использоваться без внесения изменений. Если задуманные изменения существенны, оригинальное ПО должно быть сохранено и изменения должны применяться только к идентичной копии. Все изменения должны быть протестированы и задокументированы для того, чтобы их можно было повторить для будущих обновлений ПО	2
8.5.4	10.5.4	Черные ходы и программы типа «Троянский конь»	Существуют ли средства безопасности для проверки отсутствия черных ходов, недекларированных возможностей и программ типа «Троянский конь» в новом ПО и обновлениях. Черный ход может воздействовать на информацию скрытыми методами. Программы типа «Троянский конь» создаются для несанкционированного воздействия на систему	1
8.5.5	10.5.5	Разработка ПО сторонними организациями	Существуют ли средства защиты при разработке ПО сторонними организациями. Моменты, которые необходимо учитывать: лицензионное соглашение, требования по гарантии качества, тестирование перед инсталляцией на отсутствие черных ходов и недекларированных возможностей	2
Управление непрерывностью бизнеса				
9.1	11.1	Аспекты управления непрерывностью бизнеса		
9.1.1	11.1.1	Процесс управления непрерывностью бизнеса	Существует ли процесс по развитию и поддержке непрерывности бизнеса компании. Он должен включать: план обеспечения непрерывности бизнеса компании, регулярную проверку и обновление плана, формулирование и документирование стратегии непрерывности бизнеса	3

Продолжение табл. 3.1

Сообщение		Область аудита, цель и вопросы		Результаты
Требования	*Пункт стандарта*	*Область управления ИБ*	*Вопрос аудита безопасности*	*Выполнение Шкала от 1 до 5*
9.1.2	11.1.2	Непрерывность бизнеса и анализ ущерба	Определены ли действия, которые могут быть причиной нарушения бизнес-процессов, например: аварии оборудования, наводнения, пожары Проведен ли анализ рисков для определения ущерба таких воздействий Разработан ли стратегический план, основанный на проведенном анализе рисков и определяющий общий подход к обеспечению непрерывности бизнеса	3
9.1.3	11.1.3	Создание и реализация плана непрерывности бизнеса	Разработаны ли планы по восстановлению бизнес-операций в случае аварий в течение требуемого промежутка времени Регулярно ли обновляется и тестируется план	3
9.1.4	11.1.4	Среда разработки плана непрерывности бизнеса	Существует ли единый подход по разработке плана непрерывности бизнеса Поддерживается ли эта инфраструктура для гарантии того, что все планы согласованы и определены приоритеты по тестированию и поддержке Определены ли условия активации и персональная ответственность по выполнению каждого компонента плана	3
9.1.5	11.1.5	Тестирование, поддержка и переоценка планов непрерывности бизнеса	Регулярно ли тестируется план непрерывности бизнеса для гарантии того, что он актуален и эффективен Существуют ли процедуры, в которых определен порядок аудита плана непрерывности бизнеса по оценке его эффективности Включены ли процедуры в программу управления изменениями для соответствия плану непрерывности бизнеса	3

Сообщение		Область аудита, цель и вопросы		Результаты
Требования	*Пункт стандарта*	*Область управления ИБ*	*Вопрос аудита безопасности*	*Выполнение Шкала от 1 до 5*
Соответствие				
10.1	12.1	Соответствие требованиям законодательства		
10.1.1	12.1.1	Определение применимых требований законодательства	Определены ли и задокументированы для каждой информационной системы все требования законодательства, нормативных актов и договорных обязательств Определены ли и задокументированы средства защиты и персональная ответственность по соблюдению этих требований	4
10.1.2	12.1.2	Право интеллектуальной собственности	Существуют ли процедуры, гарантирующие соответствие с требованиями законодательства по использованию материалов, в отношении которых могут быть установлены такие права на защиту интеллектуальной собственности, как авторское право, конструкторское право, торговая марка Правильно ли осуществлены процедуры Поставляется ли ПО под действием лицензионного соглашения, которое ограничивает использование продукта определенными компьютерами. Исключение может быть сделано только для резервных копий ПО	4
10.1.3	12.1.3	Защита документов компании	Защищены ли важные документы компании от уничтожения и фальсификации	4
10.1.4	12.1.4	Защита персональных данных и права на частную жизнь	Существует ли структура управления и средства защиты персональных данных и права на частную жизнь	4

Продолжение табл. 3.1

Продолжение табл. 3.1

Сообщение		Область аудита, цель и вопросы		Результаты
Требования	*Пункт стандарта*	*Область управления ИБ*	*Вопрос аудита безопасности*	*Выполнение Шкала от 1 до 5*
10.1.5	12.1.5	Предотвращение неправомерного использования средств обработки информации	Рассматривается ли использование средств обработки информации для любого нецелевого или несанкционированного назначения без одобрения руководства как ненадлежащее использование средств Появляется ли при регистрации предупреждающее сообщение на мониторе компьютера о том, что система, в которую осуществляется вход, является частной собственностью и несанкционированный доступ запрещен	3
10.1.6	12.1.6	Требования законодательства по использованию шифрования	Существуют ли и учтены ли требования отечественного законодательства по использованию шифрования	4
10.1.7	12.1.7	Сбор доказательств	Приведен ли процесс, связанный со сбором доказательств, в соответствие с требованиями законодательства и лучшей практикой	3
10.2	12.2	Аудит ПИБ и технического соответствия		
10.2.1	12.2.1	Соответствие ПИБ	Регулярно ли проводится аудит всех областей компании на соответствие ПИБ, стандартам и процедурам	3
10.2.2	12.2.2	Проверка технического соответствия	Регулярно ли проверяются информационные системы на соответствие техническим стандартам безопасности Осуществляется ли проверка технического соответствия компетентными и авторизованными сотрудниками или под их наблюдением	3
10.3	12.3	Рекомендации по аудиту систем		
10.3.1	12.3.1	Средства аудита систем	Тщательно ли спланированы и согласованы требования аудита и проверки работы ОС для минимизации риска нарушения бизнес-процессов	3

Окончание табл. 3.1

Сообщение		Область аудита, цель и вопросы		Результаты
Требования	*Пункт стандарта*	*Область управления ИБ*	*Вопрос аудита безопасности*	*Выполнение Шкала от 1 до 5*
10.3.2	12.3.2	Защита средств аудита систем	Защищен ли доступ к средствам аудита, таким, как ПО или файлы данных, для предотвращения любых возможностей злоупотребления или компрометации	2

В целом вопросами развития стандарта ISO 17799 (BS 7799) занимаются международный комитет Joint Technical Committee ISO/IEC JTC 1 совместно с Британским институтом стандартов и служба UKAS (United Kingdom Accredited Service). Названная служба производит аккредитацию организаций на право аудита информационной безопасности в соответствии со стандартом BS 7799:2002. Сертификаты, выданные этими органами, признаются во многих странах. При этом в случае сертификации компании по

стандартам ISO 9001 или ISO 9002 стандарт BS 7799-1:2002 разрешает совместить сертификацию системы информационной безопасности с сертификацией на соответствие стандартам ISO 9001 или 9002 как на первоначальном этапе, так и при контрольных проверках. Для этого необходимо выполнить условие участия в совмещенной сертификации зарегистрированного аудитора по стандарту BS 7799:2002. Кроме того, в планах совместного тестирования должны быть четко указаны процедуры проверки системы информационной безопасности, а сертифицирующие органы должны гарантировать тщательность проверки информационной безопасности. Ниже, в табл. 3.2, рассматриваются различия и сходство вопросов сертификации на соответствие требованиям стандартов ISO 17799 (BS 7799) и ISO 9001.

3.2. Международный стандартISO 15408

Следуя по пути интеграции, в 1990 году Международная организация по стандартизации (ISO) и Международная электротехническая комиссия (TEC) разработали специализированную систему мировой стандартизации, а ISO начала создавать международные стандарты по критериям оценки безопасности информационных технологий для общего использования, названные «Common Criteria for Information Technology Security Evaluation» («Общие критерии оценки безопасности информационных технологий») или просто «Common Criteria» («Общие критерии») (см. рис. 3.6). В их разработке участвовали: Национальный институт стандартов и технологии и Агентство национальной безопасности (США), Учреждение безопасности коммуникаций (Канада), Агентство информационной безопасности (Германия), Агентство национальной безопасности коммуникаций (Нидерланды), Органы исполнения программы безопасности и сертификации ИТ (Англия), Центр обеспечения безопасности систем (Франция).

...

Рис. 3.6. Этапы развития ISO/IEC 15408

В дальнейшем «Общие критерии» неоднократно редактировались. В результате 8 июня 1999 года был утвержден Международный стандарт ISO/IEC 15408 под названием «Общие критерии оценки безопасности информационных технологий» (ОК) (см. рис. 3.7).

...

Рис. 3.7. Состав стандарта ISO/IEC 15408

Таблица 3.2. Вопросы сертификации, поднимаемые в стандартах ISO 17799 и ISO 9001

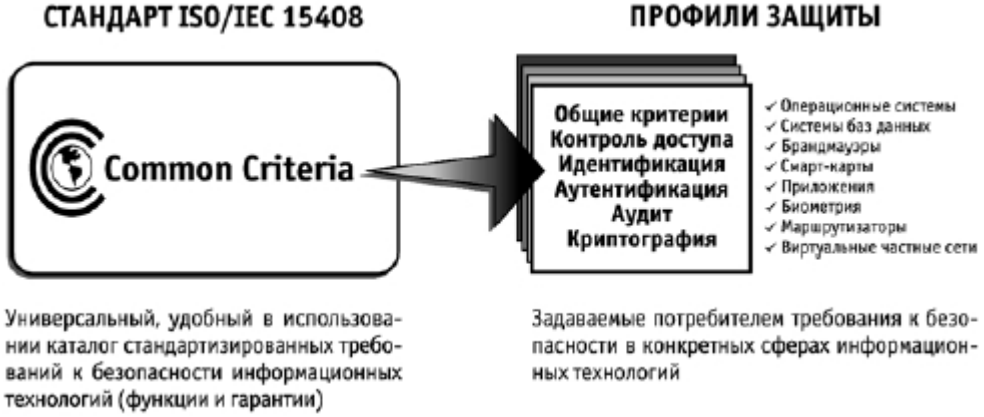
Номер статьи стандарта BS 7799-2: издание 1999 г.	Номер статьи стандарта BS 7799-2: издание 2002 г.	Номер статьи стандарта ISO 9001: 2000 г.
–	0 Введение	0 Введение
1 Сфера применения	1 Сфера применения	1 Сфера применения
	2 Нормативные отсылки	2 Нормативные отсылки
2 Термины и определения	3 Термины и определения	3 Термины и определения
	3.1 Доступность	
	3.2 Конфиденциальность	
	3.3 Информационная безопасность	
	3.4 Система управления информационной безопасностью	
	3.5 Целостность	
	3.6 Принятие рисков	
	3.7 Анализ рисков	
	3.8 Оценка рисков	
	3.9 Анализ рисков	
	3.10 Управление рисками	
	3.11 Обращение и рисками	
2.1 Отчет о применимости	3.12 Отчет о применимости	

Требования системы управления информационной безопасностью	Система управления информационной безопасностью	Требования системы управления качеством
3.1 Общие положения	4.1 Общие требования	
3.2 Создание структуры управления	4.2 Создание и управление ISMS	
	4.2.1 Создание ISMS	
	4.2.2 Реализация и эксплуатация ISMS	
	4.2.3 Контроль и изучение ISMS	
	4.2.4 Содержание и совершенствование ISMS	
	4.3 Требования к документации	4.2 Требования к документации
	4.3.1 Общие положения	4.2.1 Общие положения
	4.3.2 Контроль документов	4.2.3 Контроль документов
	4.3.3 Контроль учетно-отчетных документов	4.2.4 Контроль учетно-отчетных документов
	5 Ответственность руководства	5 Ответственность руководства
	5.1 Обязательства руководства	5.1 Обязательства руководства
	5.2 Управление ресурсами	6 Управление ресурсами
	6 Проверка системы управления	5.6 Проверка системы управления
	6.1 Общие положения	5.6.1 Общие положения
	6.2 Входные данные проверки	5.6.2 Входные данные проверки
	6.3 Выходные данные проверки	5.6.3 Выходные данные проверки
	6.4 Внутренний аудит ISMS	8.2.2 Внутренний аудит ISMS
	7 Совершенствование ISMS	8 Совершенствование ISMS
	7.1 Постоянное совершенствование	8.5.1 Постоянное совершенствование
	7.2 Коррективы	8.5.2 Коррективы
	7.3 Профилактика	8.5.3 Профилактика

4 Детальные меры контроля	Приложение «А» Задачи контроля и меры контроля	
-	A.1 Введение	
-	A.2 Рекомендации передовой практики	
4.1 Политика безопасности	A.3 Политика безопасности	
4.2 Организационная безопасность	A.4 Организационная безопасность	
4.3 Классификация и контроль активов	A.5 Классификация и контроль активов	
4.4 Безопасность персонала	A.6 Безопасность персонала	
4.5. Физическая и окружающая безопасность	A.7 Физическая и окружающая безопасность	
4.6. Управление связью и операциями	A.8 Управление связью и операциями	
4.7 Контроль доступа	A.9 Контроль доступа	
4.8 Разработка и содержание системы	A.10 Разработка и содержание системы	
4.9 Управление непрерывностью бизнеса	A.11 Управление непрерывностью бизнеса	
4.10 Соблюдение норм	A.12 Соблюдение норм	
	Приложение «В» Рекомендации по использованию стандарта	
	Приложение «С» Соответствие между ISO 9001:2000, ISO 14001:1996 и BS 7799, Часть 2:2002	Приложение «А» Связи между ISO 14001 и ISO 9001

Окончание табл. 3.2

Таким образом, «Общие критерии» обобщили содержание и опыт использования «Оранжевой книги», развили европейские и канадские критерии и воплотили в реальные структуры концепцию типовых профилей защиты федеральных критериев США. В ОК проведена классификация широкого набора требований безопасности ИТ, определены структуры их группирования и принципы использования (рис. 3.8). Главные достоинства ОК – полнота требований безопасности и их систематизация, гибкость в применении и открытость для последующего развития.



...

Рис. 3.8. Схема классификации требований ISO/IEC 15408

Использование методик данного стандарта позволяет определить для компании те критерии, которые могут быть основой для выработки правил и политик безопасности компании. Кроме того, эти критерии позволяют проводить наиболее полное сравнение результатов оценки защитных свойств корпоративных информационных систем с помощью общего перечня (набора) требований, а также методов точных измерений, которые проводятся во время получения оценок защиты. На основе этих требований в процессе выработки оценки уровня защиты устанавливается уровень доверия.

Результаты оценок защиты позволяют определить для компании достаточность защиты корпоративной информационной системы.

Вместе с тем в ОК главное внимание уделено защите от несанкционированного доступа. Модификации или потери доступа к информации в результате случайных или преднамеренных действий и ряд других аспектов информационной безопасности остались не рассмотренными. Например, оценка административных мер безопасности, оценка защиты безопасности от побочных электромагнитных излучений, методики оценки различных средств и мер безопасности, критерии для оценки криптографических методов защиты информации.

Поэтому необходимо дополнять данный подход рядом своих собственных апробированных методик оценки важнейших элементов защиты. Дополненные таким образом ОК можно использовать как при задании требований к продуктам и системам информационных технологий, правилам и политикам безопасности компании, так и при оценке безопасности ИТ.

В результате на практике становится возможным реализовать следующие существенные особенности:

• охватить весь спектр ИТ и учесть особенности каждой конкретной системы при задании требований и правил безопасности;

Предлагаемые адаптированные ОК предназначены для оценки безопасности как систем ИТ, разрабатываемых для автоматизации в конкретной области применения, так и отдельных продуктов ИТ, которые имеют универсальное предназначение. Такие ОК применимы к оценке безопасности и аппаратных средств, и программного обеспечения ИТ.

• избежать жесткой классификации ИТ по уровню безопасности;

Вместо этого становится возможным использовать сформированные по определенным правилам типовые наборы требований по различным видам ИТ, уровням ЗИ и другим классификационным признакам. Перечень типовых требований не регламентируется – они формируются по результатам прохождения определенной процедуры согласования и апробации. Для оптимального сочетания типовых требований с требованиями, учитывающими особенности конкретной области применения ИТ, используются два ключевых понятия: профиль защиты и задание по безопасности.

Профиль защиты представляет собой функционально полный, прошедший апробацию, стандартизованный набор требований, предназначенный для многократного использования.

Задание по безопасности – это полная комбинация требований, являющихся необходимыми для создания и оценки информационной безопасности конкретной системы или продукта ИТ.

Таким образом, работы по анализу требований, реализуемые на основе стандарта ОК, позволяют грамотно задать требования к безопасности ИТ. Результаты работы могут также использоваться для сравнительного анализа различных систем и продуктов ИТ. В целом же предоставляется развитая система структурированных требований для выбора механизмов обеспечения безопасности при проектировании и разработке ИТ.

• предложить детальный и структурированный перечень требований для механизмов

безопасности, мер и средств обеспечения их реализации;

Предлагаемые адаптированные ОК содержат две категории требований: функциональные и требования гарантированности.

Первые описывают функции, которые необходимо реализовать в ИТ для обеспечения их безопасности. Вторые определяют меры и средства, которые должны быть использованы в процессе создания ИТ для полной уверенности в правильности реализации механизмов безопасности и в их эффективности. Все требования ОК разбиваются по классам, семействам, компонентам и элементам с определением зависимостей одних компонентов от других. Определяются допустимые действия над компонентами, которые могут применяться для конкретизации задаваемых требований безопасности.

• охватить весь жизненный цикл ИТ, начиная от формирования целей и требований обеспечения безопасности, разработки действенных политик безопасности и кончая поставкой и наладкой ИТ на конкретном объекте;

• реализовать возможность формирования наборов требований и правил безопасности по уровням безопасности ИТ, сопоставимых с другими системами оценки;

Преемственность предлагаемых оценок безопасности достигается за счет возможности формирования профилей защиты, соответствующих наборам требований, которые определяют уровни безопасности ИТ в других системах.

• гарантировать комплексность подхода к обеспечению безопасности ИТ;

Адаптация ОК позволяет обеспечить безопасность ИТ на всех этапах жизненного цикла КИС – от этапа анализа требований (на этапе формирования замысла информационной системы) до реализации, эксплуатации и сопровождения системы. Здесь предусматриваются следующие уровни рассмотрения безопасности ИТ:

– безопасность окружающей среды (законы, нормативные документы, организационные меры, физическое окружение, определяющие условия применения ИТ, а также существующие и возможные угрозы безопасности ИТ);

– цели безопасности (намерения, определяющие направленность мер по противодействию выявленным угрозам и обеспечению безопасности);

– требования безопасности (полученный в результате анализа целей безопасности набор технических требований для механизмов безопасности и гарантированности их реализации, обеспечивающий достижение сформулированных целей);

– спецификации безопасности (проектное представление механизмов безопасности, реализация которых гарантирует выполнение требований безопасности);

– разработка (реализация механизмов безопасности со спецификациями).

• обеспечение комплексности оценки безопасности ИТ;

Адаптация ОК позволяет оценивать безопасность ИТ в процессе их разработки на наиболее важных этапах. Предусмотрены следующие стадии оценки:

– профиля защиты,

– задания по безопасности,

– реализованных механизмов безопасности.

В первом случае устанавливается, что сформированный профиль является полным, последовательным, технически правильным и пригодным для использования в качестве типового для определенного класса ИТ. Использование оцененных, апробированных и стандартизованных профилей защиты дает возможность избежать затрат на разработку требований по информационной безопасности к создаваемым системам и изделиям и исключить дополнительные затраты на их обоснование. Вторая стадия призвана установить, что задание соответствует требованиям профиля защиты и содержит полный, последовательный и технически правильный набор требований, необходимых для обеспечения безопасности конкретного объекта. Задание по безопасности подлежит согласованию на предприятии и является в дальнейшем основным документом, в соответствии с которым оценивается безопасность разрабатываемой ИС.

Наконец, цель третьей стадии – установить, что механизмы безопасности обеспечивают

выполнение всех требований, содержащихся в задании по безопасности.

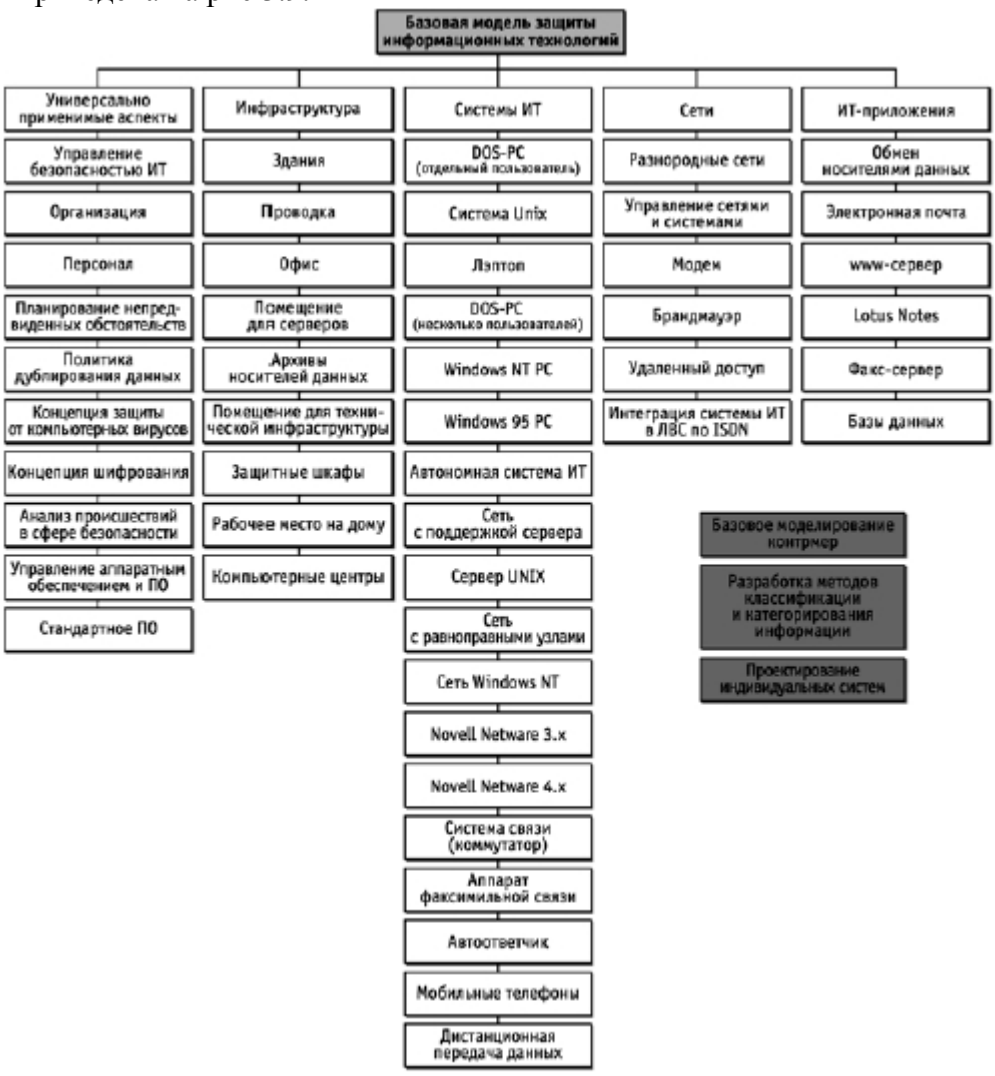
• предусмотреть расширяемость требований к безопасности ИТ.

Адаптация ОК позволяет предложить наиболее полный на сегодня набор критериев в области безопасности ИТ, который удовлетворяет потребностям основных категорий и групп пользователей, а также разработчиков информационных систем. Интересно отметить, что в настоящее время Европейской ассоциацией производителей компьютерной техники ECMA уже осуществляются проекты по разработке стандарта «Расширенный коммерческий функциональный класс оценки безопасности (E-COFC)». В этом документе принятый в 1993 году стандарт ECMA-205 «Коммерческий функциональный класс оценки безопасности (COFC)» перерабатывается в соответствии с требованиями и терминологией ОК.

И если данный подход дополнить, кроме того, анализом требований по организации режима информационной безопасности компании, то получится достаточно мощный инструмент для оценки безопасности информационных технологий отечественных компаний и разработки эффективных политик безопасности.

3.3. Германский стандарт BSI

В отличие от ISO 17799 германское «Руководство по защите информационных технологий для базового уровня защищенности» 1998 года посвящено детальному рассмотрению частных вопросов создания политик безопасности компании и управления безопасностью в целом. Это руководство представляет собой гипертекстовый электронный учебник объемом примерно 4 Мб (в формате HTML). Общая структура германского стандарта BSI приведена на рис 3.9.



...

Рис. 3.9. Структура германского стандарта BSI

В германском стандарте BSI представлены:

• общая методика разработки политик безопасности и управления информационной безопасностью в целом (организация менеджмента в области информационной безопасности, методология использования руководства);

• описания компонентов современных информационных технологий;

• описания основных компонентов организации режима информационной безопасности (организационный и технический уровни защиты данных, планирование действий в чрезвычайных ситуациях, поддержка непрерывности бизнеса);

• характеристики объектов информатизации (здания, помещения, кабельные сети, контролируемые зоны);

• характеристики основных информационных активов компании (в том числе аппаратное и программное обеспечение, например рабочие станции и серверы под управлением операционных систем семейства DOS, Windows и UNIX);

• характеристики компьютерных сетей на основе различных сетевых технологий, например сети Novell NetWare, сети UNIX и Windows;

• характеристика активного и пассивного телекоммуникационного оборудования ведущих вендоров, например Cisco Systems;

• подробные каталоги угроз безопасности и мер контроля (более 600 наименований в каждом каталоге).

Существенно, что политики безопасности компании рассматриваются по определенному сценарию: общее описание информационного актива компании – возможные угрозы и уязвимости безопасности – возможные меры и средства контроля и защиты. С версиями этого стандарта на немецком и английском языках можно познакомиться подробнее на Web-сервере BSI (http://www.bsi.de).

3.4. Стандарт CobiT

К настоящему времени аудиторскими компаниями образованы различные государственные и негосударственные ассоциации, объединяющие профессионалов в области аудита информационных систем, которые занимаются созданием и сопровождением, как правило, закрытых, тщательно охраняемых от посторонних глаз стандартов аудиторской деятельности в области информационных технологий (см. табл. 3.3).

Таблица 3.3. Сравнение некоторых стандартов аудита ИТ

	CobIT	SAC	COSO	SAS 78/94
Целевая аудитория	TOP-менеджеры, пользователи, аудиторы информационных систем	Внутренние аудиторы компании	TOP-менеджеры	Внешние аудиторы
Под аудитом понимается	Системный процесс проверки на соответствие декларируемым целям политики безопасности Организация обработки данных, норм эксплуатации	Системный процесс проверки на соответствие декларируемым целям бизнес-процессов, политики безопасности и кадровой политики	Системный процесс проверки на соответствие декларируемым целям бизнес-процессов, а также политики безопасности компании	Системный процесс проверки на соответствие декларируемым целям бизнес-процессов, а также политики безопасности компании
Цели аудита	Развитие бизнеса, повышение его эффективности и рентабельности, следование нормативно-правовой базе	Развитие бизнеса, финансовый контроль, следование нормативно-правовой базе	Развитие бизнеса, финансовый контроль, следование нормативно-правовой базе	Развитие бизнеса, финансовый контроль, следование нормативно-правовой базе
Область применения	Планирование и организация, постановка задач и выполнение, эксплуатация и сопровождение, мониторинг	Управление производством, эксплуатация автоматизированных и автоматических систем управления	Управление производством, риск-менеджмент, управление информационными системами, мониторинг корпоративных информационных систем	Управление производством, управление рисками, мониторинг и управление корпоративными информационными системами
Акцент	Информационный менеджмент	Информационный менеджмент	Менеджмент	финансовый менеджмент
Срок действия сертификата аудита	Интервал времени	Время проверки	Интервал времени	Интервал времени
Заинтересованные лица	TOP-менеджеры компании	TOP-менеджеры компании	TOP-менеджеры компании	TOP-менеджеры компании
Объем документов, регламентирующих проведение аудита	4 документа общим объемом 187 страниц	12 частей общим объемом 1193 страницы	4 тома общим объемом 353 страницы	2 документа общим объемом 63 страницы

Ассоциация ISACA, в отличие от других, занимается открытым аудитом информационных систем. Она основана в 1969 году и в настоящее время объединяет более 35 тыс. членов из более чем 100 стран, в том числе и России. Ассоциация ISACA координирует деятельность более чем 38 тыс. сертифицированных аудиторов информационных систем (CISA – Certified Information System Auditor), имеет свою систему стандартов в этой области, ведет исследовательские работы, занимается подготовкой кадров, проводит конференции. Ассоциация ISACA под аудитом информационной безопасности в информационной системе понимает процесс сбора сведений, позволяющих установить, обеспечиваются ли безопасность ресурсов компании, необходимые параметры целостности и доступности данных, достигаются ли цели предприятии в части эффективности информационных технологий.

По заявлениям руководящих органов ISACA, основная цель ассоциации – исследование, разработка, публикация и продвижение стандартизованного набора документов по управлению информационной технологией для ежедневного использования администраторами и аудиторами информационных систем. В интересах профессиональных аудиторов, руководителей информационных систем, администраторов и всех заинтересованных лиц ассоциация развивает свою концепцию управления информационными технологиями в соответствии с требованиями информационной безопасности. На основе этой концепции описываются элементы информационной технологии, даются рекомендации по разработке политик безопасности компании.

Концепция изложена в документе под названием CobiT 3rd Edition (Control Objectives for Information and Related Technology), который состоит из шести частей:

Часть 1: Резюме для руководителей (Executive Summary);

Часть 2: Определения и основные понятия (Framework). Помимо определений и основных понятий в этой части сформулированы требования к ним;

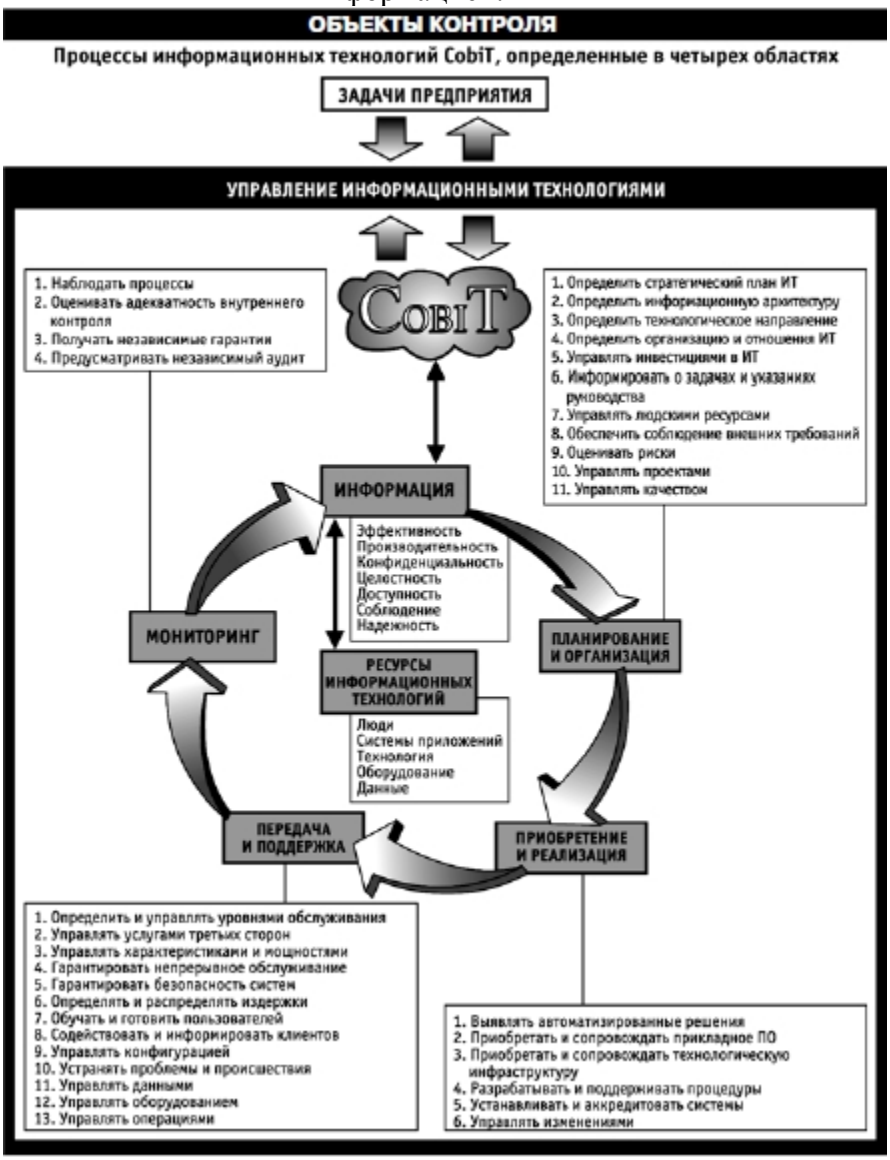
Часть 3: Цели контроля (Control Objectives);

Часть 4: Принципы аудита (Audit Guidelines);

Часть 5: Набор средств внедрения (Implementation Tool Set);

Часть 6: Принципы управления (Management Guidelines).

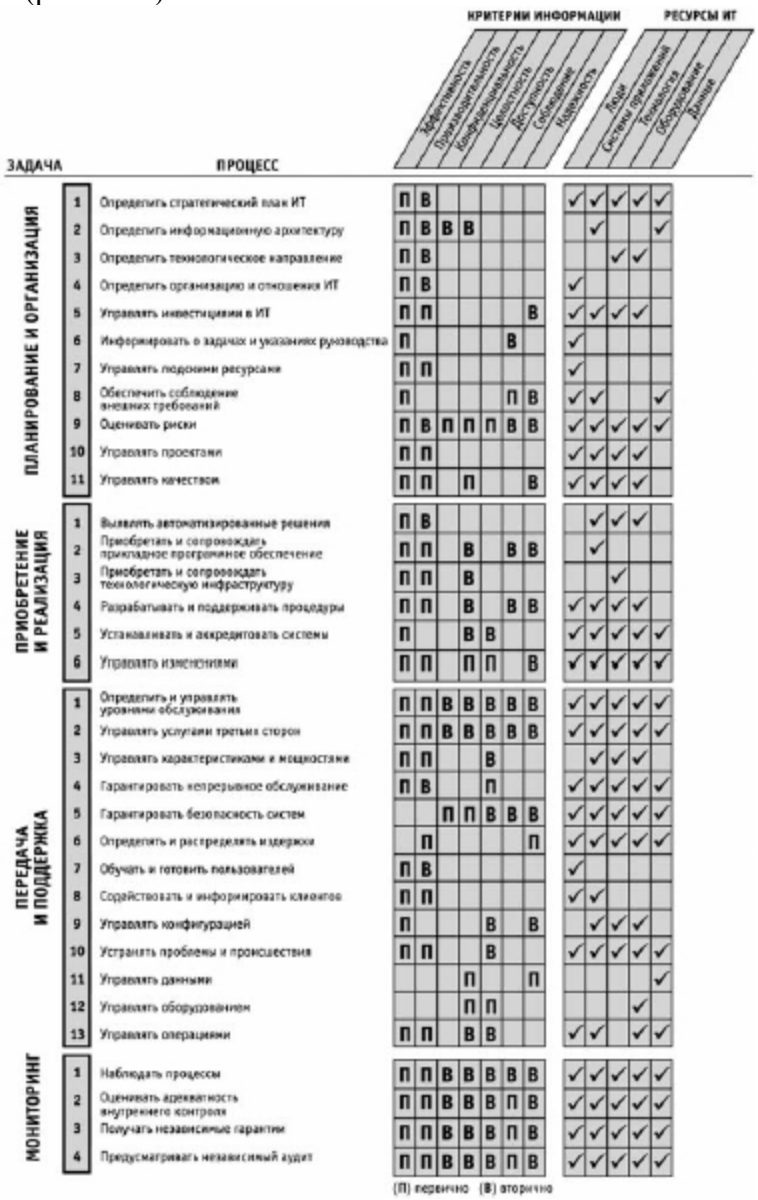
Третья часть этого документа в некотором смысле аналогична международному стандарту ISO 17799:2005 (BS 7799-1:2002). Примерно так же подробно приведены практические рекомендации по разработке политик безопасности и управлению информационной безопасностью в целом, но модели систем управления в сравниваемых стандартах сильно различаются. Стандарт CobiT (Control Objectives for Information and Related Technology) – пакет открытых документов, первое издание которого было опубликовано в 1996 году. Кратко основная идея стандарта CobiT выражается следующим образом: все ресурсы информационной системы должны управляться набором естественно сгруппированных процессов (рис. 3.10) для обеспечения компании необходимой и надежной информацией.



...

Рис. 3.10. Процессы управления ресурсами информационной системы

В модели CobiT присутствуют ресурсы информационных технологий, являющиеся источником информации, которая используется в бизнес-процессе. Информационная технология должна удовлетворять требованиям бизнес-процесса, сгруппированным определенным образом (рис. 3.11).



...

Рис. 3.11. Объекты контроля и управления информационными технологиями

Во-первых, требования к качеству технологии составляют показатели качества и стоимости обработки информации, характеристики ее доставки получателю. Показатели качества подробно описывают возможные негативные аспекты, которые в обобщенном виде входят в понятия целостности и доступности. Кроме того, в эту группу включаются показатели, относящиеся к субъективным аспектам обработки информации, например стиль, удобство интерфейсов. Характеристики доставки информации получателю – показатели, в

обобщенном виде входящие в показатели доступности и частично – в показатели конфиденциальности и целостности. Рассмотренная система показателей используется при управлении рисками и оценке эффективности информационной технологии.

Во-вторых, доверие к технологии – группа показателей, описывающих соответствие компьютерной информационной системы принятым стандартам и требованиям, достоверность обрабатываемой в системе информации, ее действенность.

В-третьих, показатели информационной безопасности – конфиденциальность, целостность и доступность обрабатываемой в системе информации.

3.5. Общие рекомендации по созданию политик безопасности

Обобщая изложенное выше, отметим, что в современных стандартах управления информационной безопасностью (см. табл. 3.4) вопросам разработки политик безопасности уделяется достаточное внимание (см. табл. 3.5).

Таблица 3.4. Новые стандарты в области защиты информации

Стандарт / Нормативный акт	Отрасль	Тип	Комментарии / указатели ресурса
ISO/IEC 17799	Международный – базовый	Стандарт	Международная организация по стандартизации www.iso-17799.com
BS 7799 Часть 1	Правительство Великобритании	Стандарт	Британский стандарт. Предшественник стандарта ISO 17799
AS4444/NZS4444	Правительство Австралии	Стандарт	Австралийский стандарт / Новозеландский стандарт. Заменен стандартом ISO 17799
HIPAA	Здравоохранение	Нормативный акт	Закон о праве перевода и отчетности медицинского страхования 1996 г.
Тестовые программы CIS	Всемирный консорциум	Стандарт	Тестовая программа Центра безопасности Интернет Solaris
Закон Грэмм-Лич-Билли (GLBA)	Закон о финансовых услугах США	Нормативный акт	Законодательный акт США, принятый в ноябре 1999 г.
Список 20 лучших SANS/FBI	Общая безопасность	Стандарт	Системное администрирование, организация сетей и безопасность / Федеральное бюро расследований
CVE	Общая безопасность	Стандарт	Общие факторы уязвимости и незащищенности MITRE
VISA	Банковское дело	Стандарт	Visa International и Visa USA
ISO 15408 (Общие критерии)	Международная программа безопасности – системы	Стандарт	Может заменять «Красную книгу» и «Оранжевую книгу» NSA
CASPR	Передовая практика GNU	Стандарт	Общепринятые правила и рекомендации по безопасности
OCC	Банковское дело	Нормативный акт	Управление контролера денежного обращения
FDIC	Банковское дело	Нормативный акт	Федеральная депозитная страховая корпорация
SysTrust	AICPA	Стандарт	Американский институт дипломированных присяжных бухгалтеров
FISCAM	GAO (Федеральное правительство) Финансовые системы	Нормативный акт	Руководство по аудиту и контролю федеральных информационных систем
CobiT	ISACA	Стандарт	Задачи контроля для информационных и смежных технологий
Справочники по безопасности IETF	Интернет-сообщество	Стандарт	Рабочая группа интернет-инженеров

...

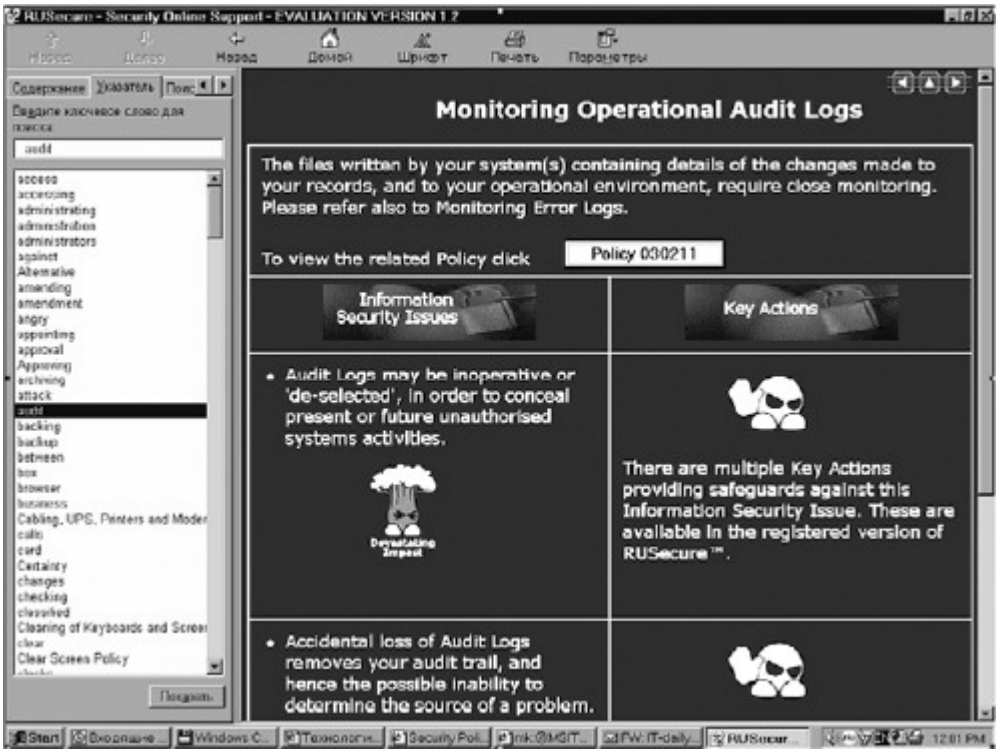
BS 7799 – British Standards Institute
NFPA – National Fire Protection Association
AICPA – Association of Independent Auditors
FIPS – Federal Information Processing Standards
ISO – International Standards Organization
SunTone – Sun Microsystems E-commerce Certification
FIDNet – PDD-63 Guidelines

Таблица 3.5. Роль политик безопасности в новых стандартах безопасности

Требование	BS 7799	NFPA 75	AICPA (SAS-70)	FFIEC (SP-5)	FEPS (80-140)	AICPA (SysTrust)	ISO (9004-2)	SunTone	FDDNet
Политика информационной безопасности	✓	✗	✓	✓	✓	✓	✓	✓	✓
Управление непрерывностью бизнеса	✓	✓	✓	✓	✓	✓	✓	✓	✓
Контроль доступа	✓	✗	✓	✓	✓	✓	✓	✓	✓
Разработка и сопровождение систем	✓	✗	✓	✓	✓	✓	✓	✓	✓
Физическая и окружающая безопасность	✓	✓	✓	✓	✓	✓	✓	✓	✓
Соблюдение норм	✓	✗	✗	✗	✗	✗	✗	✗	✓
Безопасность персонала	✓	✓	✓	✓	✓	✓	✗	✓	✓
Организация безопасности	✓	✗	✓	✓	✓	✓	✓	✓	✓
Управление связью и операциями	✓	✗	✓	✓	✓	✓	✓	✓	✓
Контроль и классификация активов	✓	✓	✓	✓	✓	✓	✓	✓	✓
Анализ рисков	✓	✓	✓	✓	✓	✓	✓	✓	✓
Испытания на проникновение	✓	✗	✓	✓	✓	✓	✗	✓	✓
Сертификация	✓	✗	✓	✓	✓	✓	✓	✓	✓

Например, в стандарте ISO 17799 (BS 7799-1) рекомендуется управление информационной безопасностью компании осуществлять на основе политик безопасности (рис. 3.12).

Рис. 3.12. Роль политики безопасности согласно стандарту ISO 17799 Для детализации требований к политикам безопасности можно воспользоваться специальными справочниками. Вид подобного справочника согласно рекомендациям стандарта ISO 17799 представлен на рис. 3.13.



...

Рис. 3.13. Справочник «\'ONLINE\' SECURITY POLICIES AND SUPPORT»

Демонстрационные версии (Evaluation version) Information Security Police SOS – Interactive «\'ONLINE\' SECURITY POLICIES AND SUPPORT» Security Professionals Guide можно загрузить с сайта www.rusecure.com. Явным достоинством справочника является гипертекстовая структура и удобная навигация. Еще один аналогичный продукт – «ISO 17799\'TOOLKIT POLICY TEMPLATES» – представляет электронную версию документа с примерными текстами политик безопасности в соответствии с рекомендациями стандарта ISO 17799. Содержание документа представлено ниже.

...

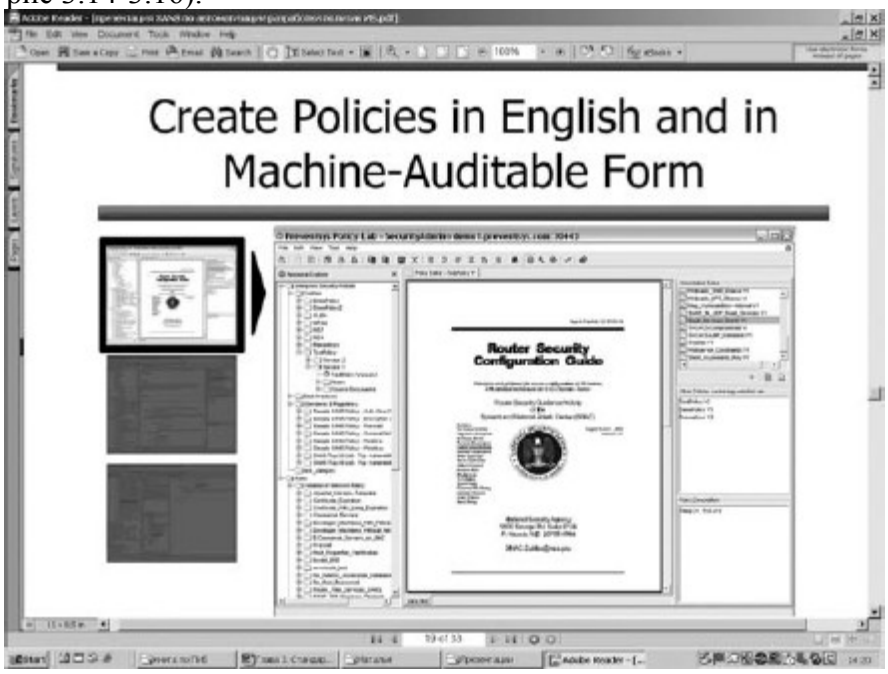
Contents

SECTION 02 SOFTWARE MAINTENANCE & UPGRADE
SECTION 03 OTHER SOFTWARE ISSUES
Chapter 05 Securing Hardware, Peripherals and Other Equipment SECTION 01 PURCHASING AND INSTALLING HARDWARE
SECTION 02 CABLING, UPS, PRINTERS AND MODEMS
SECTION 03 CONSUMABLES
SECTION 04 WORKING OFF PREMISES OR USING OUTSOURCED PROCESSING
SECTION 05 USING SECURE STORAGE
SECTION 06 DOCUMENTING HARDWARE
SECTION 07 OTHER HARDWARE ISSUES
Chapter 06 Combating Cyber Crime SECTION 01 COMBATING CYBER CRIME
Chapter 07 Controlling e?Commerce Information Security SECTION 01 E□COMMERCE ISSUES
Chapter 08 Developing and Maintaining In?House Software SECTION 01 CONTROLLING SOFTWARE CODE
SECTION 02 SOFTWARE DEVELOPMENT
SECTION 03 TESTING & TRAINING
SECTION 04 DOCUMENTATION
SECTION 05 OTHER SOFTWARE DEVELOPMENT
Chapter 09 Dealing with Premises related Considerations SECTION 01 PREMISES SECURITY
SECTION 02 DATA STORES
SECTION 03 OTHER PREMISES ISSUES
Chapter 10 Addressing Personnel Issues relating to Security SECTION 01 CONTRACTUAL DOCUMENTATION
SECTION 02 CONFIDENTIAL PERSONNEL DATA
SECTION 03 PERSONNEL INFORMATION SECURITY RESPONSIBILITIES
SECTION 04 HR MANAGEMENT
SECTION 05 STAFF LEAVING EMPLOYMENT
SECTION 06 HR ISSUES OTHER
Chapter 11 Delivering Training and Staff Awareness SECTION 01 AWARENESS
SECTION 02 TRAINING
Chapter 12 Complying with Legal and Policy Requirements SECTION 01 COMPLYING WITH LEGAL OBLIGATIONS
SECTION 02 COMPLYING WITH POLICIES
SECTION 03 AVOIDING LITIGATION
SECTION 04 OTHER LEGAL ISSUES
Chapter 13 Detecting and Responding to IS Incidents SECTION 01 REPORTING INFORMATION SECURITY INCIDENTS
SECTION 02 INVESTIGATING INFORMATION SECURITY INCIDENTS
SECTION 03 CORRECTIVE ACTIVITY
SECTION 04 OTHER INFORMATION SECURITY INCIDENT ISSUES
Chapter 14 Planning for Business Continuity SECTION 01 BUSINESS CONTINUITY MANAGEMENT (BCP)

3.6. Проблемы разработки политик безопасности

Сегодня отечественные предприятия остро нуждаются в политиках безопасности. Например, 44 % предприятий финансового и государственного сектора вынуждены пересматривать политики безопасности два или более раз в год. К тому же здесь часто возникают проблемы, которые заключаются в том, что высокоуровневые политики

безопасности, как правило, далеки от практики и никак не связаны с низкоуровневыми техническими политиками безопасности. В свою очередь технические политики безопасности не учитывают цели и задачи организации режима информационной безопасности компании в должной мере. При этом одни технические политики безопасности задают требуемые настройки маршрутизаторов и межсетевых экранов, другие определяют правила создания паролей и порядок использования Интернета, но, как правило, они рассматриваются разрозненно и не позволяют отладить целостную интегрированную систему управления политиками безопасности. В результате если спросить у ИТ-специалистов, что такое управление политиками безопасности, то можно получить более десяти различных ответов: управление правилами и конфигурациями, управление паролями, управление уязвимостями, управление критичными обновлениями, управление пользователями и пр. В действительности, эти определения, а также многие другие верны. Именно поэтому создание, внедрение и отслеживание политик безопасности – одна из самых важных и трудных задач для специалистов в области информационных технологий и защиты информации (см. рис 3.14-3.16).



...

Рис. 3.14. Пример создания политики безопасности для маршрутизатора Cisco

Среди наиболее общих проблем разработки требуемых политик безопасности следует отметить:

• сложности с поиском шаблонов или примеров подходящих по содержанию политик безопасности;

• недостаток собственных ресурсов или времени на разработку политик безопасности;

...

Рис. 3.15. Пример доработки шаблона политики безопасности

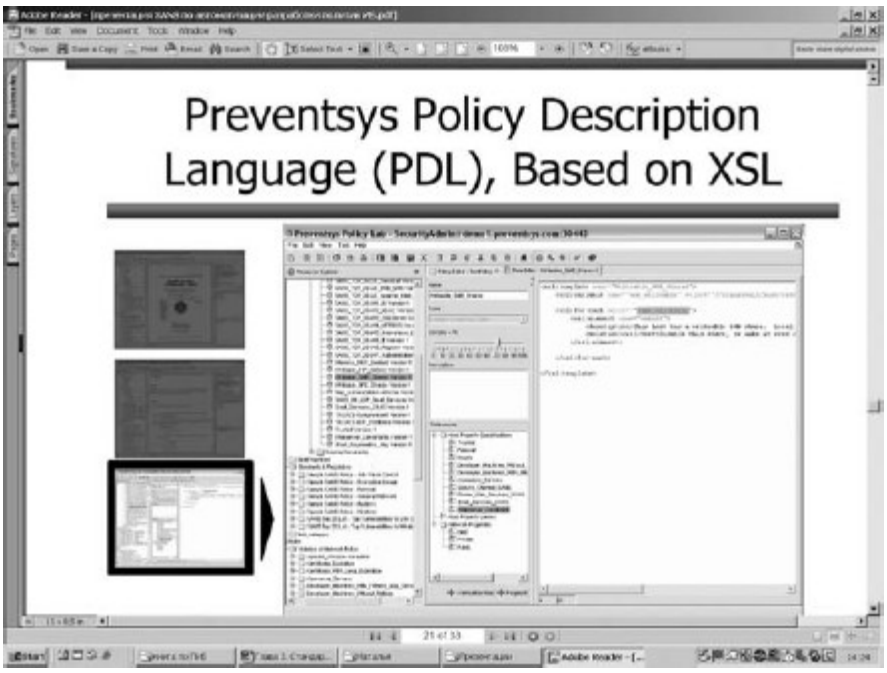
• сложности с обновлением политик безопасности, особенно в территориально распределенных компаниях, где часто мониторинг соответствия версий политик безопасности на конечных местах не осуществляется;

• слишком дорогие или не достигающие поставленной цели обучение, тестирование и аттестация знаний персонала по безопасности;

• сложности с обучением пользователей требованиям политик безопасности, отслеживанием компетентности сотрудников; потребность в использовании учебных средств с Web-интерфейсом для снижения издержек на поездки сотрудников в центральный офис для обучения и тестирования (аттестации);

• сложности с доведением политик безопасности до конечных пользователей;

• нехватка сотрудников, ответственных за управление политиками безопасности.



...

Рис. 3.16. Пример трансляции текста политики в технические спецификации

Для решения этих и других проблем можно воспользоваться специальными системами управления политиками безопасности. К основным задачам названных систем относятся:

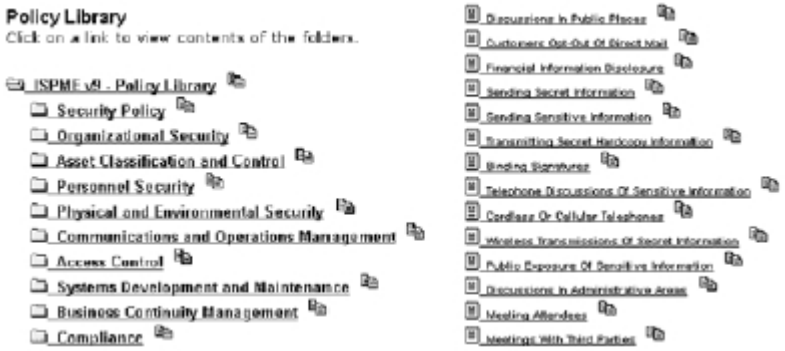
• эффективное создание текстовых политик безопасности и управление ими;

• осуществление программы ознакомления сотрудников с политиками информационной безопасности, проверка знаний и понимания названных политик;

• обеспечение связи между высокоуровневыми текстовыми политиками безопасности и техническими политиками конфигураций аппаратно-программных средств защиты информации и пр.

3.7. Обзор возможностей современных систем управления политиками безопасности

Как правило, современные системы управления политиками безопасности используют лицензированные библиотеки политик безопасности, разработанные другими компаниями. Так, например, продукт компании NetlQ, использует библиотеку Information Security Policies Made Easy (ISPME), решение компании Bindview ориентировано на применение библиотеки Meta Security Group, а система управления компании Zequel поставляется вместе с библиотекой компаний Protiviti и Bizmanualz. Каждый из названных продуктов включает примеры политик безопасности, разработанные на основе международного стандарта ISO 17799. Ряд компаний, например компания NetlQ, создавая политики безопасности на основе требований стандарта ISO 17799, сортируют их по функционалу и темам – от классификации данных до безопасности Web-серверов (см. рис. 3.17).



...

Рис. 3.17. Пример библиотеки политик безопасности

Общей особенностью современных систем управления политиками безопасности является возможность оперативно создавать высоуровневые и низкоуровневые политики безопасности, распространять эти политики сотрудникам компании и ослеживать факты ознакомления и согласия с политиками. Далее рассмотрим возможности современных инструментальных систем управления политиками безопасности на примере решений Bindview Policy Operations Center (POC), NetlQ VigilEnt Policy Center (VPC), Zequel Dynamic Policy. Сводные характеристики указанных систем управления политиками безопасности представлены в табл. 3.6 и 3.7.

Таблица 3.6. Характеристики систем управления политиками безопасности

Policy Manager Features			
	Bindview Policy Operations Center 5,1	**NetIQ VigilEnt Policy Center 4**	**Zequel Dynamic Policy 2.5.9**
INFRASTRUCTURE			
Server architecture	Service	Microsoft Windows 2000, XP.NT4	Microsoft Windows 2000
Web browser support	Any	Internet Explorer 4+, Netscape 7.x	Internet Explorer 5.5+
Import local users	Y	Y	Y
Database support	Service	Microsoft Data Engine, SQL	MySQL, Microsoft SQL
Web server included	Service	Y	Y
Multiple languages	N	N	Y
Customizable interface	Y	Y	Y
Context-sensitive help	Y	N	N
Digital signatures	N	Y	N
Distributed administration	Y	Y	Y
SSL	Default	Optional	Optional
Audit logs for system access	N	Y	N
Advanced password management	N	Y	N
Create users and groups	Users	Users, groups	Users, groups
USER ACCOUNTS			
Directory integration	Service	Active Directory, LDAP, NTD	LDAP, Sun One N
Users cancreate own accounts	N	Y	N
Role-based access to information	Y	Y	Y
Policy-creation editor	HTML	HTML, Word, VFC	HTML
POLICY CREATION & MANAGEMENT			
Version tracking	Y	Y	Y
Work flow	Y	Y	Y
Subfolder organization	Y	Y	Y
Search	Y	Y	Y
Export to XML	N	Y	N
Export to PDF	N	N	Y
Export to external security-management app	N	Vulnerability Manager	N
User alerts to view and review new documents	N	Y	Y
Spellcheck	N	Y	N
Templates	GbBA, HIPAA, ISO 17799	GLBA, HIPAA, ISO 17799, SOX	ISO 17799, SOX
Create and publish quiz	Y	Y	Y
Create and publish presentation	Y	N	N
Automated news alerts	Y	Y	Y
Automated vulnerability alerts	Y	N	N
User incident report form	N	Y	Y
Anonymous incident report form	N	Y	N
Standard reports	Y	Y	Y
Configurable reports	N	N	N
Export reports	Y	Y	N
Publishes reports to Web interface for review	Y	N	N
Price per user (1000 users)	$35	$10	$29.50

Y—Yes, N—No

Таблица 3.7. Оценка возможностей систем управления политиками безопасности

Report Card: Policy Managers			
	NetIQ VigilEnt Policy Center 4	**Bindview Policy Operations Center 5,1**	**Zequel Dynamic Policy 2.5.9**
CREATION			
Archive [10%)	3,75	4,5	2,5
Content (10%)	4	4,5	3,5
Edit [10%]	4,5	3,5	3,5
Work flow (10%)	4	4	3,5
PUBLICATION (20%)	4	4,5	4
FEATURES (15%)	4,5	3,75	3,75
IMPLEMENTATION Reporting [10%)	4,5	3	3,5
Quizes (5%)	4,5	3,5	4
PRICE (10%)	5	3	4
TOTAL SCORE (100%)	4,28	3,89	3,61
A>4,3; B>3,5; C>2,5; D> 1,5; F<1,5 A÷C grades include + OR - in their ranges. Total scores and weighted scores are based on a scale of 0÷5.	**b+**	**b**	**b−**
Customize the results of this report card using the Interactive report Card, a Java applet, at www.secureenterprisemag.com			

3.7.1 Bindview Policy Operations Center

Основное отличие Policy Operations Center Bindview Corp. (www.bindview.com) от других систем управления политиками безопасности заключается в том, что Bindview POC

по существу является удаленным сервисом компании Bindview. В качестве библиотеки шаблонов политик безопасности используется разработка компании Meta Security Group.

Уникальной особенностью системы является встроенная возможность анализа защищенности корпоративной информационной системы (vulnerability reporting). Однако в целом названная система уступает по функциональным возможностям NetlQ, VigilEnt Policy Center (VPC) и DynamicPolicy. Особенно это заметно при создании и внедрении политик безопасности, а также соответствующих тестов для проверки знаний сотрудников компании.

Как сервис Bindview POC не требует каких-либо затрат на серверное оборудование. Но поскольку продукт работает удаленно, нет возможности подключить к нему корпоративную службу каталога, однако пользователи могут быть импортированы через текстовый файл. Для безопасного удаленного доступа к серверу может использоваться протокол SSL (128-bit encryption). Пользовательский интерфейс POC наиболее развит из всех продуктов. POC отображает, в каком статусе находится политика безопасности – в черновом варианте, на согласовании, на утверждении или уже утверждена.

Для создания политики безопасности используется мастер (wizard), который позволяет выбрать подходящий способ создания политики безопасности – наследование примера политики безопасности или загрузка готовой политики.

После подготовки на своем компьютере черновой версии политики безопасности уполномоченное лицо производит загрузку политики на сервер. После импортирования политика безопасности получает новый номер версии, при этом старая версия политики архивируется. При необходимости сотрудники, согласующие политики безопасности, могут обращаться к предыдущим версиям политики безопасности.

3.7.2. Zequel Technologies DynamicPolicy

DynamicPolicy функционирует под управлением Windows 2000 Server (с поддержкой SMTP) на платформе Pentium IV (с минимальным объемом ОЗУ 512 Мб) и поставляется с собственным Web-сервером (Apache 1.3.27 и PHP 4.3.1). После установки DynamicPolicy для запуска и остановки Apache и MySQL используется специальный скрипт.

Текущая версия Zequel Technologies DynamicPolicy (www.zequel.com) по своей функциональности не уступает POC и VPC. Эта система управления политиками безопасности позволяет импортировать и экспортировать примеры политик безопасности, в частности политики безопасности стандартов ISO 17799 и SOX. Далее становится возможным разрабатывать свои собственные, оригинальные политики безопасности. При этом пользовательский интерфейс DynamicPolicy достаточно сложен и может вызвать определенные трудности на начальном этапе изучения системы.

DynamicPolicy позволяет определить группы пользователей с определенными ролями, например для согласования или утверждения политик безопасности. При согласовании политик безопасности имеется возможность ограничить для отдельных сотрудников просмотр комментариев и замечаний других сотрудников, а также проводить закрытые обсуждения политик безопасности.

DynamicPolicy не поставляется с примерами тестов для проверки качества понимания соответствующей политики, однако при необходимости эти тесты можно создать. Например, можно создать тест из 10 вопросов (максимально 100), используя смешанный выбор – многовариантный выбор или ответ «да/нет», а также установить процент правильных ответов для прохождения теста (например, 100 %). После связывания теста с политикой безопасности пользователь не может указать на то, что ознакомлен с политикой до тех пор, пока не сдаст тест и не наберет требуемого процента правильных ответов. При этом его начальник имеет возможность получить отчет по не сдавшим к определенному моменту времени тест пользователям и, соответственно, не способным нести ответственность за нарушение политики безопасности. Формально это может являться причиной для отклонения прав доступа сотрудника к работе с определенными данными и приложениями компании и даже понижения формы допуска в целом.

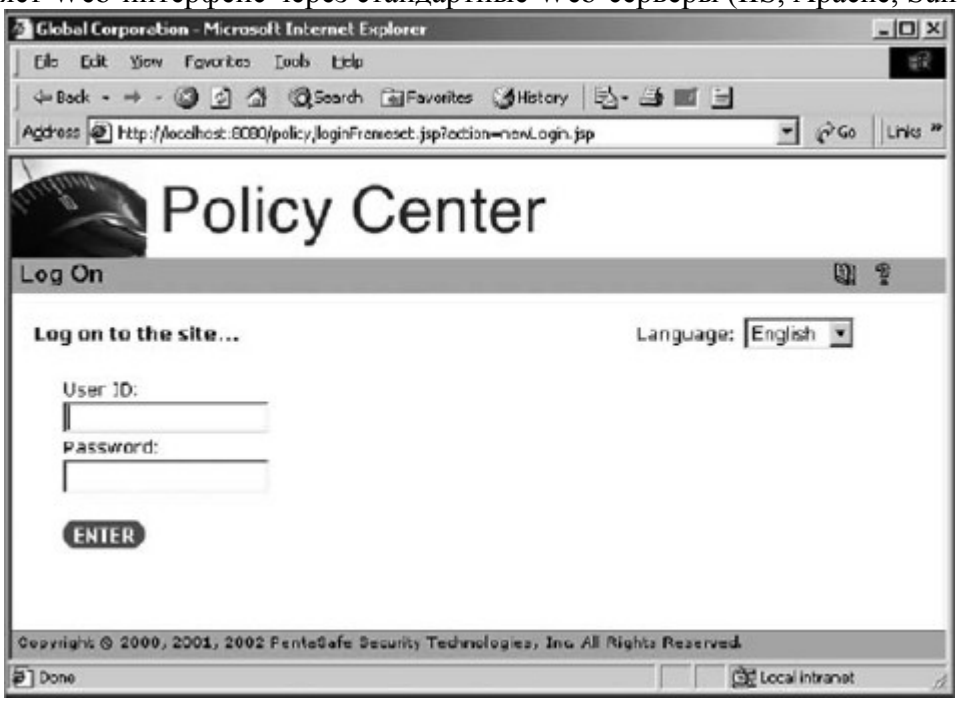
3.7.3. NetlQ VigilEnt Policy Center

VigilEnt Policy Center NetlQ, Corp. (www.netiq.com) позволяет управлять жизненным циклом создания и внедрения текстовых политик безопасности в крупных организациях и на предприятиях. Это дает возможность поддерживать политики безопасности компании в актуальном состоянии, легко изменять их и предоставлять к ним доступ целевым группам сотрудников через Web-браузеры. Также Policy Center позволяет проводить проверку осведомленности и определять степень знания политик безопасности отдельных категорий сотрудников компании (см. рис. 3.18 и 3.19).

По сравнению с рассмотренными ранее системами управления политиками безопасности NetlQ VPC обладает наиболее развитыми функциональными возможностями по созданию и внедрению политик безопасности.

VPC была разработана компанией Pentasafe Security Technologies (в 2002 году приобретена компанией NetlQ). VPC работает под управлением Windows 2003/2000 Server, XP, NT 4 на платформе с CPU от 866 МГц. NetlQ VPC использует СУБД Microsoft SQL Server версии 7 и выше или Oracle версии 9 и выше, а также включает MSDE (Microsoft Data Engine) 1.0.

Установка VPC не вызывает затруднений, продукт устанавливается как сервис и предоставляет Web-интерфейс через стандартные Web-серверы (IIS, Apache, Sun One).



...

Рис. 3.18. Интерфейс системы управления политиками безопасности

...

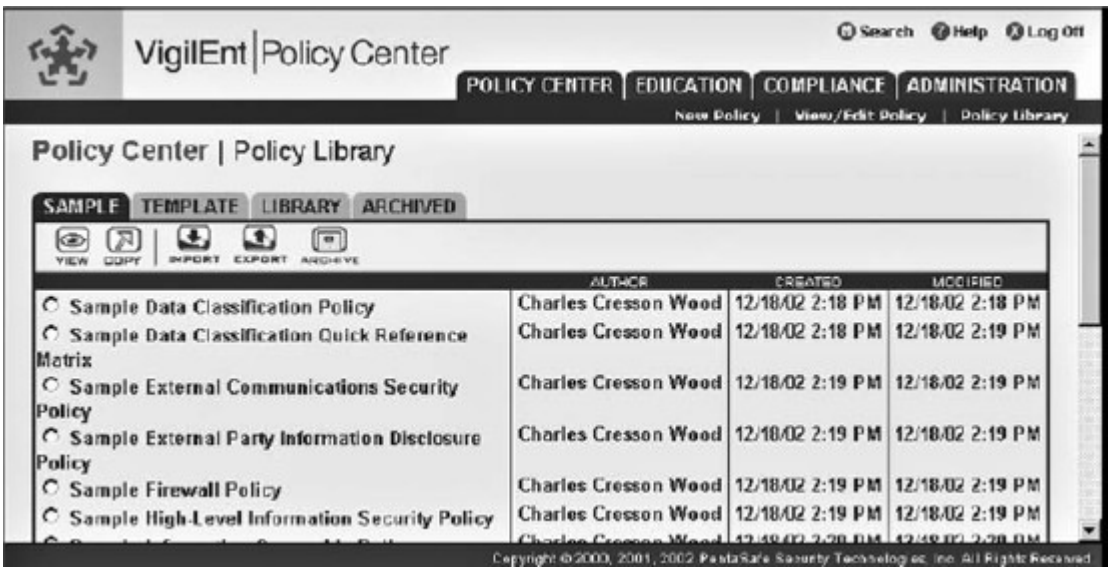
Рис. 3.19. Выбор политики безопасности

VPC поддерживает наибольшее количество каталогов пользователей LDAP, Active Directory, NT Domain или Microsoft Exchange (имеется возможность импорта списка пользователей из тестовых файлов).

VPC позволяет назначать стандартные роли – администратор, пользователь и редактор политики безопасности. Имеется возможность гибко распределять полномочия между пользователями для создания отчетов, управления административными задачами, создания и управления документами. Также можно управлять полномочиями по доступу к политикам безопасности на основе списков доступа.

Для редактирования политик безопасности VPC можно использовать HTML-редактор или редактор Microsoft Word.

Чтобы создать новую политику безопасности, необходимо на закладке Policy Center выбрать «Новая политика», затем выбрать шаблон политики безопасности (см. рис. 3.20) из интересующего раздела и, руководствуясь подсказками, заполнить либо изменить определенные секции шаблона политики безопасности. В VPC имеется уникальная возможность использования при разработке политик безопасности библиотеки политик безопасности ISPME (Information Security Policies Made Easy).



...

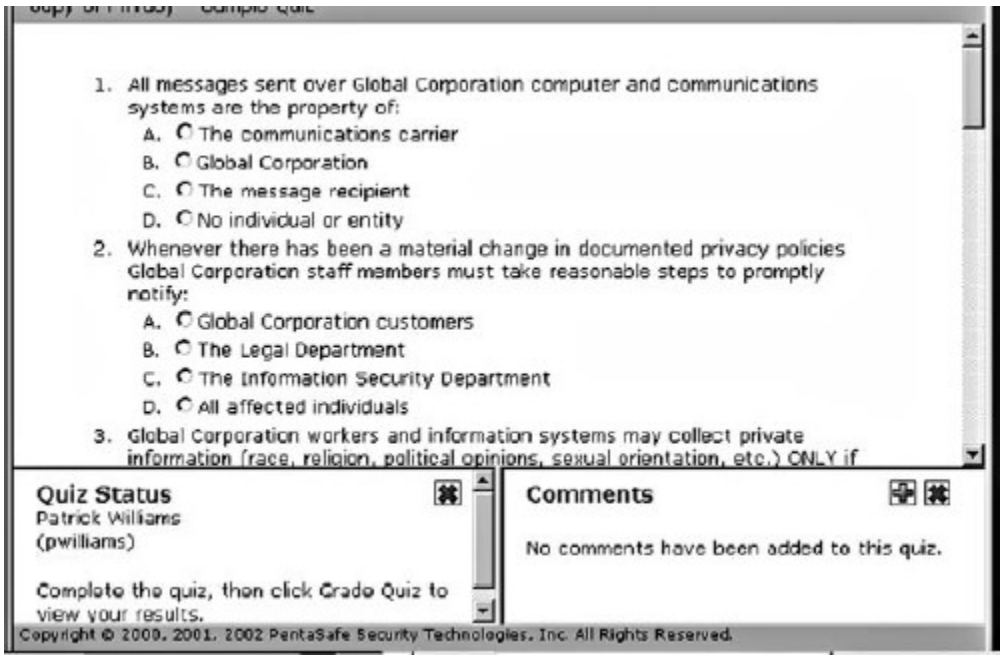
Рис. 3.20. Выбор шаблона политики безопасности

В настоящее время более 4 тыс. организаций по всему миру используют политики безопасности из библиотеки ISPME. Создателем названной библиотеки является признанный эксперт Чарльз Крейсон Вуд (Charles Cresson Wood), обладающий сертификатами CISA, CISSP и автор более 225 технических публикаций и 5 книг по информационной безопасности. Библиотека политик ISPME содержит более 1 300 примеров политик, разработанных на основе международного стандарта ISO 17799 (BS 7799).

Также в библиотеку политик безопасности входят:

- 802.11 Wireless Ethernet Technical Protection Standard,
- Firewall Technical Protection Standard,
- Internet Information Services (IIS) Technical Protection Standard,
- Internet Protocol (IP) Router Technical Protection Standard,
- UNIX Technical Protection Standard,
- Web Server Technical Protection Standard,
- Novell NetWare Technical Protection Standard,
- Windows 2000 Technical Protection Standard,
- Windows NT 4.0 Technical Protection Standard,
- Windows XP Technical Protection Standard.

Дополнительно могут поставляться шаблоны политик безопасности, специфичные только для США (CEBA и HIPAA). Имеется также возможность создавать собственные политики безопасности «с нуля» или импортировать готовые политики безопасности. Примеры тестов, поставляемых вместе с VPC, коррелируют с примерами политик безопасности из библиотеки ISPME (см. рис. 3.21). Вопросы тестов связаны с соответствующими положениями из текста политик безопасности.



...

Рис. 3.21. Пример теста на знание политики безопасности

Тесты позволяют оперативно оценить уровень соответствия корпоративной политики безопасности определведомственному акту или стандарту безопасности. Имеется возможность получить метрические оценки состояния безопасности, а также отслеживать динамику изменения этих оценок.

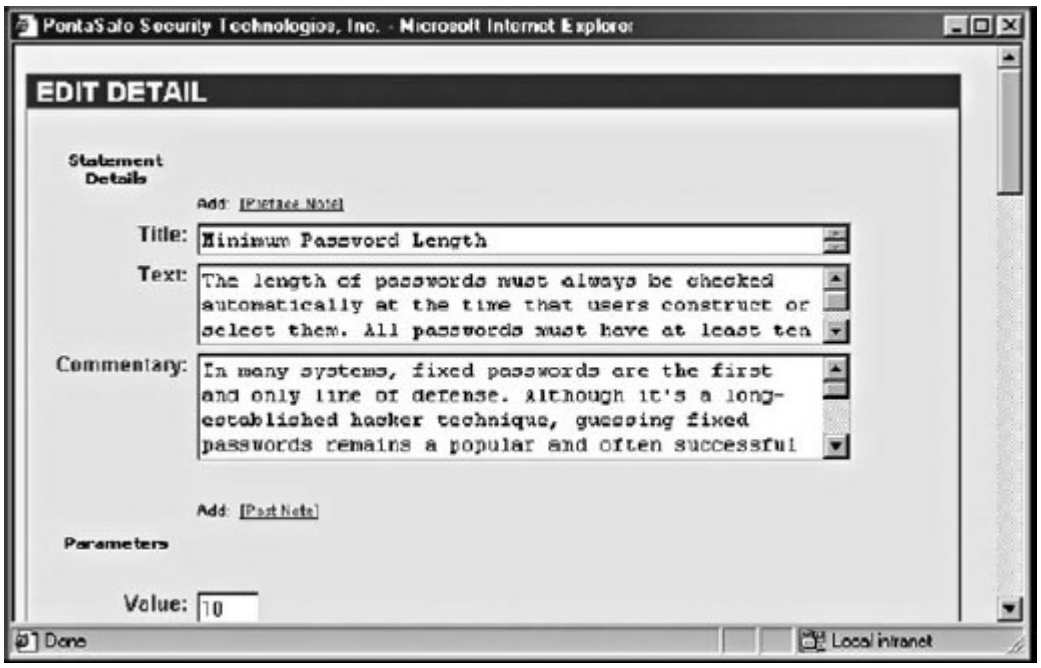
Для фиксации факта ознакомления с политикой безопасности NetlQ, VPC использует ЭЦП. Отчеты, создаваемые VPC, позволяют ознакомиться со списком сотрудников компании, подписавших политику безопасности. Имеется возможность установить различные напоминания для не ознакомленных с нею сотрудников.

Администратор может установить срок действия политики безопасности – после его окончания (по умолчанию 5 лет) сотрудники компании получат уведомление о необходимости пересмотра политики безопасности.

Важной особенностью NetlQ, VigilEnt Policy Center, отличающей его от других продуктов данного класса, является его способность интегрироваться с системами управления техническими политиками, в частности с NetlQ, VigilEnt Security Manager. То есть имеется возможность проводить онлайн-мониторинг и проверку соответствия технической политики и ее текущего состояния на различных технологических платформах существующим политикам более высокого уровня, а также политикам, определяющим требования к параметрам конечных систем. Это помогает существенно экономить время и ресурсы при подготовке отчетов для инспекций контролирующих ведомств, проверке правильности ведения финансовой отчетности, при проведении финансовых аудитов, а также в повседневной работе службы информационной безопасности.

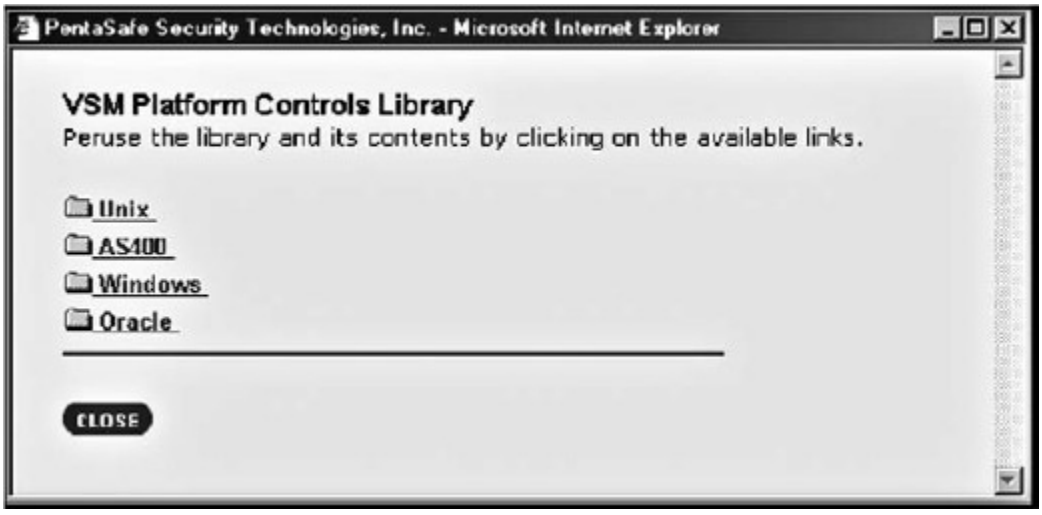
Таким образом, NetlQ VPC позволяет транслировать политики безопасности, созданные на основе шаблонов или примеров политик стандарта ISO 17799, в детальные технические политики для всех основных компонент корпоративной информационной системы, включая серверы приложений, СУБД, продукты контентной фильтрации и межсетевые экраны, работающие на платформах Win2K или Solaris.

Далее представлен пример задания технической политики безопасности (см. рис, 3.22-3.25).



...

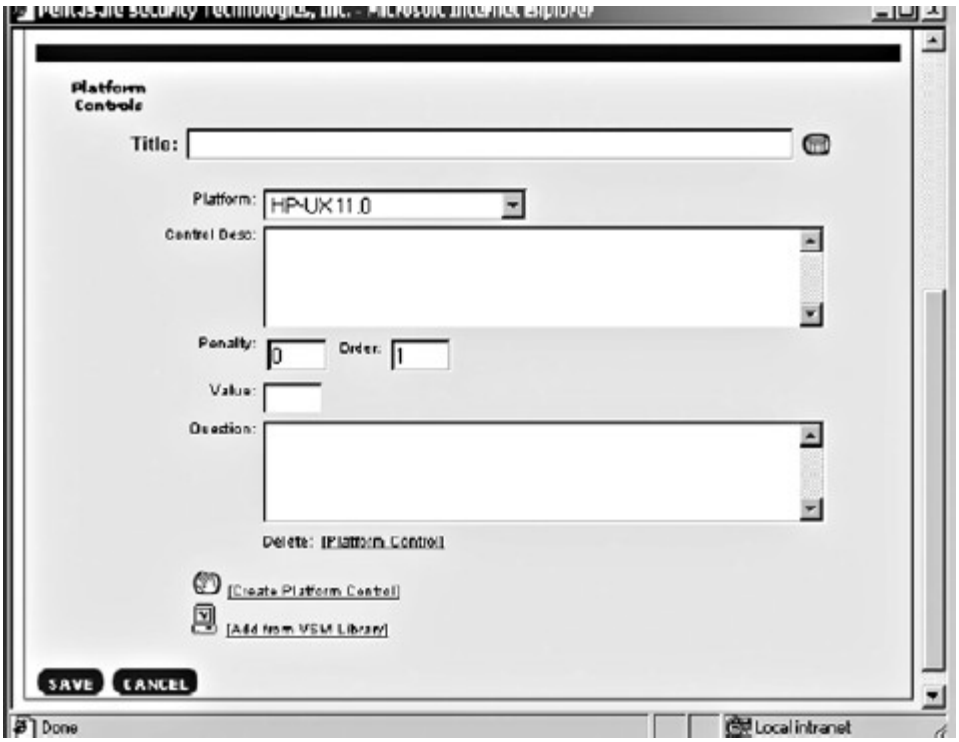
Рис. 3.22. Пример задания правил безопасностис



...

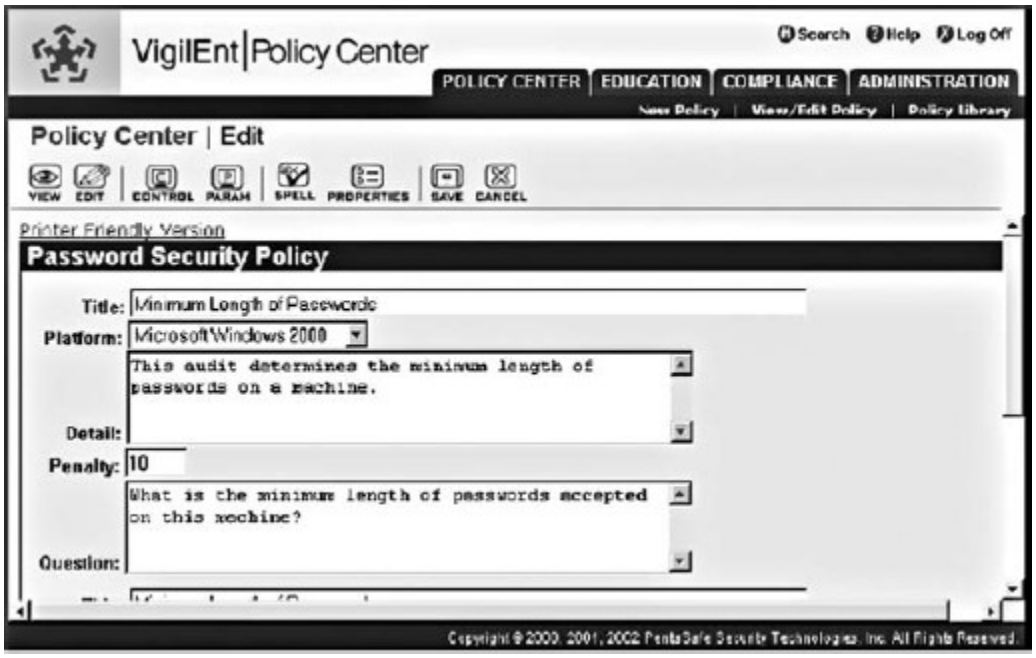
Рис. 3.23. Выбор платформы

Пример выбора параметров, которые может контролировать агент NetlQ, Vulnerability Manager на выбранной платформе, представлен на рис. 3.24.



...

Рис. 3.24. Детализация характеристик платформы



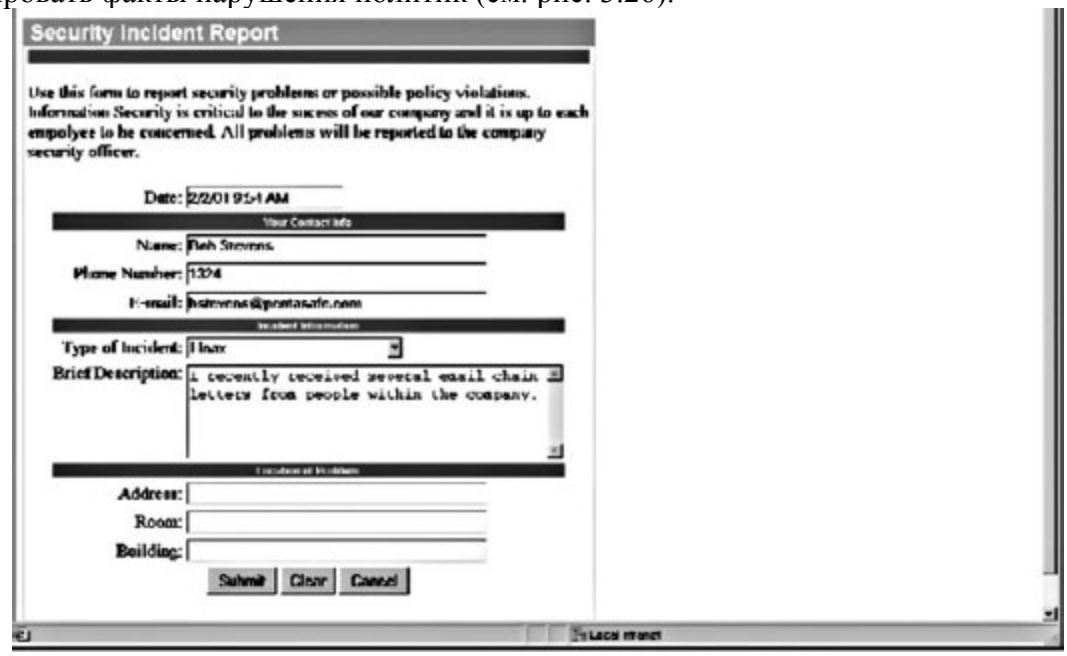
...

Рис. 3.25. Пример задания политики безопасности

В состав линейки NetIQ, входит также Security Manager, который позволяет централизованно собирать, сохранять, очищать, агрегировать, коррелировать и в удобной для анализа форме отображать события от таких систем, как Cisco IOS, Check Point FW-1,

ISS RealSecure и TrendMicro InterScanVirusWall. Другой компонент, VigilEnt User Manager (VUM), автоматизирует процесс управления пользователями – управление учетными записями и паролями, включая самообслуживание пользователей по управлению своими паролями через Web-портал.

VigilEnt Policy Center позволяет не только проверять факт прочтения и понимания политик, но также предоставляет сотрудникам возможность легко регистрировать и документировать факты нарушения политик (см. рис. 3.26).



...

Рис. 3.26. Пример регистрации инцидента безопасности

3.8. Отечественная специфика разработки политик безопасности

Новое поколение стандартов в области защиты информации отличается как от предыдущего, так и от руководящих документов Гостехкомиссии России 1992–1998 годов большей формализацией политик безопасности и более детальным комплексным учетом качественно и количественно проверяемых и управляемых показателей информационной безопасности компании. Комплексный учет показателей предполагает комплексный же подход к разработке политик безопасности, когда на соответствие определенным правилам безопасности проверяется не только программно-техническая составляющая защиты информации компании, но и организационно-административные меры по ее обеспечению. Вместе с тем необходимо учитывать перспективы и тенденции развития стандартов безопасности (см. рис. 3.27).

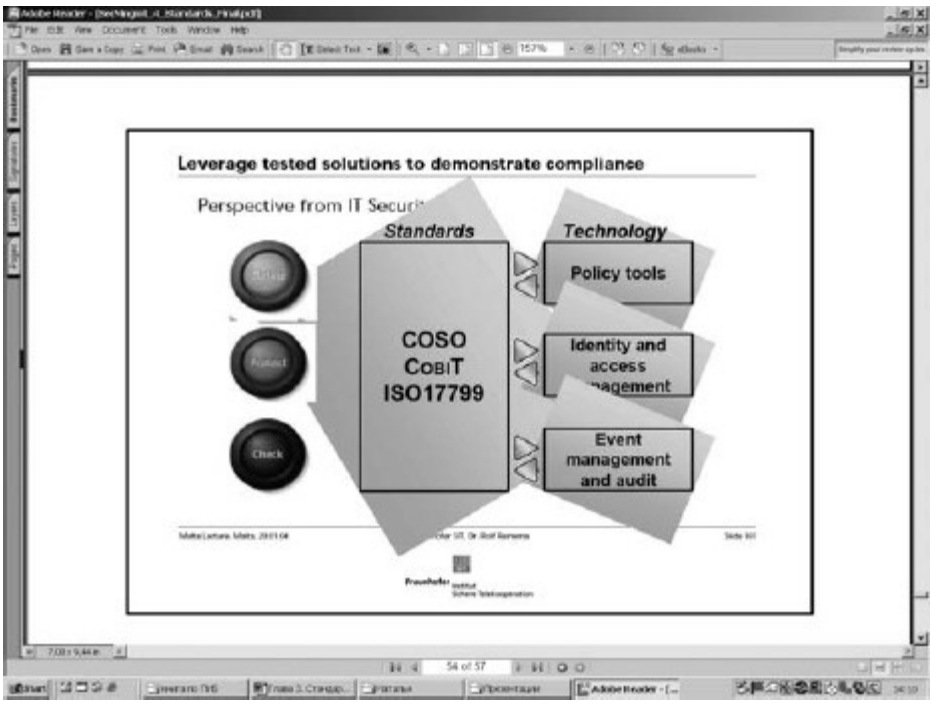


Рис. 3.27. Перспективы и тенденции развития стандартов безопасности В противоположность германскому стандарту BSI, предоставляющему возможность использовать конкретные «частные» политики безопасности, стандарты ISO 15408, ISO 17799 и CobiT позволяют рассмотреть только наиболее общие политики информационной безопасности, характерные для процессов защиты информации в целом. При этом все названные подходы обладают определенными ограничениями. Ограничением германского стандарта BSI является невозможность распространить рекомендации этого стандарта на политики безопасности в российских компаниях, инфраструктура которых отличается от ранее рассмотренных примеров корпоративных систем защиты информации и соответствующих политик безопасности. Ограничением стандартов ISO 17799 и CobiT является трудность перехода от общих политик безопасности к частным политикам информационной безопасности в российских компаниях. Основная причина этого заключается в том, что требуемые политики безопасности любой российской компании дополнительно характеризуются определенными индивидуальными специфическими условиями бизнес-деятельности, в частности ограничениями и регулированием российской нормативной базы в области защиты информации. Так, в России нормативную базу в области защиты информации в автоматизированных системах (АС) составляют нормативно-правовые документы (федеральные законы, указы Президента, постановления Правительства) и нормативно-технические документы (государственные стандарты, руководящие документы Гостехкомиссии (ФСТЭК) России, отраслевые и ведомственные стандарты). В Приложении 7 приведены основные документы, регулирующие вопросы защиты информации на территории РФ. Также надо учитывать, что после принятия и вступления в силу Федерального закона «О техническом регулировании», а также ГОСТ Р ИСО/МЭК 15408 статус ряда нормативных документов (государственных стандартов, отраслевых стандартов, стандартов организаций и др.) изменился. При этом государственные стандарты Российской Федерации из основного инструмента технического регулирования трансформировались в российские национальные стандарты, требования которых стали носить добровольный характер. Обязательные требования стали устанавливаться в технических регламентах.

Другими словами, только совместно используя сильные стороны рассмотренных международных стандартов, а также адаптировав полученные рекомендации в соответствии с требованиями российской нормативной базы в области защиты информации, можно

эффективно разработать и внедрить политики безопасности в конкретных отечественных организациях и на предприятиях. И первые положительные примеры не заставили себя долго ждать. Так, например, Банком России с целью повышения уровня информационной безопасности как самого банка, так и организаций банковской системы Российской Федерации в соответствии с Федеральным законом № 184-ФЗ «О техническом регулировании» Распоряжением от 18 ноября 2004 года № Р-609 с 1 декабря 2004 года введен в действие стандарт «Обеспечение информационной безопасности организаций банковской системы Российской Федерации. Общие положения» (далее – «стандарт»).

Стандарт был разработан коллективом, в который вошли представители Банка России, Ассоциации российских банков, Ассоциации региональных банков, Национальной валютной ассоциации, Института банковского дела Ассоциации российских банков, Акционерного коммерческого Сберегательного банка Российской Федерации, Альфа-банка, Россельхозбанка, банка «Петрокоммерц», банка «Российский кредит», Московской межбанковской валютной биржи, НПФ «Кристалл», Государственного научно-исследовательского института проблем защиты информации Федеральной службы по техническому и экспортному контролю, аудиторской компании KPMG.

Основные цели и задачи разработки стандарта заключались в следующем:

• повышение доверия к банковской системе Российской Федерации;

• повышение стабильности функционирования организаций банковской системы Российской Федерации и на этой основе – стабильности функционирования банковской системы России в целом;

• достижение адекватности мер по устранению реальных угроз информационной безопасности;

• предотвращение и/или снижение ущерба от инцидентов информационной безопасности;

• установление единых требований по обеспечению информационной безопасности для организаций банковской системы Российской Федерации;

• повышение эффективности мероприятий по обеспечению и поддержанию информационной безопасности организаций банковской системы Российской Федерации.

По мнению экспертов, стандарт содержит наиболее важные рекомендации по разработке основополагающих документов по проблеме информационной безопасности, необходимые требования по безопасности информационных и телекоммуникационных технологий. При этом в соответствии с Федеральным законом № 184-ФЗ «О техническом регулировании» стандарт отнесен к категории «стандарт организации», и его положения не носят обязательного характера и рекомендованы к применению кредитными организациями на добровольной основе. Стандарт является открытым документом, предполагающим его регулярную корректировку в соответствии с динамикой изменения угроз информационной безопасности. Новую (уточненную) редакцию стандарта предполагается подготовить к концу 2005 года. Работы по дальнейшему сопровождению и доработке стандарта ведутся специально созданным Подкомитетом 3 «Защита информации в кредитно-финансовой сфере» Технического комитета 362 «Защита информации» Федерального агентства по техническому регулированию и метрологии [12] .

Глава 4 РЕАЛИЗАЦИЯ ПОЛИТИК БЕЗОПАСНОСТИ

В предыдущих главах мы с вами рассмотрели основные понятия и определения политик безопасности. Познакомились с опытом разработки политик безопасности и различными подходами ведущих компаний-производителей в отрасли информационных технологий и информационной безопасности. Подробно рассмотрели этапы жизненного цикла разработки политик безопасности компании. Как реализовать разработанные политики безопасности компании на практике? Как правильно задать правила безопасности? Как настроить аппаратно-программные средства защиты информации? Постараемся

ответить на эти вопросы.

4.1. Задание общих правил безопасности

Пусть объектом защиты является информационная система компании ЗАО «XXI век» (далее – «компания»). Название объекта защиты вымышленное, возможные совпадения случайны и носят непреднамеренный характер.

Состав и структура политик безопасности. Общая политика безопасности компании разработана и утверждена руководством организации. В этой политике определены принципы, порядок и правила предоставления доступа к информационным ресурсам компании, а также степень ответственности в случае нарушения правил безопасности. Также существует ряд других политик безопасности, в частности политика допустимого использования, определяющая доступ к сервисам. При приеме на работу каждый новый сотрудник должен подписать соглашение о том, что с политиками безопасности компании ознакомлен и обязуется их выполнять. Партнеры, поставщики и клиенты банка при получении доступа к конфиденциальной информации компании подписывают Соглашение о неразглашении конфиденциальной информации. Политики безопасности компании регулярно пересматриваются (не реже одного раза в год).

Характеристика инфраструктуры компании. Взаимодействие с партнерами, клиентами и поставщиками осуществляется с использованием сервисов Интернета. Для этих целей разработан ряд Web-приложений. Архитектура приложений использует три уровня для реализации разделения ресурсов:

уровень представления – выполняется на Microsoft IIS 5.0 на Microsoft Windows 2000 Server Service Pack 4 со всеми необходимыми обновлениями. Вся бизнес-логика выполняется на серверах второго уровня архитектуры;

• *промежуточный уровень* – содержит все бизнес-компоненты и также выполняется на Microsoft Windows 2000 Server Service Pack 4. К этому уровню нет доступа из Интернета. Страницы Active Server Pages на серверах уровня представления активируют компоненты COM+ и позволяют выполнить бизнес-логику. Компоненты запускаются под непривилегированной учетной записью с необходимым минимумом привилегий;

• *уровень баз данных* – состоит из базы данных и защищенного хранилища данных. Microsoft SQL Server 2000 Service Pack 3 используется как сервер управления базой данных и выполняется на двухузловом кластере Microsoft Windows 2000 Advanced Server Service Pack 4 Cluster для обеспечения отказоустойчивости. Только серверы промежуточного уровня имеют доступ к этим серверам. Серверы расположены в изолированном сегменте сети, разделенном межсетевыми экранами.

Правила использования сервисов Интернета. Согласно принятой в компании политики безопасности для сотрудников определены следующие правила использования сервисов Интернета: • разрешается исходящий Web-трафик – HTTP, SSL и FTP для различных групп сотрудников. Доступ в Интернет контролируется и регистрируется, доступ к некоторым категориям Web-ресурсоВ блокируется в соответствии с политикой использования ресурсов Интернета;

• запрещается применять средства обмена мгновенными сообщениями (например, ICQ) и одноранговые файлообменные системы (например, Napster). Также запрещено получать и отправлять электронную почту с использованием внешних почтовых серверов, не принадлежащих компании (например, www.mail.ruV.

• разрешается использование внешних DNS-имен, разрешение на использование дополнительных сервисов зависит от политики использования ресурсов Интернета.

Правила доступа в сеть компании. Для сотрудников, работающих вне офиса компании, определяются следующие правила доступа в сеть компании: • доступ к внутреннему почтовому серверу Outlook Web Access осуществляется через HTTPS. Обмен файлами реализуется с использованием Microsoft SharePoint Portal Server 2003 через HTTP/HTTPS.

Это позволяет не настраивать межсетевой экран для трафика SMB/CISF, что упрощает конфигурацию межсетевого экрана;

• доступ администраторов организуется через VPN к сегменту управления, для удаленного администрирования серверов используется Microsoft Terminal Services.

Правила обеспечения физической безопасности. Для должного обеспечения физической безопасности все оборудование компании расположено в защищенных помещениях с резервными источниками питания, оборудованных системами пожаротушения и кондиционерами. Доступ в помещения осуществляется с использованием биометрической системы контроля доступа сотрудников. Действует правило обязательного сопровождения гостей компании во время деловых визитов. Над каждым рядом стоек находится видеокамера с датчиком движения, ведется запись всех действий сотрудников и приглашенных лиц компании.

4.2. Архитектура корпоративной системы защиты информации

Основной задачей при создании защищенной инфраструктуры компании (см. рис. 4.1) является реализация надежного контроля доступа на уровне приложений и сети в целом. При этом логический контроль доступа на уровне сети осуществляется путем сегментации сетей и разграничения трафика с помощью межсетевых экранов. Созданы две раздельные подсети – одна для доступа извне к Web-приложениям и вторая для доступа сотрудников в Интернет. Этим обеспечивается полное разделение входящего из Интернета и исходящего в Интернет трафика. Многоуровневый подход с несколькими межсетевыми экранами обеспечивает фильтрацию всего нежелательного трафика.

В компании было создано несколько зон безопасности:

• *зона подключения к Интернету* – эта зона представляет собой подсеть между пограничным маршрутизатором и внешними межсетевыми экранами. Пограничные маршрутизаторы используют списки контроля доступа (ACL), сконфигурированные для фильтрации входящего и исходящего трафика и защиты внешних межсетевых экранов;

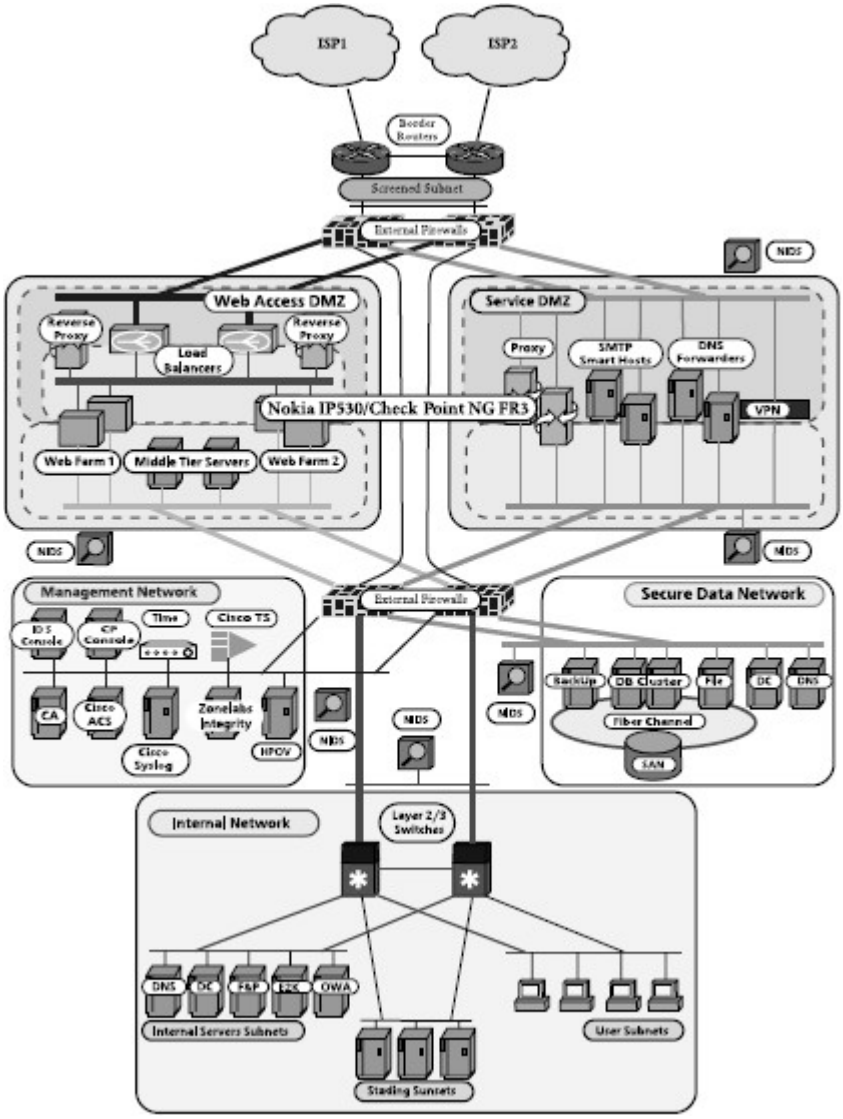
• *зона доступа к Web-приложениям компании (Web Access DMZ)* – в этой подсети находятся Web-приложения компании и разрешены только входящие через межсетевой экран запросы из Интернета. Доступ из внутренней сети запрещен;

• *зона выхода в Интернет (Service DMZ)* – эта зона представляет собой подсеть, с помощью которой сотрудникам компании предоставляется доступ в Интернет. Разрешен только исходящий через межсетевой экран трафик, за исключением доступа к электронной почте с помощью VPN;

• *зона управления ресурсами сети компании (Management Network)* – в этой зоне находятся приложения для мониторинга, аутентификации и журналирования событий в сети компании;

• *зона защищаемых данных компании (Secure Data Network)* – эта зона содержит все важные для компании Web-приложения, базы данных и базу данных пользователей (Active Directory);

• *зона внутренней сети компании (Internal Network)* – зона содержит серверы, рабочие станции сотрудников и приложения интранета.



...

Рис. 4.1. Архитектура корпоративной системы защиты информации

При этом компания использует следующие диапазоны IP-адресов: 70.70.70.0/24 и 90.90.1.0/30 (в действительности сети 70.x.x. x и 90.90.1.0/30 зарезервированы IANA, но мы будем считать, что они реально существуют). Сеть 70.70.70.0/24 разбита на подсети с использованием различных масок подсетей, задействована только первая часть – 70.70.70.0/25, все остальные адреса зарезервированы для последующего расширения сети. Для внутренней сети используется подсеть 172.16.0.0/16. Общее распределение адресного пространства подсетей компании представлено в табл. 4.1:

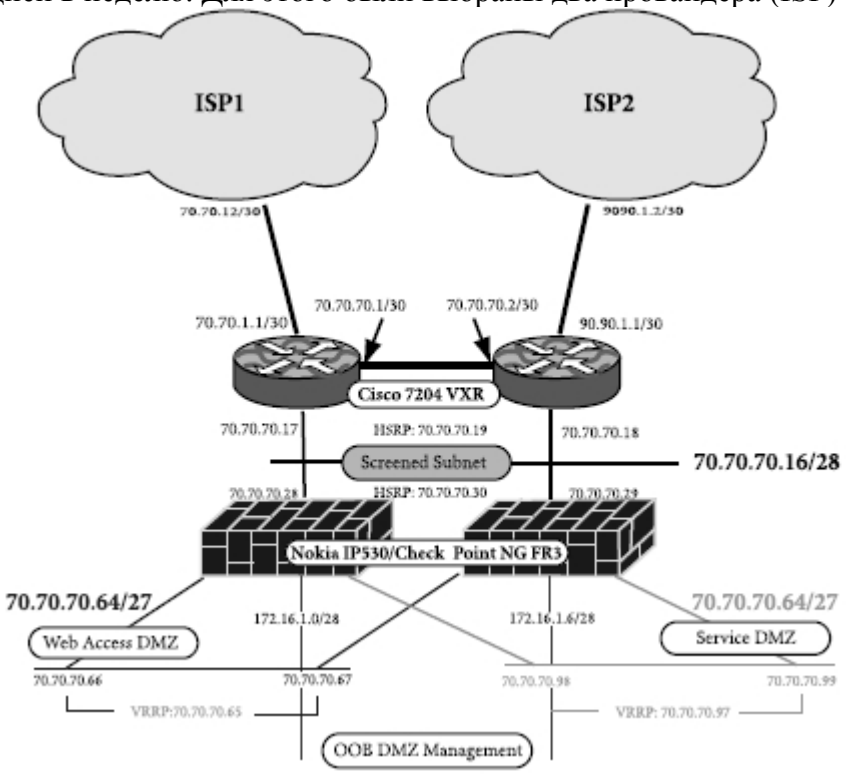
Теперь рассмотрим каждую из перечисленных зон безопасности компании подробно и определим правила безопасности.

Таблица 4.1. Распределение адресного пространства

Сеть	Подсеть
Соединение с ISP1	70.70.1.0/30
Соединение с ISP2	90.90.1.0/30
Подсеть между пограничными маршрутизаторами и внешними межсетевыми экранами	70.70.70.16/28
Сеть между пограничными маршрутизаторами	70.70.1.0/30
Сеть управления устройствами в демилитаризованной зоне	172.16.1.0/28
Сеть между внешними межсетевыми экранами	172.16.1.16/29
Внешние адреса Web-приложений	70.70.70.64/27
Внутренние адреса Web-приложений (NAT)	172.16.2.0/24
Внутренние адреса Web-приложений	172.16.3.0/24
Внешние адреса зоны Service DMZ	70.70.70.96/27
Внутренние адреса зоны Service DMZ	172.16.4.0/24
Сеть данных	172.16.5.0/24
Сеть управления	172.16.6.0/24
Внутренняя магистраль	172.16.9.0/28
Внутренние серверы	172.16.16.0/21
Внутренние серверы тестирования	172.16.24.0/21
Внутренние пользовательские компьютеры	172.16.32.0/20

4.2.1. Зона подключения к Интернету

Одно из главных бизнес-требований компании – обеспечение доступности Интернета 24 часа в сутки 7 дней в неделю. Для этого были выбраны два провайдера (ISP) (см. рис. 4.2).



...

Рис. 4.2. Схема подключения к Интернету

С целью надлежащего распределения маршрутизации и избыточности был сконфигурирован BGP v.4 между пограничными маршрутизаторами и маршрутизаторами провайдеров Интернета. В качестве пограничных маршрутизаторов используется Cisco 7204

VXR Router с Cisco IOS Release 12.3. Преимуществом этой модели является поддержка Cisco Express Forwarding (CEF), что существенно увеличивает производительность маршрутизаторов.

Пограничные маршрутизаторы – это первая линия обороны. Так как они являются первой точкой входа в сеть, то на них настроены списки контроля доступа (ACL) для фильтрации нежелательного трафика, что уменьшает нагрузку на остальную сетевую инфраструктуру. Реализована фильтрация как входящего, так и исходящего трафика. Для защиты от атак SYN Flood используется возможность Cisco IOS TCP Intercept. Другая задача, которую решают пограничные маршрутизаторы, – защита внешних межсетевых экранов от трафика, направленного на IP-адреса межсетевых экранов. Адресное пространство 70.70.70.16/28 используется для подсети между пограничными маршрутизаторами и внешними межсетевыми экранами. Подсети 70.70.70.4/30 и 70.70.70.8/29 зарезервированы для будущего решения с балансировкой нагрузки между межсетевыми экранами. «Горячее» резервирование на внутренних интерфейсах маршрутизаторов обеспечивает протокол HSRP (Hot Standby Routing Protocol). Для соединения устройств в DMZ используются коммутаторы Cisco Catalyst 3550. Коммутаторы не имеют IP-адресов и управляются посредством консольного доступа через Cisco 2620 Terminal Server.

Внешние межсетевые экраны. В качестве внешних межсетевых экранов используются Nokia IPSO v.3.6 FCS4, Check Point FW-1 NG FP3. К основным факторам, повлиявшим на выбор данных устройств, относятся:

• высокая надежность, защищенность и производительность аппаратных платформ Nokia;

• развитая функциональность и технологическая зрелость межсетевого экрана Check Point FW-1 NG FP3;

• наличие в компании подготовленных специалистов.

Как было сказано выше, в компании существуют две DMZ-зоны, одна для доступа к Web-приложениям и другая для выхода в Интернет, каждая из зон защищена межсетевыми экранами. Это было сделано для разделения ресурсов, чтобы проникновение злоумышленников в одну из зон не сказалось на работе другой зоны. Каждый межсетевой экран имеет 5 интерфейсов, подключенных к разным зонам. Межсетевые экраны также имеют выделенный интерфейс для управления Out-of-band посредством сервера Check Point Management Console из зоны управления. Это повышает защищенность управляющего трафика и делает недоступным изменение наблюдаемого трафика, так как он не проходит через общую сеть.

Система межсетевых экранов реализована в варианте с полной избыточностью и масштабируемостью. Это достигается путем использования Nokia IPSO VRRP и возможностью синхронизации соединений Firewall-1. Через межсетевые экраны разрешен ограниченный набор трафика согласно принятой в компании политики безопасности. На этом же уровне реализована и защита от атак SYN Flood.

4.2.2. Зона доступа к Web-приложениям компании

Эта зона защищена на уровне представления, промежуточном уровне, а также на уровне баз данных компании. Серверы названной зоны защищены в соответствии с рекомендациями руководств SANS (www.sans.org): Level-1 Benchmark for Windows 2000, Level-2 Windows 2000 Professional Operating System Benchmark, Level-2 Windows 2000 Server Operating System Benchmark, а также в соответствии с официальными руководствами компании Microsoft (www.microsoft.com): Security Operations Guide for Windows 2000, Hardening Guide for Windows 2000.

Для централизованного управления обновлениями используется продукт Microsoft SMS 2003. На Web-сереерах выполняется Microsoft IIS 5.0. Серверы имеют по два сетевых интерфейса. Через один интерфейс поступают запросы из Интернета, через другой осуществляются запросы к базе данных. Таким образом реализуется изоляция Web-приложений от базы данных.

4.2.3. Зона выхода в Интернет

Эта зона безопасности обеспечивает доступ в Интернет из внутренней сети. Здесь также используется концепция разделения сети. Каждое устройство имеет два интерфейса – один для подключения к публичной зоне и другой для доступа к внутренней зоне с отключенной маршрутизацией пакетов между ними. Все оборудование дублируется для обеспечения высокой степени доступности. DNS Forwarder установлен на Windows 2000 Service Pack 4, Microsoft DNS Service на аппаратной платформе Compaq Proliant DL360. SMTP Smart Host установлен на OpenBSD 3.2 with Sendmail v.8.12.6 на аппаратной платформе Compaq Proliant DL360.

Для реализации политики использования Интернета развернут продукт Websense. Он предназначен для ограничения доступа к определенным Web-ресурсам, запрещенным политикой использования Интернета, например к Web-почте, чатам, сайтам с непристойным содержанием, блокирует службы мгновенного обмена сообщениями и одноранговые файлообменные сети. Websense также обеспечивает определение и удаление ActiveX и Java applets, позволяет создавать отчеты об использовании ресурсов Интернета конкретными сотрудниками. Для обнаружения вирусов в трафике HTTP, SMTP и FTP используется продукт Trend Micro InterScan Virus Wall.

SMTP-серверы. SMTP-серверы работают на OpenBSD 3.2 с Sendmail v.8.12.6. Это один из немногих случаев, когда используется продукт, не произведенный Microsoft. Выбор обусловлен тем, что Microsoft Exchange 2000 Server обладает избыточными для компании функциональными возможностями, которые не нужно делать доступными из Интернета. Также, по сравнению с Sendmail, Microsoft Exchange характеризуется достаточно слабым уровнем защиты. По этим причинам и был сделан выбор в пользу Sendmail на платформе OpenBSD, которая является одной из самых защищенных операционных систем. OpenBSD и Sendmail бесплатны, что ведет к уменьшению расходов на построение системы. OpenBSD и Sendmail были защищены в соответствии с рекомендациями производителей. Установлен минимально необходимый набор пакетов, включены только необходимые сервисы и установлены все существующие обновления и сервисные пакеты. На SMTP-сервере также установлено программное обеспечение для защиты от спама. Все входящие сообщения перенаправляются на внутренний сервер Microsoft Exchange, функционирующий в режиме кластера. Принимаются и направляются вне сети только сообщения, которые были получены от этого внутреннего сервера. Во всех исходящих сообщениях изменяется заголовок для удаления информации о внутренней маршрутизации и изменяется SMTP-приглашение, чтобы затруднить злоумышленникам получение информации о версии программного обеспечения внешнего SMTP-сервера. Для предупреждения возможности просмотра списка почтовых ящиков и сервисов отключены команды VRFY и EXPN.

DNS. В качестве концепции построения DNS было выбрано решение по разделению на внутренний и внешний DNS. Внешний DNS-сервер обслуживается интернет-провайдерами и находится в их зоне ответственности. Эта опция обеспечивает дополнительную безопасность, связанную с проблемами администрирования, и уменьшает необходимость разрешения входящего DNS-трафика, так как исторически DNS-серверы являются одним из наиболее слабо защищенных сервисов и постоянной мишенью для атак злоумышленников. Этот дизайн также обеспечивает избыточность и улучшает доступность сервисов, потому что вероятность, того что DNS-серверы обоих провайдеров одновременно подвергнутся атаке и не смогут обслуживать запросы, достаточно мала.

DNS-сервер, расположенный в DMZ, работает с использованием службы Microsoft DNS и установлен на операционную платформу Microsoft Windows 2000 Service Pack 4. Серверы сконфигурированы как «только кэширующие», без установленных DNS-зон и перенаправляют все запросы на DNS-серверы провайдера. С провайдерами подписаны специальные соглашения по защите этого сервиса. Процесс разрешения имен, таким образом, становится более защищенным, так как используются строго определенные внешние серверы.

VPN. Для обеспечения доступа к корпоративной сети работающим удаленно сотрудникам и персоналу, ответственному за управление сетевыми устройствами, используется концентратор Cisco VPN 3030. Доступ по коммутируемым соединениям запрещен. Так как сервис VPN не является критичным для обеспечения бизнес-процессов, то применяется только одно устройство. При изменении этих требований может быть установлено дополнительное устройство для обеспечения избыточности. Доступ с использованием VPN построен на следующих принципах:

• каждый сотрудник, использующий этот сервис, подписывает политику использования VPN;

• разрешен к применению только протокол IPSec с шифрованием 3DES. PPTP и L2TP не поддерживаются;

• для аутентификации на этапе 1 (IKE) используются сертификаты;

• сертификаты выпускаются и распределяются внутренним Центром управления сертификатами;

• сертификаты хранятся на аппаратном токене Aladdin Software eToken. Выдаются каждому сотруднику компании, использующему этот сервис, отделом информационной безопасности. eToken является небольшим, простым в применени USB-устройством, где доступ к сертификату защищен паролем. После создания ключи сертификатов не могут быть экспортированы из устройства;

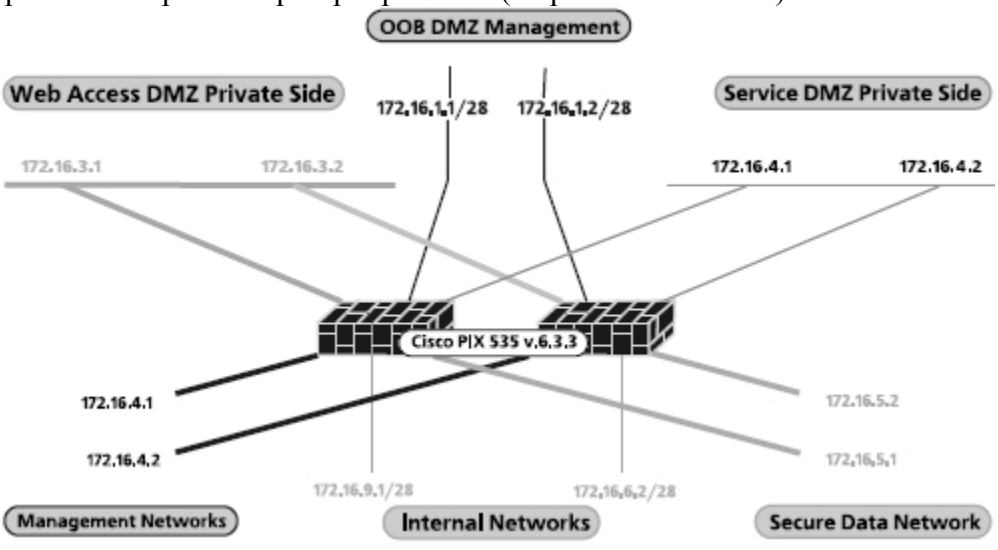
• каждый сотрудник имеет персональный идентификатор и пароль для этого сервиса. Аутентификация и управление идентификаторами осуществляются с использованием Cisco ACS RADIUS;

• Cisco ACS RADIUS также обеспечивает выдачу IP-адресов и применение списков контроля доступа для подключающихся сотрудников компании;

• Zone Labs Integrity Server применяет политику на персональном межсетевом экране и антивирусном программном обеспечении на каждом подключаемом через VPN компьютере. Эта политика определяется отделом информационной безопасности и принудительно применяется при подключении;

• журналирование VPN-сессий осуществляется на сервере Cisco Security Information Management Solution v.3.1.1 (NetForensics) с использованием syslog.

Внутренние межсетевые экраны. Наличие внутренних межсетевых экранов обеспечивает больший контроль и безопасность информационных потоков между внутренними сетями. Кроме того, достигается изоляция сегмента управления от остальной сети, управление доступом через VPN, защита внутренней сети путем запрещения трафика из менее защищенных зон сети и пр. Каждый межсетевой экран имеет шесть интерфейсов, подключенных к разным зонам (см. рис. 4.3), также существует выделенный интерфейс для поддержания режима «горячего» резервирования (на рис. не показано).



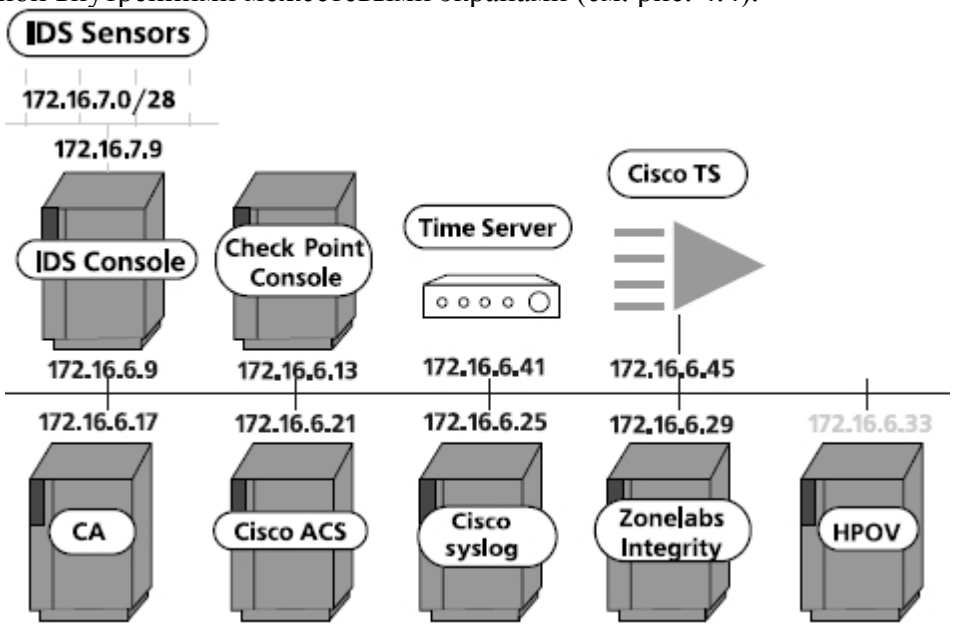
...

Рис. 4.3. Реализация шлюза между внутренней и внешней сетями

Система построена на двух межсетевых экранах Cisco PIX 535, функционирующих в режиме «горячего» резервирования. Выбор продукта был обусловлен его высокой производительностью, надежностью и приемлемой для компании стоимостью решения. Кроме того, использование межсетевых экранов разных производителей увеличивает общую защищенность сети компании, так как, при возникновении уязвимости в Check Point FW-1, эта уязвимость вряд ли может быть использована против Cisco PIX, и наоборот.

4.2.4. Зона управления ресурсами сети компании

Все серверы управления сетью и серверы мониторинга расположены на выделенной сети, защищенной внутренними межсетевыми экранами (см. рис. 4.4).



...

Рис. 4.4. Центр управления сетью

В компании организован центр управления сетью для мониторинга и управления сетевыми устройствами. Центр находится в защищенном от проникновения посторонних лиц помещении. График работы персонала 16 часов в сутки 5 дней в неделю. Поддержка в ночное время реализуется через VPN-соединения. Сотрудник должен сначала зайти на один из компьютеров данной сети и только потом, с этого компьютера, он может получить доступ к сетевому оборудованию. Это является дополнительным уровнем защиты. Кроме того, доступ к любому сетевому оборудованию ограничен списком IP-адресов сети управления. Пограничные маршрутизаторы и все коммутаторы управляются через консоль с использованием маршрутизатора доступа Cisco 2620, остальные управляющие интерфейсы на устройствах отключены. Другие устройства – SMTP-серверы, VPN-концентратор – управляются с помощью SSH. Серверы с операционной системой Windows 2000 работают под управлением Microsoft Terminal Services, который поднят на внутренних интерфейсах серверов и сконфигурирован для использования максимального уровня шифрования. Помимо этого фильтры IPSec настроены таким образом, чтобы разрешать доступ к серверам с использованием Terminal Services (TCP 3389), если соединение инициируется из сети

управления.

Консоль управления IDS. В качестве сетевой системы обнаружения вторжений используется Cisco IDS 4250, а на серверах установлены системы предупреждения вторжений Cisco Security Agent v.4.0 (продукция компании Okena, продаваемая под торговой маркой Cisco). В системе Cisco IDS 4250 один интерфейс работает в режиме сниффера и не имеет IP-адреса, а другой используется для получения сообщений о найденных сигнатурах и для управления. Передача сообщений осуществляется по протоколу SSL. В качестве устройства управления выбран Cisco Works VPN/Security Management Solution v.2.2. Данное программное обеспечение позволяет управлять конфигурациями следующих устройств:

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

В состав продукта входят следующие функциональные модули: • Cisco Works Common Services,

• Management Center for Firewalls,
• Management Center for IDS Sensors,
• Management Center for Cisco Security Agents,
• Management Center for VPN Routers,
• Monitoring Center for Security,
• Monitoring Center for Performance,
• Cisco View,
• Auto Update Server,
• Resource Manager Essentials.

Monitoring Center for Security позволяет принимать и коррелировать сообщения со всех вышеперечисленных устройств, а кроме того, он оснащен средствами мониторинга производительности и инвентаризации сети. Доступ к этому устройству из сети, отличной от сети управления, запрещен. *Сервер Check Point Management Console.* Сервер Check Point Management Console используется для управления модулями Check Point Firewall-1 и журналирования событий. Доступ к нему ограничен IP-адресами интерфейсов администрирования Nokia Check Point FW-1.

Сервер времени. Синхронизация сетевого времени – очень важный аспект правильного функционирования сети и надлежащего журналирования. Если на нескольких устройствах установлено разное время, то при анализе журналов очень трудно будет разбираться, когда реально и в какой последовательности произошли события, к тому же каждый из сертификатов имеет определенный срок жизни и, при неправильно установленном времени, его будет невозможно эксплуатировать. Нередко слабости в защите протокола NTP или неправильные настройки сетевых устройств дают злоумышленникам возможность проведения атак с целью установки неверного времени и, таким образом, выведения из строя всех устройств и соединений, использующих сертификаты. Кроме того, Microsoft Active Directory для аутентификации применяет протокол Kerberos, который очень сильно зависит от точных настроек времени. Из-за важности обеспечения точного времени был приобретен аппаратный сервер времени Datum TymServe TS2100 с GPS-антенной для синхронизации с сервером времени NIST (Национальный институт стандартов США). Это устройство служит мастер-сервером для всех устройств в сети. К нему разрешен только NTP-трафик и используется NTP-аутентификация везде, где это возможно. На случай отказа сервера компания заключила соглашение с владельцами одного из NTP-серверов в Интернете о получении точного времени. В случае возникновения такой ситуации будут внесены соответствующие изменения в списки доступа на межсетевых экранах.

Cisco Terminal Server. Для управления всеми сетевыми устройствами (маршрутизаторами, коммутаторами) с помощью консольного соединения используется Cisco Router 2620. На всех устройствах отключены все протоколы сетевого управления.

Соединения к самому Cisco Router 2620 ограничены списком IP-адресов из сети управления и определенным списком инженеров, подключающихся через VPN-соединение. Разрешен доступ только по SSH, и все сотрудники должны быть аутентифицированы с использованием TACACS+. Уровень доступа регулируется членством в группах и настройками на сервере TACACS+.

Cisco Security Information Management Solution. Cisco Security Information Management Solution v.3.1 (продукт компании Netforensics) на аппаратной платформе Cisco 1160 используется для сбора, коррелирования, анализа и хранения журналов. Данное программное обеспечение позволяет производить мониторинг безопасности в режиме реального времени и поддерживает широкий перечень устройств и программных продуктов (28 источников), от которых оно может принимать и обрабатывать сообщения. В компании используется часть из них:

- Check Point Firewall-1,
- Cisco IOS ACL, FW, IDS,
- Cisco Secure ACS,
- Cisco Secure IDS,
- Cisco Secure PIX,
- Cisco Secure PIX IDS,
- Cisco Security Agent,
- Концентратор Cisco VPN,
- Cisco Firewall Switch Module,
- Tripwire NIDS,
- Web-серверы Microsoft IIS,
- Windows Events,
- UNIX OS Events.

Центр управления сертификатами. В сети широко применяются сертификаты: для доступа посредством VPN, к Web-сайтам по SSL, для шифрования электронной почты. Сервер центра управления сертификатами является частью внутренней инфраструктуры открытых ключей и используется для выпуска или отзыва внутренних сертификатов и публикации списка отозванных сертификатов (Certificate Revocation List). Центр управления сертификатами развернут на неподключенном к сети Windows 2000 Server Service Pack 4. В качестве процедуры установки инфраструктуры открытых ключей основной (root) центр управления сертификатами был использован только однажды, с целью выпуска сертификата для выпускающего центра управления сертификатами, и после этого был немедленно переведен в офлайн-режим. Секретный (private) ключ основного центра сертификации был перемещен на дискету, удален с жесткого диска, и эта дискета была помещена в сейф отдела информационной безопасности. Копия дискеты хранится за пределами офиса в защищенном помещении в сейфе. *Cisco Secure ACS Server.* С помощью Cisco Secure ACS Server v.3.3 for Windows осуществляется аутентификация:

- сотрудники, использующие VPN, аутентифицируются и получают IP-адрес из ACS-сервера на основе протокола RADIUS;
- доступ к сетевым устройствам для администрирования контролируется с использованием протокола TACACS+.

TACACS+ является протоколом последнего поколения из серии протоколов TACACS. TACACS – это простой протокол управления доступом, он основан на стандартах User Datagram Protocol (UDP), разработанных компанией Bolt, Beranek, and Newman, Inc. (BBN) для военной сети Military Network (MILNET). Компания Cisco несколько раз совершенствовала и расширяла протокол TACACS, и в результате появилась ее собственная версия TACACS, известная как TACACS+. TACACS+ пользуется транспортным протоколом TCP. «Демон» (процесс, запускаемый на машине UNIX или NT) сервера «слушает» порт 49, который является портом протокола IP, выделенным для протокола TACACS. Этот порт зарезервирован для выделенных номеров RFC в протоколах UDP и TCP. Все текущие версии

TACACS и расширенные варианты этого протокола используют порт 49.

Протокол TACACS+ работает по технологии «клиент-сервер», где клиентом TACACS+ обычно является NAS, а сервером TACACS+, как правило, считается «демон». Фундаментальным структурным компонентом протокола TACACS+ является разделение аутентификации, авторизации и журналирования (AAA – Authentication, Authorization, Accounting). Это позволяет обмениваться идентификационными сообщениями любой длины и содержания и, следовательно, использовать для клиентов TACACS+ любой механизм аутентификации, в том числе PPP PAP, PPP CHAP, аппаратные карты и Kerberos.

Транзакции между клиентом TACACS+ и сервером TACACS+ идентифицируются с помощью общего ключа – «секрета», который никогда не передается по каналам связи. Обычно этот секрет вручную устанавливается на сервере и на клиенте. TACACS+ можно настроить на шифрование всего трафика, который передается между клиентом TACACS+ и «демоном» сервера TACACS+. Процесс обмена информацией между ACS и сервером TACACS+ во время процесса аутентификации протекает по следующей схеме:

• ACS посылает START-запрос на сервер TACACS+ для начала процесса аутентификации;

• сервер отсылает ACS-пакет с запросом GETUSER, содержащий запрос пользователю на ввод имени;

• ACS отображает запрос пользователю и отсылает серверу TACACS+ введенное пользователем имя в пакете CONTINUE;

• сервер отсылает ACS-пакет с запросом GETPASS, содержащий запрос пользователю на ввод пароля;

• ACS высылает пакет CONTINUE, содержащий пароль, введенный пользователем серверу TACACS+;

• сервер TACACS+ выполняет проверку полученной пары «имя-пароль» и в зависимости от результата проверки отсылает ACS-пакет, содержащий результат (FAIL – в случае несовпадения, PASS – успешная аутентификация). На этом процесс аутентификации завершается.

Процесс обмена информацией между ACS и сервером TACACS+ во время процесса авторизации протекает по следующей схеме: • ACS от отсылает пакет START AUTHORIZATION серверу TACACS+;

• сервер TACACS+ обрабатывает полученные данные и принимает решение, основываясь на политике безопасности, связанной с данным пользователем. Результат отсылается ACS-серверу в RESPONSE-пакете.

Здесь под авторизацией понимается процесс определения действий, которые позволены данному пользователю. Обычно идентификация предшествует авторизации, однако это не обязательно. В запросе на авторизацию можно указать, что идентификация пользователя не проведена (личность пользователя не доказана). В этом случае лицо, отвечающее за авторизацию, должно самостоятельно решить, предоставлять такому пользователю запрашиваемые услуги или нет. Протокол TACACS+ предусматривает только положительную или отрицательную авторизацию и допускает настройку на потребности конкретного заказчика. Авторизация может проводиться на разных этапах, например, когда пользователь впервые входит в сеть и хочет открыть графический интерфейс или когда пользователь запускает PPP и пытается использовать поверх PPP протокол IP с конкретным адресом IP. В этих случаях «демон» сервера TACACS+ может разрешить предоставление услуг, но наложить ограничения по времени или потребовать список доступа IP для канала PPP.

Следом за идентификацией и авторизацией следует журналирование, которое представляет собой запись действий пользователя. В системе TACACS+ журналирование может выполнять две задачи. Во-первых, оно может применяться для учета использованных услуг (например, для выставления счетов). Во-вторых, его можно применять в целях безопасности. Для этого TACACS+ поддерживает три типа учетных записей. Записи «старт»

указывают, что услуга должна быть запущена. Записи «стоп» говорят о том, что предоставление услуги только что прекратилось. Записи «обновление» (update) являются промежуточными и указывают на то, что услуга все еще предоставляется.

Учетные записи TACACS+ содержат всю информацию, которая используется в ходе авторизации, а также другие данные, такие, как время начала и окончания (если это необходимо), и данные об использовании ресурсов.

Механизм взаимодействия ACS и сервера TACACS+ выглядит следующим образом:

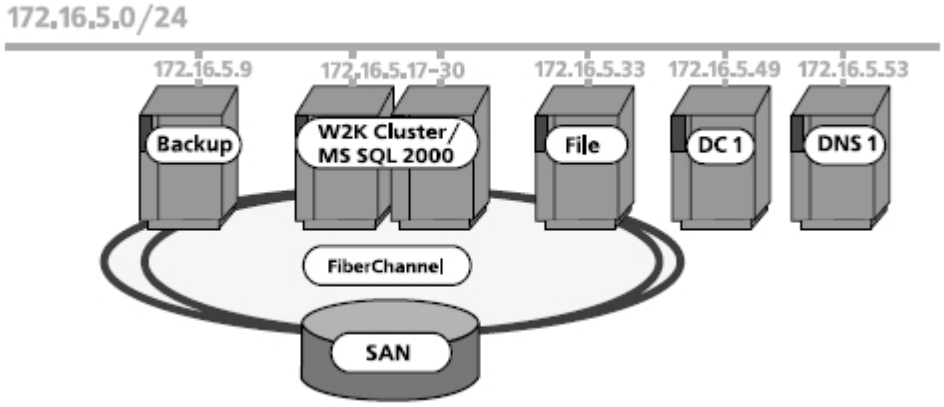
• ACS отсылает учетную запись серверу TACACS+, основываясь на выбранных методах и событиях;

• сервер TACACS+ отсылает ответный пакет ACS-серверу, подтверждая прием учетной записи.

Zone Labs Integrity Server. Zone Labs Integrity Server v. 1.6 используется для принудительного применения политики безопасности организации VPN на компьютерах сотрудников, которые подключаются посредством VPN. В данном случае потребуется установка на каждом компьютере Integrity Agent для приема и применения политики во время установления VPN-соединения. Integrity Agent позволяет также производить мониторинг антивирусного программного обеспечения на клиенте и отключает VPN-соединение, если программное обеспечение не установлено или не имеет последних обновлений. Это очень важно, так как удаленный компьютер может быть не защищен надлежащим образом и стать точкой входа во внутреннюю сеть для вирусов и злоумышленников. Единственным устройством, которому разрешено устанавливать соединение с этим сервером, является VPN-концентратор. *HP OpenView.* Для мониторинга всех сетевых устройств и серверов используется HP OpenView Network Node Manager v.6.31. Компания осознает необходимость мониторинга в режиме 24 часа в сутки 7 дней в неделю для обеспечения высокой доступности сервисов. Из-за большой степени риска разрешено использовать SNMP только в режиме read-only. Правила на межсетевых экранах разрешают данный трафик только на станцию управления NNM. Этот сервер использует Windows 2000 Server Service Pack 4 и защищен в соответствии с перечисленными выше руководствами. Все устройства сконфигурированы для отправления SNMP traps на сервер NNM, и любой другой доступ из-за пределов сети управления запрещен.

4.2.5. Зона защищаемых данных компании

В этой сети (см. рис, 4.5) находятся все данные Web-приложений. Также здесь располагаются серверы Active Directory, контроллеры доменов Web-приложения и DNS-серверы. Каждый из них является кластером, который состоит из двух компьютеров. На рис. 4.5 это не отображено для того, чтобы сделать его более читабельным.



...

Рис. 4.5. Схема зоны защищаемых данных компании (Secure Data Network)

Система управления базами данных и файл-серверы. В качестве сервера баз данных используется Microsoft Windows 2000 Advanced Server Service Pack 4 и Microsoft SQL Server 2000 Service Pack 3. Файл-серверы построены на Microsoft Windows 2000 Server Service Pack 4 и Microsoft File and Print Services. Для обеспечения избыточности и высокой доступности на файл-серверах развернута интегрированная с Active Directory служба Distributed File System. Только серверы промежуточного уровня имеют доступ к Microsoft SQL Server. При этом стандартный порт TCP 1433 изменен на нестандартный порт TCP 2000. Доступ из внутренней сети к базе данных ограничен только выполнением запросов к базе данных и только с определенного списка IP-адресов.

Active Directory. «Лес» (forest) Active Directory Web-приложений полностью отделен от внутреннего «леса». Серверы из Web-зоны подключаются к контроллеру домена с использованием IPSec в режиме Authentication Header (AH). Этот дизайн имеет следующие преимущества:

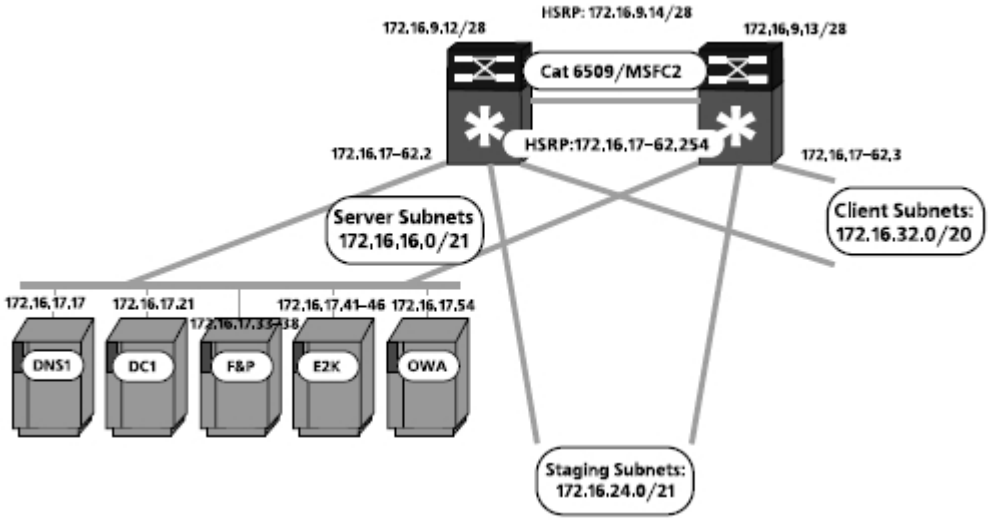
• разрешается использование IPSec-фильтрования на самих серверах;

• упрощается конфигурирование межсетевого экрана, так как требуется только два правила;

• нагрузка на процессор минимальная, так как используется не шифрование, а только аутентификация.

Active Directory DNS-серверы сконфигурированы для использования DNS-серверов Web-зоны как перенаправляющих для разрешения внешних адресов. Резервное копирование реализовано с помощью Fiber Channel, поэтому не требуется дополнительный сетевой сегмент. Серверы, которые осуществляют резервное копирование, не имеют сетевых подключений за пределами сегмента. 4.2.6. Зона внутренней сети компании

Во внутренней сети находятся рабочие станции сотрудников и внутренние серверы. Сеть логически разделена на две части: подсеть серверов и подсеть сотрудников. Ядром проекта являются два коммутатора Cisco Catalyst 6509 с модулями маршрутизации MSFC2. Коммутаторы используют trunk для избыточности. Для каждой внутренней подсети создан отдельный VLAN и сконфигурирован HSRP на каждом из VLAN-интерфейсов для «горячего» резервирования. Раздельные маршрутизирующие интерфейсы для каждого VLAN позволяют задействовать дополнительные списки контроля доступа для ограничения доступа из определенных подсетей или компьютеров. На рис. 4.6 изображен только один сервер каждого типа для читабельности.



...

Рис. 4.6. Пример организации сегмента сети (VLAN)

Внутренняя сеть Windows 2000 использует изолированный «лес» Active Directory со своими собственными DNS-серверами и контроллерами домена. На всех серверах установлен Windows 2000 Server Service Pack 4, при этом они защищены в соответствии с перечисленными выше руководствами.

DNS-серверы – это Microsoft DNS Server с использованием Dynamic DNS в режиме «Allow Secure Updates Only». Данные серверы применяются только для разрешения имен внутренних ресурсов и перенаправляют запросы на разрешение внешних имен в зону Интернета.

В качестве внутреннего сервера обмена сообщениями и совместной работы используется Microsoft Exchange 2000 Service Pack 3. Он работает на двухузловом кластере Windows 2000 Advanced Server Service Pack 4 для обеспечения избыточности и балансировки нагрузки. Все исходящие сообщения перенаправляются к SMTP-серверам в интернет-зону. В качестве антивирусного программного обеспечения применяется Sybari Antigen v.7.0 for Exchange с проверкой входящих и исходящих сообщений.

Работа с почтой удаленных пользователей обеспечивается сервером Exchange 2000 Service Pack 3 Outlook Web Access, который доступен через VPN-соединение поверх HTTPS. Выбор объясняется тем, что для подключения достаточно только одного порта (HTTPS). При обычном же способе доступа к Exchange пришлось бы открывать целый набор портов, что существенно увеличивает риск взлома системы.

Файл-серверы реализованы с использованием Microsoft SharePoint Portal Server 2003. Доступ к файлам осуществляется через VPN поверх HTTP/HTTPS. Это делает ненужной настройку межсетевого экрана для трафика SMB/CISF, что упрощает конфигурацию межсетевого экрана и делает дизайн более защищенным.

Исходящий доступ разрешен только для HTTP/HTTPS из сети сотрудников через ргоху-сервер. В целях обеспечения безопасности не разрешен доступ из подсети серверов в Интернет. При необходимости установки драйверов или обновлений они загружаются обслуживающим персоналом на свои рабочие места и далее переносятся на серверы на CD-дисках или дискетах.

Доступ к серверам баз данных предоставлен ограниченному списку администраторов баз данных из определенного списка IP-адресов. Таким же образом предоставляется доступ к серверам данных и для менеджеров, ответственных за наполнение Web-страниц приложения.

В сети тестирования тестируются приложения перед их перемещением в действующую сеть. Данная сеть полностью имитирует рабочие серверы и также используется для тестирования сервисных пакетов и обновлений перед их установкой на серверы и рабочие станции. Это позволяет уменьшить вероятность несовместимости приложений и увеличить надежность функционирования сети и приложений. Реализована процедура управления изменениями.

4.3. Настройки основных компонент системы защиты компании

4.3.1. Настройки пограничных маршрутизаторов

Пограничные маршрутизаторы являются первой линией защиты. Для создания технических настроек использовались руководства Агентства национальной безопасности США: NSA/SNAC Router Security Configuration Guide, NSA/SNAC Router Security Configuration Guide Executive Summary.

Пароли. Пароли на маршрутизаторах должны храниться в зашифрованном виде. Нельзя использовать епаЬе-пароль, так как для его шифрования используется слабый алгоритм и злоумышленник легко вскроет его. Необходимо применить следующие команды:

...

service password-encryption

enable secret Gh!U765H!!
no enable password

Отключение неиспользуемых возможностей управления. Для управления используется консольный доступ, поэтому все остальные способы доступа должны быть отключены:

...
line vty 0 15
no login
transport input none
transport output none
line aux 0
no login
transport input none
transport output none

Отключение возможности маршрутизатора загружать конфигурацию из сети:

...
no boot network
no service config

Настройка TACACS+. Необходимо защитить доступ для управления. Хотя этот доступ не разрешен по сети, нужно использовать TACACS+ для централизованного управления аутентификацией и авторизацией доступа с целью управления и журналирования изменений, произведенных на маршрутизаторах. TACACS+ был выбран вместо RADIUS по причине большей защищенности. Имя пользователя и пароль в TACACS+ шифруются, в то время как в RADIUS шифруется только пароль. При использовании Cisco ACS TACACS+ можно настроить детальные уровни доступа для различных пользователей и групп пользователей.

Определяем IP-адрес сервера TACACS+ и пароль для аутентификации:

...
tacacs-server 172.16.6.21
tacacs-server key F$!19Ty
tacacs-server attempts 3
ip tacacs source-interface Fa0/0

Далее настраивается аутентификация, авторизация и журналирование. TACACS+ будет использоваться в качестве главного средства аутентификации, а локальная база пользователей маршрутизатора будет использоваться в случае, если сервер TACACS+ станет недоступным. Для этого обязательно должны быть созданы локальные учетные записи на маршрутизаторе. Настройка использования TACACS+ для AAA:

...
aaa new-model
aaa authentication login default group tacacs+ local
aaa authentication enable default group tacacs+ enable
aaa authorization exec default group tacacs + local

aaa authorization commands 15 default group tacacs+ local
aaa accounting exec default start-stop group tacacs+
aaa accounting commands 15 default start-stop group tacacs+

Используемый метод аутентификации применяется для консольного доступа:

...
line console 0
login authentication default exec-timeout 5 0
logging synchronous

Предупреждающий баннер:

...
banner login «This is a private computer system for authorized use only.
All access is logged and monitored. Violators could be prosecuted».

«Ежедневное» сообщение, выводимое в первую очередь при попытке получения доступа к маршрутизатору:

...
banner motd «This is a private computer system for authorized use only.
All access is logged and monitored. Violators could be prosecuted».

Сообщение, выводимое при входе в непривилегированный (EXEC) режим:

...
banner exec «Any unauthorized access will be vigorously prosecuted».

Маршрутизация «от источника». Отключение маршрутизации «от источника». Маршрутизация от источника дает пакетам возможность переносить информацию о «верном» или более удобном маршруте и позволяет пренебречь правилами, которые предписаны в таблице маршрутизации для данного пакета, то есть модифицирует маршрут пакета. Это позволяет злоумышленнику управлять трафиком по своему желанию. Необходимо отключить маршрутизацию «от источника»:

...
no ip source-route

4.3.2. Сервисы маршрутизатора

Необходимо отключить все неиспользуемые и опасные сервисы на маршрутизаторе и сконфигурировать нужные сервисы для обеспечения безопасности. Некоторые из них уже отключены по умолчанию в версии IOS 12.3, поэтому здесь они приводятся для дополнительной проверки.

«Малые» сервисы. Отключение редко используемых UDP-и TCP-сервисов диагностики:

...
no service tcp-small-servers
no service tcp-small-servers

Чтобы уменьшить для злоумышленника возможности получения дополнительной информации о маршрутизации, надо отключить сервисы finger и identd. Также требуется отключить HTTP-, DNS-, DHCP-, bootp-сервисы:

...
no ip finger
no service finger
no ip identd
no ip http server
no ip bootp service
no ip domain-lookup
no service pad
no service dhcp
no call rsvp-sync

Определяется максимальное количество получателей для SMTP-соединений для встроенной в IOS функции поддержки факсов. Установка максимального количества, равного 0, означает отключение сервиса:

...
mta receive maximum-recipients 0

Отключение протокола CDP (Cisco Discovery Protocol), который позволяет обмениваться информацией канального уровня с другими устройствами от компании Cisco:

...
no cdp running

Отключение функций proxy arp на маршрутизаторе. Proxy arp позволяет распространяться ARP-запросам по смежным сетям, что дает злоумышленнику дополнительную возможность узнать о структуре сети:

...
no ip proxy-arp

Для того чтобы в сообщениях, отправляемых по syslog, присутствовала временная метка, необходимо выполнить команды:

...
service timestamps debug datetime msec localtime showtimezone
service timestamps log datetime msec localtime showtimezone

Конфигурирование SNMP. Так как мониторинг сетевых устройств осуществляется из сети управления и является критичным аспектом обеспечения высокой доступности, решено использовать SNMP, несмотря на проблемы безопасности, связанные с ним. Для минимизации риска предприняты следующие шаги:

• запрещен SNMP-трафик в Интернет и из Интернета;

• ограничено количество используемых счетчиков.

Используемые команды:

```
...
snmp-server view NNM-Only internet included
snmp-server view NNM-Only ipRouteTable excluded
snmp-server view NNM-Only ipNetToMediaTable excluded
snmp-server view NNM-Only at excluded
```

Списки контроля доступа сконфигурированы для ограничения доступа только с HP OpenView NNM:

```
...
access-list 5 permit host 172.16.6.33
```

и SNMP используется только для чтения:

```
...
snmp-server community ThaaMasdf view NNM-Only RO 5
```

Маршрутизатор также сконфигурирован для отправки trap только к SNMP-серверу:

```
...
snmp-server host 172.16.6.33 Thaa!!asdf
snmp-server enable traps config
snmp-server enable traps envmon
snmp-server enable traps bgp
snmp-server trap-authentication
snmp-server trap-source Fa0/0
```

Конфигурирование протокола NTP Сконфигурирован список контроля доступа для ограничения получения времени через NTP только с сервера времени:

```
...
access-list 10 permit 172.16.6.41
access-list 10 deny any
ntp authentication-key 1 md5 Hn!hj
ntp authenticate
ntp trusted-key 1
ntp access-group peer 10
ntp update-calendar
ntp server 172.16.6.41 key 1
```

ntp source Fa0/0

Журналирование событий маршрутизатора. Для журналирования событий используется протокол syslog. Журналы собираются на Cisco SIMS:

...

logging buffered 16000
no logging console
logging source-interface Fa0/0
logging trap informational
logging facility local7
logging 172.16.6.25

Настройки безопасности на уровне интерфейса. Для предупреждения использования интерфейса как усилителя при проведении атаки типа «отказ в обслуживании», например smurf, надо отключить маршрутизацию пакетов на broadcast-адреса. По умолчанию маршрутизатор не пропускает широковещательных сообщений с IP-адресом приемника 255.255.255.255. Для того чтобы ограничить негативное влияние направленных широковещательных сообщений на определенные сети, необходимо использовать эту команду:

...

no ip directed-broadcast

Чтобы уменьшить для злоумышленника возможности получения информации о сети, надо выполнить следующие команды:

...

no ip unreachable
no ip mask-reply
no ip redirect

Для уменьшения проблем, вызываемых пакетами с неправильными или подмененными IP-адресами, а также с исходными IP-адресами, которые не могут быть проверены, используется функция Unicast RPF:

...

ip cef
interface hssi2/0
ip verify unicast reverse-path

Конфигурирование функции TCP Intercept. Функция TCP Intercept помогает предупредить атаки типа SYN Flood путем прерывания и проверки TCP-соединений. В режиме Intercept программное обеспечение прерывает пакеты синхронизации TCP SYN от клиентов к серверам, совпадающие с расширенным списком контроля доступа. Осуществляются проверки, и попытки достичь сервер с несуществующих (неотвечающих) компьютеров пресекаются. Включение функции TCP Intercept:

...

access-list 110 permit tcp any 70.70.70.0 0.0.0.255
ip tcp intercept list 110

Конфигурирование BGP. BGP v. 4 используется для обмена информацией о маршрутизации и политиках с маршрутизаторами интернет-провайдера. Так как уже существуют атаки, направленные против протокола BGP, то необходимо обеспечить надлежащий уровень защиты.

Для защиты используем возможность BGP аутентифицироваться с помощью MD5:

...

router bgp 5500 (здесь 5500 – номер автономной системы)
neighbor 70.70.1.2 password F!$asB!
ip as-path access-list 30 permit
router bgp 5500
neighbor 70.70.1.2 filter-list 30

Этот фильтр гарантирует, что маршрутизатор сможет принимать трафик только из определенной автономной системы. Также используется список контроля доступа на входящий трафик, разрешающий трафик по TCP 179 только от маршрутизаторов интернет-провайдера.

Маршрут «черная дыра». Для увеличения производительности маршрутизатора при запрещении пакетов с недостижимыми адресами назначения используется статический маршрут в null. Кроме этого данная конфигурация позволит предупредить простейшие атаки типа «отказ в обслуживании». Такая конфигурация стала возможной благодаря тому, что для получения маршрутов используется BGP. Маршрут должен иметь наивысший вес, то есть маршрутизатор никогда не будет запрещать любой легитимный трафик. Также необходимо отключить ICMP Unreachable на null-интерфейсе:

...

ip route 0.0.0.0 0.0.0.0 null 0 255
interface NullO
no icmp unreachables

Конфигурирование списков контроля доступа. На пограничных маршрутизаторах очень хорошо фильтровать ненужный входящий трафик, уменьшая, таким образом, нагрузку на внешние межсетевые экраны и уменьшая размеры журналов на внутренних устройствах. Пограничные маршрутизаторы также защищают внешние межсетевые экраны.

Для ограничения трафика используются расширенные списки контроля доступа. Используется новая возможность компилирования списков контроля доступа Turbo ACL, которая существенно увеличивает производительность обработки списков контроля доступа. К сожалению, эта функция не работает с рефлексивными списками контроля доступа и с CBAC (Context-Based Access Control). Для включения этой функциональности требуется всего одна команда:

...

access-list compiled

Сконфигурированы два списка контроля доступа – для входящего и исходящего трафика.

Список контроля доступа для входящего трафика. Блокируется трафик с недействительными адресами, без исходного адреса, направленный на «опасные» порты – NetBIOS, SNMP, TFTP, syslog, направленный в сеть между внешними маршрутизаторами и внешними межсетевыми экранами, направленный на диапазон адресов, используемых для multicast:

...

no ip extended Ingress
ip access-list extended Ingress
deny ip host any 255.255.255.255
deny ip host 0.0.0.0 any

Сети 70.0.0.0/8 и 90.0.0.0/8 также зарезервированы I ANA, но не включены сюда из-за нашего первоначального предположения:

Deny	ip	1.0.0.0	0.255.255.255	any
deny	ip	2.0.0.0	0.255.255.255	any
deny	ip	5.0.0.0	0.255.255.255	any
deny	ip	7.0.0.0	0.255.255.255	any
deny	ip	10.0.0.0	0.255.255.255	any
deny	ip	23.0.0.0	0.255.255.255	any
deny	ip	27.0.0.0	0.255.255.255	any
deny	ip	31.0.0.0	0.255.255.255	any
deny	ip	36.0.0.0	0.255.255.255	any
deny	ip	37.0.0.0	0.255.255.255	any
deny	ip	39.0.0.0	0.255.255.255	any
deny	ip	41.0.0.0	0.255.255.255	any
deny	ip	42.0.0.0	0.255.255.255	any
deny	ip	49.0.0.0	0.255.255.255	any
deny	ip	50.0.0.0	0.255.255.255	any
deny	ip	58.0.0.0	0.255.255.255	any
deny	ip	59.0.0.0	0.255.255.255	any
deny	ip	71.0.0.0	0.255.255.255	any
deny	ip	72.0.0.0	0.255.255.255	any
deny	ip	73.0.0.0	0.255.255.255	any
deny	ip	74.0.0.0	0.255.255.255	any
deny	ip	75.0.0.0	0.255.255.255	any
deny	ip	76.0.0.0	0.255.255.255	any
deny	ip	77.0.0.0	0.255.255.255	any
deny	ip	78.0.0.0	0.255.255.255	any
deny	ip	79.0.0.0	0.255.255.255	any
deny	ip	85.0.0.0	0.255.255.255	any
deny	ip	86.0.0.0	0.255.255.255	any
deny	ip	87.0.0.0	0.255.255.255	any
deny	ip	88.0.0.0	0.255.255.255	any
deny	ip	89.0.0.0	0.255.255.255	any
deny	ip	90.0.0.0	0.255.255.255	any
deny	ip	91.0.0.0	0.255.255.255	any

```
deny ip 92.0.0.0 0.255.255.255 any
deny ip 93.0.0.0 0.255.255.255 any
deny ip 94.0.0.0 0.255.255.255 any
deny ip 95.0.0.0 0.255.255.255 any
deny ip 96.0.0.0 0.255.255.255 any
deny ip 97.0.0.0 0.255.255.255 any
deny ip 98.0.0.0 0.255.255.255 any
deny ip 99.0.0.0 0.255.255.255 any
deny ip 100.0.0.0 0.255.255.255 any
deny ip 101.0.0.0 0.255.255.255 any
deny ip 102.0.0.0 0.255.255.255 any
deny ip 103.0.0.0 0.255.255.255 any
deny ip 104.0.0.0 0.255.255.255 any
deny ip 105.0.0.0 0.255.255.255 any
deny ip 106.0.0.0 0.255.255.255 any
deny ip 107.0.0.0 0.255.255.255 any
deny ip 108.0.0.0 0.255.255.255 any
deny ip 109.0.0.0 0.255.255.255 any
deny ip 110.0.0.0 0.255.255.255 any
deny ip 111.0.0.0 0.255.255.255 any
deny ip 112.0.0.0 0.255.255.255 any
deny ip 113.0.0.0 0.255.255.255 any
deny ip 114.0.0.0 0.255.255.255 any
deny ip 115.0.0.0 0.255.255.255 any
deny ip 116.0.0.0 0.255.255.255 any
deny ip 117.0.0.0 0.255.255.255 any
deny ip 118.0.0.0 0.255.255.255 any
deny ip 119.0.0.0 0.255.255.255 any
deny ip 120.0.0.0 0.255.255.255 any
deny ip 121.0.0.0 0.255.255.255 any
deny ip 122.0.0.0 0.255.255.255 any
deny ip 123.0.0.0 0.255.255.255 any
deny ip 124.0.0.0 0.255.255.255 any
deny ip 125.0.0.0 0.255.255.255 any
deny ip 126.0.0.0 0.255.255.255 any
deny ip 127.0.0.0 0.255.255.255 any
deny ip 169.254.0.0 0.0.255.255 any
deny ip 172.16.0.0 0.15.255.255 any
deny ip 173.0.0.0 0.255.255.255 any
deny ip 174.0.0.0 0.255.255.255 any
deny ip 175.0.0.0 0.255.255.255 any
deny ip 176.0.0.0 0.255.255.255 any
deny ip 177.0.0.0 0.255.255.255 any
deny ip 178.0.0.0 0.255.255.255 any
deny ip 179.0.0.0 0.255.255.255 any
deny ip 180.0.0.0 0.255.255.255 any
deny ip 181.0.0.0 0.255.255.255 any
deny ip 182.0.0.0 0.255.255.255 any
deny ip 183.0.0.0 0.255.255.255 any
deny ip 184.0.0.0 0.255.255.255 any
deny ip 185.0.0.0 0.255.255.255 any
deny ip 186.0.0.0 0.255.255.255 any

deny ip 187.0.0.0 0.255.255.255 any
deny ip 189.0.0.0 0.255.255.255 any
deny ip 190.0.0.0 0.255.255.255 any
deny ip 192.0.2.0 0.0.0.255 any
deny ip 192.168.0.0 0.0.255.255 any
deny ip 197.0.0.0 0.255.255.255 any
deny ip 220.0.0.0 3.255.255.255 any
deny ip 223.0.0.0 0.255.255.255 any
deny ip 224.0.0.0 31.255.255.255 any
```

Блокирование опасного трафика:

...

```
deny udp any any range 161 162
deny udp any any eq 69
deny tcp any any range 135 139
deny udp any any range 135 139
deny tcp any any eq 445
deny udp any any eq 514
permit tcp host 70.70.1.2 host 70.70.1.1 eq 79
```

permit tcp host 90.90.1.2 host 90.90.1.1 eq 79
deny ip any 70.70.70.16 0.0.0.15
permit tcp any 70.70.70.0 0.0.0.255 established
permit udp any 70.70.70.0 0.0.0.255
permit icmp any 70.70.70.0 0.0.0.255 source-quench
deny ip any any

Список контроля доступа для исходящего трафика. Для предупреждения организации атак типа «отказ в обслуживании» с подменой адресов разрешен доступ в Интернет только с IP-адресов компании. Весь трафик, направленный на «опасные» порты – NetBIOS, SNMP, TFTP, syslog, тоже удаляется:

...
no ip access-list extended Egress
ip access-list extended Egress
deny udp any any range 161 162
deny udp any any eq 69
deny tcp any any range 135 139
deny udp any any range 135 139
deny tcp any any eq 445
deny udp any any eq 514
permit tcp 70.70.70.0 0.0.255 any
permit udp 70.70.70.0 0.0.255 any
permit icmp any 70.70.70.0 0.0.0.255 source-quench
deny ip any any

Применение списков контроля доступа:

...
interface hssi2/0
ip access-group Ingress in
no ip proxy-arp
ip accounting access-violations
interface Fa0/0
ip access-group Egress in
no cdp enable
no ip proxy-arp
ip accounting access-violations

4.3.3. Настройки внешних межсетевых экранов

Внешние межсетевые экраны позволяют построить эффективный периметр защиты компании от угроз из Интернета. Политика безопасности внешних межсетевых экранов основана на бизнес-требованиях и согласована с общей политикой информационной безопасности компании. В качестве внешнего межсетевого экрана выбран Check Point Firewall-1 NG FP3, выполняющийся на аппаратной платформе Nokia IP530 с операционной системой IPSO v.3.6. В табл. 4.2 описаны все важные компоненты сети компании, подлежащие защите с помощью указанного межсетевого экрана.

Таблица 4.2. Компоненты сети, подлежащие защите

Имя	Описание	IP-адрес	Тип объекта
FWAdmin	Консоль управления Firewall-1	172.16.6.13	Check Point Host
FW-Front1	Внешний межсетевой экран № 1	70.70.70.28	Gateway
FW-Front2	Внешний межсетевой экран № 2	70.70.70.29	Gateway
FW-Front	Объект Gateway Cluster: cp-front1, cp-front2		Gateway Cluster
VRRPMulticast	VRRP Multicast-адрес	224.0.0.18	Workstation
VRRP-Front-Ext	VRRP-адрес на внешних интерфейсах	70.70.70.30	Workstation
VRRP-Front-DMZ1	VRRP-адрес на внутренних интерфейсах DMZ1	70.70.70.65	Workstation
VRRP-Front-DMZ2	VRRP-адрес на внутренних интерфейсах DMZ2	70.70.70.97	Workstation
VRRP-FW	Требуется для функционирования VRRP, включает: VRRP-Front-Ext, VRRP-Front-DMZ1, VRRP-Front-DMZ2		Group
Broadcast255	Все широковещательные адреса	255.255.255.255	Workstation
Broadcast0	Старые широковещательные адреса Broadcast0	0.0.0.0	Workstation
Broadcast	Группа, включающая: Broadcast255, Broadcast0		Group

Продолжение табл. 4.2

Имя	Описание	IP-адрес	Тип объекта
Net-Mgmt	Подсеть управления, необходима для включения функции antispoofing на административном интерфейсе межсетевых экранов	172.16.6.0 /24	Network
Net-Admin	Подсеть, соединяющая внутренние и внешние межсетевые экраны, выделенная для управления	172.16.1.0 /28	Network
Spoof-Admin	Группа, включающая: Net-Mgmt, Net-Admin		Group
Web-VIP1	Виртуальный IP-адрес для клиентской Web-фермы	70.70.70.81	Workstation
Web-VIP2	Виртуальный IP-адрес для партнерской Web-фермы	70.70.70.82	Workstation
Web-Incoming	Группа, включающая: Web-VIP1, Web-VIP2		Group
Proxy-GW1	Публичный адрес proxy-сервера № 1	70.70.70.105	Workstation
Proxy-GW2	Публичный адрес proxy-сервера № 2	70.70.70.106	Workstation
Proxy-GW	Группа, включающая: Proxy-GW1,Proxy-GW2		Group
SMTP-GW1	Публичный адрес SMTP-шлюза № 1	70.70.70.109	Workstation
SMTP-GW2	Публичный адрес SMTP-шлюза № 2	70.70.70.110	Workstation
SMTP-GW	Группа, включающая: SMTP-GW1,SMTP-GW2		Group
DNS-GW1	Публичный адрес DNS-сервера № 1	70.70.70.113	Workstation
DNS-GW2	Публичный адрес DNS-сервера № 2	70.70.70.114	Workstation
DNS-GW	Группа, включающая: DNS-GW1,DNS-GW2		Group
DNS-ISP1-1	DNS-сервер № 1 провайдера ISP1	12.x.x.x	Workstation
DNS-ISP1-2	DNS-сервер № 2 провайдера ISP1	12.x.x.x	Workstation
DNS-ISP2-1	DNS-сервер № 1 провайдера ISP2	207.x.x.x	Workstation
DNS-ISP2-2	DNS-сервер № 2 провайдера ISP2	204.x.x.x	Workstation
DNS-ISP	Группа, включающая: DNS-ISP1-1, DNS-ISP1-2, DNS-ISP2-1, DNS-ISP2-2		Group
VPN-GW1	Публичный адрес VPN-концентратора	70.70.70.117	Workstation
VPN-GW	Группа, включающая: VPNGW1		Group
Router-GW1	Внутренний адрес пограничного маршрутизатора № 1	70.70.70.18	Workstation

Окончание табл. 4.2

Имя	Описание	IP-адрес	Тип объекта
Router-GW2	Внутренний адрес пограничного маршрутизатора № 2	70.70.70.19	Workstation
Router-GW	Группа, включающая: Router-GW1, Router-GW2		Group
Net	Публичная сеть IP-адресов	70.70.70.0 /24	Network
TimeServer	Сервер времени	172.16.6.41	Workstation
HPOV	Сервер HP OpenView NNM	172.16.6.33	Workstation

Очень важно корректно определить все интерфейсы на межсетевом экране и установки anti-spoofing в свойствах объектов. Если это будет неправильно сконфигурировано, то межсетевой экран может заблокировать некоторый трафик, который должен быть разрешен, или может неправильно отработать функция anti-spoofing, которая вызовет появление новых рисков. Табл. 4.3 используется для конфигурирования интерфейсов. Таблица 4.3. Пример интерфейса межсетевого экрана

Объект	Интерфейс	Аппаратное имя	IP-адрес	Anti-spoofing
FW-Front1	External	eth-s1p1c0	70.70.70.28/28	Внешняя сеть
	DMZ1	eth-s1p2c0	70.70.70.66 /27	Эта сеть
	DMZ2	eth-s1p3c0	70.70.70.98 /27	Эта сеть
	Admin	eth-s1p4c0	172.16.1.5 /28	Сеть управления
	Cross	eth-s2p1c0	172.16.1.249 /29	Эта сеть
FW-Front2	External	eth-s1p1c0	70.70.70.29 /28	Внешняя сеть
	DMZ1	eth-s1p2c0	70.70.70.66 /27	Эта сеть
	DMZ2	eth-s1p3c0	70.70.70.99 /27	Эта сеть
	Admin	eth-s1p4c0	172.16.1.6 /28	Сеть управления
	Cross	eth-s2p1c0	172.16.1.250 /29	Эта сеть

Сервисы. В табл. 4.4 представлен список сервисов, которые необходимы для работы политики безопасности межсетевого экрана, некоторые из них были предустановлены, а некоторые пришлось создать. *Задание политики межсетевого экрана.* Чтобы политика была простой для понимания, сначала было создано небольшое количество правил. При этом учитывалось, что Check Point Firewall-1, подобно большинству других межсетевых экранов, обрабатывает правила последовательно. Поэтому более детальные правила предшествуют общим и наиболее часто повторяющиеся правила находятся в начале общего списка правил.

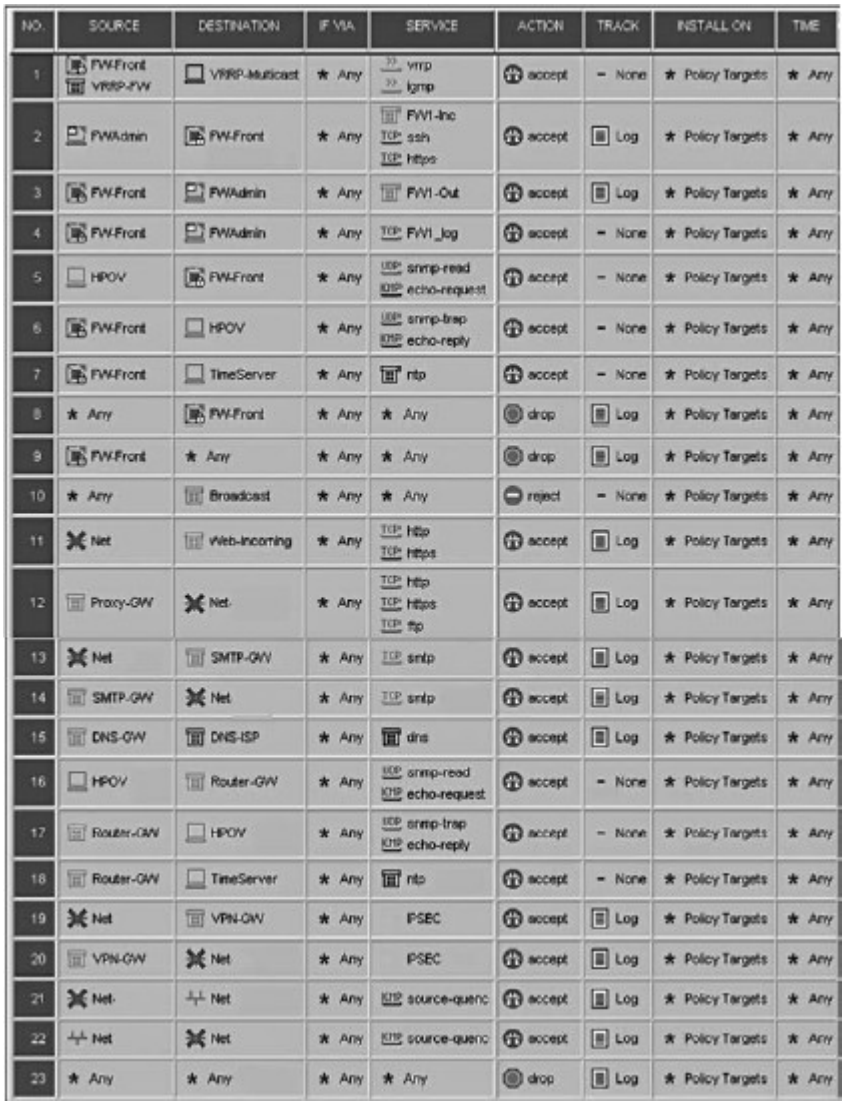
Таблица 4.4. Сервисы, необходимые для работы политики безопасности межсетевого

Сервис	Протокол	Порт получателя	Комментарии
CPD	TCP	18191	Check Point Daemon Protocol
CPD_amon	TCP	18192	Check Point Internal Application Monitoring
RDP	UDP	259	Check Point Reliable Datagram Protocol
FW1	TCP	256	Check Point VPN-1 & Firewall-1 Service
FW1_log	TCP	257	Check Point Logs
FW1_mgmt	TCP	258	Check Point Management
FW1_lca_pull	TCP	18210	Check Point Internal CA Pull Certificate Service
FW1_lca_push	TCP	18211	Check Point Internal CA Push Certificate Service
FW1-Inc	Group		CPD, CPD_amon, RDP, FW1_mgmt, FW1_lca_push, FW1
FW1-Out	Group		CPD, RDP, FW1_lca_pull, FW1
VRRP	IP type 112	n/a	
IGMP	IP type 2	n/a	
HTTP	TCP	80	
HTTPS	TCP	443	
FTP	TCP	21	
domain-udp	UDP	53	
domain-tcp	TCP	53	
DNS	Group		domain-udp, domain-tcp
SMTP	TCP	25	
NTP	UDP	123	
SSH	TCP	22	
IKE	UDP	500	
ESP	IP type 50	n/a	
TCP7456	TCP	7456	For Cisco VPN 3030 IPSec tunneling over TCP
IPSec	Group		IKE, ESP, TCP7456
SNMP-read	UDP	161	
SNMP-trap	UDP	162	
source-quench	ICMP	Type 4	

экрана

Был задан следующий порядок обработки трафика Firewall-1: • anti-spoofing;
• свойства, маркированные как «First» в Global Properties;
• все правила по порядку, за исключением последнего;
• свойства, отмеченные как «Before Last» в Global Properties;
• последнее правило;
• свойства, маркированные «Last» в Global Properties;
• неявно заданное правило «Drop».

На рис. 4.7 представлена реализованная политика межсетевого экрана. Как будет показано далее, все неявные правила межсетевого экрана были отключены на закладке Global Properties и созданы явные правила. Это позволило повысить защищенность межсетевого экрана.



NO.	SOURCE	DESTINATION	IF VIA	SERVICE	ACTION	TRACK	INSTALL ON	TIME
1	FW-Front VRRP-FW	VRRP-Multicast	★ Any	vrrp igmp	accept	– None	★ Policy Targets	★ Any
2	FWAdmin	FW-Front	★ Any	FW1-lnc TCP ssh TCP https	accept	Log	★ Policy Targets	★ Any
3	FW-Front	FWAdmin	★ Any	FW1-Out	accept	Log	★ Policy Targets	★ Any
4	FW-Front	FWAdmin	★ Any	TCP FW1_log	accept	– None	★ Policy Targets	★ Any
5	HPOV	FW-Front	★ Any	UDP snmp-read KTP echo-request	accept	– None	★ Policy Targets	★ Any
6	FW-Front	HPOV	★ Any	UDP snmp-trap KTP echo-reply	accept	– None	★ Policy Targets	★ Any
7	FW-Front	TimeServer	★ Any	ntp	accept	– None	★ Policy Targets	★ Any
8	★ Any	FW-Front	★ Any	★ Any	drop	Log	★ Policy Targets	★ Any
9	FW-Front	★ Any	★ Any	★ Any	drop	Log	★ Policy Targets	★ Any
10	★ Any	Broadcast	★ Any	★ Any	reject	– None	★ Policy Targets	★ Any
11	Net	Web-incoming	★ Any	TCP http TCP https	accept	Log	★ Policy Targets	★ Any
12	Proxy-GW	Net	★ Any	TCP http TCP https TCP ftp	accept	Log	★ Policy Targets	★ Any
13	Net	SMTP-GW	★ Any	TCP smtp	accept	Log	★ Policy Targets	★ Any
14	SMTP-GW	Net	★ Any	TCP smtp	accept	Log	★ Policy Targets	★ Any
15	DNS-GW	DNS-ISP	★ Any	dns	accept	Log	★ Policy Targets	★ Any
16	HPOV	Router-GW	★ Any	UDP snmp-read KTP echo-request	accept	– None	★ Policy Targets	★ Any
17	Router-GW	HPOV	★ Any	UDP snmp-trap KTP echo-reply	accept	– None	★ Policy Targets	★ Any
18	Router-GW	TimeServer	★ Any	ntp	accept	– None	★ Policy Targets	★ Any
19	Net	VPN-GW	★ Any	IPSEC	accept	Log	★ Policy Targets	★ Any
20	VPN-GW	Net	★ Any	IPSEC	accept	Log	★ Policy Targets	★ Any
21	Net	Net	★ Any	KTP source-quenc	accept	Log	★ Policy Targets	★ Any
22	Net	Net	★ Any	KTP source-quenc	accept	Log	★ Policy Targets	★ Any
23	★ Any	★ Any	★ Any	★ Any	drop	Log	★ Policy Targets	★ Any

...

Рис. 4.7. Правила безопасности межсетевого экрана

Задание правил безопасности межсетевого экрана. Опишем каждое правило в деталях.

Правило 1

NO.	SOURCE	DESTINATION	IF VIA	SERVICE	ACTION	TRACK	INSTALL ON	TIME
1	FW-Front VRRP-FW	VRRP-Multicast	★ Any	vrrp igmp	accept	– None	★ Policy Targets	★ Any

Источник: источник в этом правиле группирует вместе оба IP-адреса физических интерфейсов межсетевого экрана и IP-адреса, используемые VRRP (IP protocol 112) на каждом интерфейсе, где он включен. Это новое требование Check Point NG, начиная с версии FP2, для нормального функционирования VRRP. FW-Front – это объект типа Gateway Cluster, оба межсетевых экрана входят в этот объект. ***Получатель:*** VRRP multicast IP-адрес (244.0.0.18).

Сервис: VRRP (IP-protocol 112), IGMP (IP-protocol 2). Оба должны быть включены для функционирования VRRP в версиях Check Point NG FP2 и выше.

Журналирование: выключено (для уменьшения количества бесполезных записей в журнале).

Описание: правило разрешает функционирование VRRP между двумя межсетевыми

экранами для обеспечения работы в режиме кластера. Это правило установлено первым, так как очень важно, чтобы VRRP функционировал надлежащим образом между двумя межсетевыми экранами для уменьшения любых асимметричных потоков трафика.

Правило 2

Источник: сервер Check Point Management Console. ***Получатель:*** модули межсетевого экрана Check Point (объект Gateway Cluster содержит оба модуля).

Сервис: FWl-In – группа, которая содержит все сервисы для управления межсетевыми экранами. Для управления Nokia IPSO используются SSH и HTTPS. HTTPS включается только при начальной загрузке Nokia и удаляется из правила после настройки Nokia.

Журналирование: включено, все действия по управлению журналируются.

Описание: правило разрешает доступ к Nokia IPSO и межсетевому экрану Check Point для управления только от сервера управления (Management Server). Это правило должно предшествовать правилу, которое запрещает весь трафик на интерфейсы межсетевого экрана.

Правило 3

Источник: модули межсетевого экрана Check Point. ***Получатель:*** сервер Check Point Management Console.

Сервис: FWl-Out – группа которая содержит все сервисы, требуемые для управления модулями межсетевых экранов.

Журналирование: включено.

Описание: правило разрешает трафик между модулями межсетевых экранов и сервером управления. Это правило должно предшествовать правилу, которое запрещает весь трафик, исходящий от интерфейсов межсетевого экрана.

Правило 4

Источник: модули межсетевого экрана Check Point. ***Получатель:*** сервер Check Point Management Console.

Сервис: FWl-log – протокол, который используется модулями межсетевых экранов для отправки журналов на сервер управления.

Журналирование: выключено.

Описание: правило разрешает трафик журналирования, направленный к серверу управления. Это правило указано отдельно от предыдущего, потому что более эффективно журналировать управляющий трафик без самого журналирующего трафика.

Правило 5

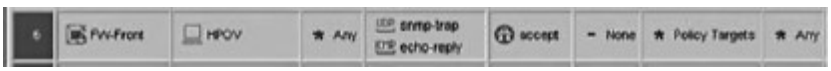
Источник: сервер HP OpenView NNM. ***Получатель:*** модули межсетевого экрана Check Point.

Сервис: SNMP-read, ICMP echo request (используется для Open View polling).

Журналирование: выключено.

Описание: правило разрешает мониторинг модулей межсетевого экрана с сервера HP OpenView NNM. Как уже было сказано выше, этот мониторинг является критически важным. Доступ по SNMP только в режиме read-only и только некоторые Nokia IPSO SNMP MIB включены. Расширения Check Point SNMP отключены.

Правило 6



Источник: модули межсетевого экрана Check Point. ***Получатель:*** сервер HP OpenView NNM.

Сервис: SNMP-trap, ICMP echo reply (используется для Open View polling).

Журналирование: выключено.

Описание: правило разрешает отправлять Nokia SNMP traps к серверу HP Open-View NNM. Только некоторые traps включены в конфигурации Nokia IPSO.

Правило 7

Источник: модули межсетевого экрана Check Point. ***Получатель:*** сервер времени.

Сервис: NTP.

Журналирование: выключено.

Описание: правило разрешает модулям межсетевого экрана синхронизировать время с сервером времени. Это очень важно для журналирования и правильного функционирования VRRP.

Правила 8–9

Сервис: любой. ***Журналирование:*** включено, все попытки установить соединение с и из модулей межсетевого экрана должны быть зафиксированы.

Описание: оба правила удаляют любой трафик, направленный к модулям межсетевых экранов или исходящий из модулей межсетевых экранов, разрешают модулям межсетевого экрана синхронизировать время с сервером времени. Трафик также будет удаляться последним правилом в списке, но важно зарегистрировать сам факт такого трафика. Специальные агенты на сервере SIMS осуществляют мониторинг этого трафика и отправляют сообщения администраторам при его возникновении.

Правило 10

Получатель: адреса широковещательной рассылки (broadcast). ***Сервис:*** любой.

Журналирование: выключено.

Описание: правило удаляет «шум», возникающий из-за широковещательной рассылки (broadcast) в файлах журналов.

Правило 11

Источник: любой, за исключением публичной подсети (70.70.70.0/24). ***Получатель:*** виртуальные IP-адреса двух ферм Web-приложений.

Сервис: HTTP, HTTPS.

Журналирование: включено. Эта установка может быть изменена после полной реализации всей архитектуры, потому что правило будет создавать слишком много записей в журналах.

Описание: первое реальное правило; относящееся к зоне Web. Правило разрешает Web-трафик к серверам Web-приложений. Публичные IP-адреса были исключены из адресов источников для уменьшения вероятности атаки с подменой IP-адресов, хотя это и не требуется, так как функция anti-spoofing будет отрабатывать этот вариант. Это просто дополнительный уровень защиты. Правило размещено выше всех остальных правил для увеличения производительности, из-за частого его использования.

Правило 12

Источник: proxy-серверы демилитаризованной зоны. ***Получатель:*** любой, за исключением публичной IP-подсети (70.70.70.0/24).

Сервис: HTTP, HTTPS, FTP.

Журналирование: включено. Эта установка может быть изменена после полной реализации всей архитектуры, потому что правило будет создавать слишком много записей в журналах. Весь исходящий трафик к внешним Web-серверам будет журналироваться.

Правило 13

Описание: правило разрешает внутренним пользователям получать доступ к внешним Web-серверам, определенным в политике компании. Это второе по частоте использования правило. ***Источник:*** любой, за исключением публичной IP-подсети (70.70.70.0/24).

Получатель: внешние SMTP-серверы компании.

Правило 14

Источник: внешние SMTP-серверы компании. ***Получатель:*** любой, за исключением публичной IP-подсети (70.70.70.0/24).

Сервис: SMTP.

Журналирование: включено, журналируются все входящие и исходящие SMTP-соединения.

Описание: 13-е и 14-е правила разрешает внешним SMTP-серверам принимать и отправлять электронную почту.

Правило 15

Источник: внешние DNS-серверы компании. ***Получатель:*** DNS-серверы ISP1 и ISP2.

Сервис: DNS, TCP и UDP.

Журналирование: включено, журналируются все входящие и исходящие STMP-соединения.

Описание: правило позволяет разрешать внешние DNS-имена. TCP разрешен для того случая, когда DNS-ответ слишком большой для размещения в UDP-пакете. Эта установка обеспечивает наиболее защищенный способ разрешения внешних DNS-имен, потому что требуется только доступ к четырем внешним DNS-серверам, которые принадлежат двум известным провайдерам.

Правило 16

Источник: сервер HP OpenView NNM. ***Получатель:*** внутренние интерфейсы пограничных маршрутизаторов.

Сервис: SNMP-read, ICMP echo request (используется для Open View polling).

Правило 17

Источник: внутренние интерфейсы пограничных маршрутизаторов. ***Получатель:*** сервер HP OpenView NNM.

Сервис: SNMP-trap, ICMP echo reply (используется для Open View polling).

Журналирование: выключено.

Описание: правило позволяет осуществлять мониторинг пограничных маршрутизаторов с помощью сервера HP OpenView NNM. Как уже было сказано выше, этот мониторинг является критически важным. Разрешен только доступ в режиме read-only; 16-е и 17-е правила используются редко, поэтому расположены именно здесь.

Правило 18

Источник: внутренние интерфейсы пограничных маршрутизаторов. ***Получатель:*** сервер времени.

Сервис: NTP.

Журналирование: выключено.

Описание: правило разрешает пограничным маршрутизаторам синхронизировать время с сервером времени.

Правило 19

Источник: любой, за исключением публичной IP-подсети (70.70.70.0/24).

Получатель: VPN-шлюз.

Правило 20

Источник: VPN-шлюз. ***Получатель:*** любой, за исключением публичной IP-подсети (70.70.70.0/24).

Сервис: IPSec: IKE, ESP, TCP 7456 (Cisco IPSec tunneling over TCP).

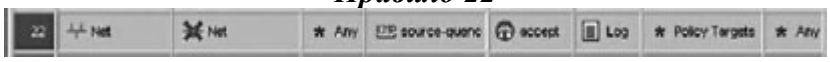
Журналирование: включено (для журналирования всей активности, связанной с использованием VPN).

Описание: 19-е и 20-е правила разрешают удаленный доступ через VPN. Журналирование используется, хотя VPN-концентратор имеет свое собственное журналирование, потому что VPN-шлюз обеспечивает доступ во внутреннюю сеть компании, что очень важно. Публичные IP-адреса компании были исключены из списка для предупреждения попыток осуществить VPN-соединение из внутренней сети компании, VPN-соединение должно быть доступно только из Интернета.

Правило 21

Источник: любой из публичной IP-подсети (70.70.70.0/24). ***Получатель:*** любой, за исключением публичной IP-подсети (70.70.70.0/24).

Правило 22



Источник: любой, за исключением публичной IP-подсети (70.70.70.0/24). ***Получатель:*** любой из публичной IP-подсети (70.70.70.0/24).

Сервис: ICMP source quench.

Журналирование: включено.

Описание: 21-е и 22-е правила разрешают сообщения ICMP source quench для оптимизации скорости передачи, увеличивающей производительность.

Правило 23

Источник: любой. ***Получатель:*** любой.

Сервис: любой.

Журналирование: включено; весь трафик, не удовлетворяющий предыдущим правилам, должен быть записан и проанализирован.

Описание: правило блокирует весь трафик, который не был явно разрешен в предыдущих правилах. Действие на это правило – drop, а не reject для того, чтобы к отправителю не посылался никакой трафик. В этом случае злоумышленникам трудно провести сетевую разведку.

Настройки безопасности Nokia IPSO. Выбор Nokia IPSO был обусловлен следующим:
• операционная система – урезанная версия Unix BSD;

• все исполняемые файлы находятся в файловой системе в режиме «только для чтения»;

• все настройки конфигурации хранятся в одном файле, что упрощает резервное копирование и проверки внесенных изменений;

• сервис Inetd стартует пустым, и каждый новый сервис должен быть добавлен явно;

• нет сервисов, способных отдать дополнительную информацию о системе удаленным пользователям, типа finger, who или talk;

• нет экспортируемой файловой системы или X Windows;

• система однопользовательская, то есть отсутствует угроза повышения привилегий непривилегированными пользователями;

• нет возможности добавлять новых пользователей.

Также были проделаны следующие шаги по повышению защищенности системы: • начальное конфигурирование было произведено без подключения в сеть;

• все неиспользуемые интерфейсы отключены;

• для удаленного администрирования используется SSH v.2 в режиме RSA, отключен SSH v.l;

• Telnet отключен;

• HTTP отключен, для начального администрирования был использован SSL. После настройки конфигурации SSL был отключен и для администрирования используется только SSH и локальный браузер Lynx;

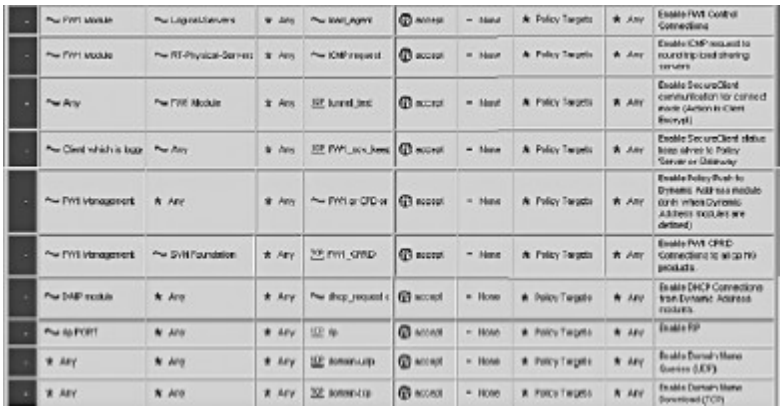
• доступ для управления и администрирования ограничен определенным списком IP-адресов через списки контроля доступа;

• на межсетевых экранах используется статическая маршрутизация.

Настройки безопасности сервера управления Check Point Firewall-1. Сервер управления установлен на Windows 2000 Service Pack 4 и сконфигурирован в соответствии с руководствами по безопасности, указанными ранее. *Глобальные свойства Check Point Firewall-1.* Первый и наиболее важный шаг после начальной настройки Firewall-1 – отключить неявные правила, установленные по умолчанию на закладке Global Properties. На рис. 4.8 показаны правила, имеющие обозначение «First», то есть они обрабатываются перед любыми другими правилами.

...

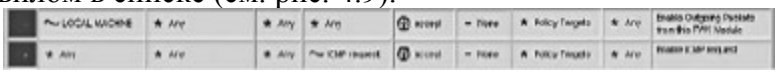
Рис. 4.8. Пример правил безопасности межсетевого экрана



...

Рис. 4.8а. Пример правил безопасности межсетевого экрана (продолжение)

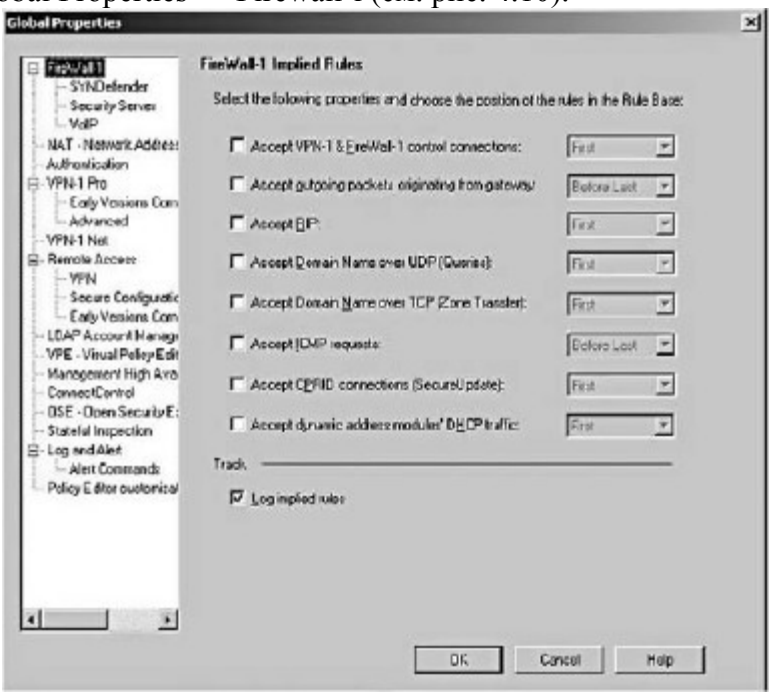
Вдобавок существуют и два правила, именуемые «Before Last», которые исполняются перед последним правилом в списке (см. рис. 4.9).



...

Рис. 4.9. Правила «Before Last»

Существует много проблем, связанных с этими правилами по умолчанию. Для многих из них в качестве источника или получателя указан «любой», что ведет к уменьшению степени защищенности как самого межсетевого экрана, так и сети, которую он защищает. Другая проблема заключается в том, что действия по этим правилам не журналируются и нет возможности включить журналирование. Все неявные правила по умолчанию должны быть отключены и указаны явные правила для включения только тех сервисов, которые действительно необходимы. Для отключения правил по умолчанию можно использовать закладку Policy → Global Properties → Firewall-l (см. рис. 4.10).



...

Рис. 4.10. Отключение неявных правил безопасности межсетевого экрана

4.3.4. Настройки VPN

Для обеспечения удаленного доступа в сеть компании используется концентратор Cisco VPN 3030. В основу архитектуры VPN-доступа были положены следующие правила:

• для удаленного доступа используется протокол IPSec (проколы PPTP и L2TP не поддерживаются из-за низкой защищенности);

• для аутентификации и шифрования используется Encapsulating Security Protocol (ESP);

• для аутентификации IKE используются цифровые сертификаты (preshared-ключи не

применяются из-за низкой защищенности);

• VPN-сертификаты сотрудников компании хранятся на устройствах Aladdin eToken USB. Это позволило обеспечить защищенное хранение сертификатов;

• для аутентификации пользователей VPN и выдачи IP-адресов VPN-клиентам применяется сервер Cisco Access Control Service с использованием протокола RADIUS;

• сервер Zone Labs Integrity используется для реализации политики безопасности и проверки настроек антивирусного программного обеспечения на подключаемых компьютерах. С его помощью осуществляется контроль программ и приложений, которые могут быть использованы внутри VPN-соединения;

• VPN-концентратор разрешает доступ только к некоторым подсетям и компьютерам, основываясь на членстве в группах пользователей, созданных на концентраторе.

Аутентификация пользователей VPN. Сервер Cisco Secure ACS выполняет аутентификацию пользователей VPN и выдачу IP-адреса. Конфигурирование VPN-концентратора необходимо выполнять только после того, как сконфигурирован сервер ACS с соответствующими идентификаторами пользователей, групп и диапазонами IP-адресов. Кроме этого VPN-концентратор должен быть сконфигурирован в качестве клиента сервера ACS, в противном случае он не сможет воспользоваться его сервисами. Принципы аутентификации пользователей на VPN-концентраторе:

• создаются два раздельных пула IP-адресов – один для удаленных пользователей, другой для удаленного управления сетью. Эти диапазоны будут использованы в правилах внутренних межсетевых экранов для ограничения доступа на основе принадлежности к различным группам пользователей:

– удаленные пользователи – 172.16.61.1-254;

– удаленные администраторы – 172.16.62.1–6;

• внутренняя аутентификация на VPN-концентраторе не используется, но должны быть созданы локальные группы и названия групп должны быть идентичны названиям групп на сервере ACS;

• очень важно понимать, что названия групп должны быть идентичны первому полю клиентских сертификатов OU, потому что VPN-концентратор получает информацию о членстве в группе именно из этого поля;

• идентичные названия групп также должны быть установлены на сервере Zone Labs Integrity, потому что различные политики персональных межсетевых экранов будут выдаваться на основе анализа членства в группах;

• для журналирования доступа через VPN используется RADIUS.

4.3.5. Настройки внутренних межсетевых экранов

Этот уровень контролирует сетевой доступ между внутренними зонами безопасности. Данные зоны были созданы для разделения внутренних ресурсов, на основе их уровня безопасности и важности информации, а также для управления потоками информации во внутренней сети компании. В качестве внутренних межсетевых экранов используется Cisco Secure PIX 535 с программным обеспечением PIX OS v.6.3.3. Два межсетевых экрана функционируют в режиме «горячего» резервирования (failover).

Характеристика Cisco PIX. Межсетевой экран PIX компании Cisco Systems относится к классу пакетных фильтров, использующих технологию контроля состояния (stateful inspection). Он позволяет контролировать доступ как из Интернета во внутреннюю сеть, так и наоборот.

Для настройки PIX можно использовать графическую оболочку Cisco PDM v.3.0, что облегчает и упрощает этот процесс. В отличие от обычных пакетных фильтров с помощью PIX можно осуществлять аутентификацию пользователей. Для этого используются протоколы TACACS+ и RADIUS, которые позволяют применять для аутентификации как обычные UNIX-пароли, так и систему одноразовых паролей S/Key.

Cisco Secure PIX Firewall позволяет поддерживать до 500 тыс. одновременных TCP/IP-соединений и обеспечивать общую пропускную способность до 1700 Мбит/с. PIX

построен на базе сетевой операционной системы Cisco PIX OS, что гарантирует полную совместимость по протоколам и средствам мониторинга и управления с оборудованием Cisco, масштабируемость сетей, построенных на базе Cisco, привычный для администраторов Cisco-маршрутизаторов интерфейс.

Использование межсетевого экрана Cisco PIX позволяет обеспечить:

• управление информационными потоками на основе технологии контроля состояния защиты сетевых соединений, что позволяет ограничить доступ неавторизованных пользователей к сетевым ресурсам;

• аутентификацию пользователей с использованием стандартных протоколов TACACS+ и RADIUS;

• поддержку более 500 тыс. одновременных соединений;

• поддержку нескольких сетевых интерфейсов (интерфейсов демилитаризованной зоны) для организации открытых для пользователей интернет-сервисов типа WWW, электронной почты и др.;

• поддержку протокола Oracle SQLfNet для защиты приложений «клиент-сервер»;

• дублирование и «горячее» резервирование;

• трансляцию сетевых адресов (NAT) согласно RFC 1631;

• трансляцию портов (PAT), позволяющую расширить пул адресов компании: через один IP-адрес можно отображать 64 тыс. адресов (16 384 одновременно);

• отображение перекрывающихся IP-адресов в одно адресное пространство с помощью псевдонимов сетевых адресов;

• возможность отмены режима трансляции адресов для зарегистрированных IP-адресов, что позволяет пользователям использовать их настоящие адреса;

• прозрачную поддержку всех распространенных TCP/IP-сервисов – WWW, FTP, Telnet и т. д.;

• поддержку мультимедийных типов данных с использованием трансляции адресов и без нее, включая Progressive Networks\' RealAudio, Xing Technologies\' Streamworks, White Pines\' CuSeeMe, Vocal Tec\'s Internet Phone, VDOnet\'s VDOLive, Microsoft\'s NetShow, VXtreme\'s Web Theater 2;

• поддержку приложений для работы с видеоконференциями, совместимыми с H.323 спецификацией, включая Internet Video Phone (Intel) и Net-Meeting (Microsoft);

• возможность фильтрации потенциально опасных Java-апплетов;

• поддержку нескольких уровней входа в систему;

• поддержку прерываний (trap) SNMP-протокола;

• протоколирование и регистрацию сетевой активности;

• поддержку Management Information Base (MIB) для syslog;

• аудит использования URL и обменов по FTP-протоколу;

• поддержку удаленного вызова процедур (RPC);

• защиту от SYN-атак, ограждающую хост от атак типа «отказ в обслуживании».

В основе работы PIX лежит алгоритм адаптивной защиты (ASA), который обеспечивает защиту соединений с контролем состояния. Межсетевой экран PIX Firewall обеспечивает высокий уровень безопасности при использовании ASA. Каждый раз при установлении соединения наружу или вовнутрь через PIX Firewall информация о соединении сохраняется в таблице, которая содержит адреса источника и получателя, номера портов, информацию о TCP-последовательностях и дополнительные флаги сессии, такие, как SYN, ACK, FIN. Эта информация о сессии составляет так называемый «объект-соединение». Весь трафик данного соединения сверяется с данным объектом. Этот объект существует до завершения соединения.

Для безопасности ASA использует и содержит адреса источника и получателя, номера портов, информацию о TCP-последовательностях и дополнительные флаги сессии, а также результат применения хеш-функции к заголовку IP-пакета. Это хеширование является своего рода подписью клиента, установившего соединение, – данный код однозначно

идентифицирует клиента. Таким образом, для подмены клиента злоумышленникам необходимо получить не только IP-адрес машины, но и номера портов, дополнительные флаги сессии, а также номер TCP-последовательности. Последнее – невозможно, так как межсетевой экран PIX Firewall создает случайные номера TCP-последовательности для каждой сессии. Межсетевой экран PIX Firewall поддерживает аутентификацию и авторизацию с использованием сквозного механизма cut-through proxy, а также учет с использованием системного журнала и PIX Device Manager.

Высокая скорость работы межсетевого экрана PIX Firewall обеспечивается за счет cut-through proxy. В отличие от обычных proxy-серверов, которые анализируют каждый пакет на уровне приложений согласно семиуровневой модели OSI (что отнимает много времени и ресурсов процессора), PIX запрашивает у сервера TACACS+ или RADIUS информацию для аутентификации. Когда пользователь ввел свое имя и PIX проверил права доступа, образуется прямое соединение между сторонами и контролируется только состояние сессии. Таким образом, производительность PIX благодаря сквозным proxy много выше, чем у обычных proxy-серверов.

Еще одним фактором, который замедляет работу обычного proxy-сервера является то, что для каждой TCP-сессии последний должен запустить отдельный процесс. Если работают 300 пользователей, должно быть запущено 300 процессов, а эта процедура занимает значительные ресурсы процессора. PIX может поддерживать более 500 тыс. сессий одновременно.

Для обеспечения аутентификации пользователей межсетевой экран Cisco PIX Firewall использует механизм cut-through proxy. Данный механизм позволяет обеспечить:

• высокую пропускную способность;

• аутентификацию и авторизацию пользователей на прикладном уровне;

• возможность использования как TACACS+, так и RADIUS-сервера безопасности;

• аутентификацию как входящих, так и исходящих соединений.

Механизм cut-through межсетевого экрана PIX Firewall начинает свою работу на прикладном уровне как proxy-сервер. Но как только пользователь аутентифицирован с помощью стандартной базы данных, построенной либо на TACACS+, либо на RADIUS, и проведена проверка политики, межсетевой экран PIX Firewall возвращает поток данных на сетевой уровень. Этот механизм обеспечивает значительное увеличение производительности без уменьшения уровня безопасности. Для гарантирования такой возможности не требуется никакого дополнительного программного обеспечения на машине клиента. Механизм cut-through proxy работает следующим образом:

• пользователь выполняет попытку доступа к ресурсам, как будто он не находится за межсетевым экраном PIX Firewall;

• межсетевой экран PIX Firewall прерывает запрос на соединение и удостоверяется, что это новое соединение (оно отсутствует в списке уже установленных соединений);

• межсетевой экран PIX Firewall посылает запрос пользователю на ввод имени пользователя и пароля. Полученные имя и пароль межсетевой экран PIX Firewall передает серверу безопасности для проверки пользовательских привилегий. Поддерживается работа как с TACACS+, так и с RADIUS-серверами. Межсетевой экран PIX Firewall аутентифицирует следующие виды трафика: Telnet, FTP и HTTP;

• в случае успешной аутентификации межсетевой экран PIX Firewall инициирует соединение с запрашиваемым ресурсом;

• межсетевой экран PIX Firewall возвращает поток данных сессии на сетевой уровень, в высокоскоростное ядро сетевого уровня, и после этого весь трафик проходит непосредственно между источником и получателем.

Имена интерфейсов и уровни безопасности. Каждый интерфейс должен иметь имя и уровень безопасности. Уровни безопасности определяют доступ между системами, расположенными за различными интерфейсами. В компании используется следующая схема наименования и распределения уровней безопасности (см. табл. 4.5). Таблица 4.5.

Наименование и распределение уровней безопасности

Устройство	Имя интерфейса	Уровень безопасности	IP-адрес
PIX1	AdminDMZ	0	172.16.1.1/28
	WebDMZ	10	172.16.3.1/24
	ServiceDMZ	20	172.16.4.1/24
	SecureData	60	172.16.5.1/24
	Management	80	172.16.6.1/24
	Internal	100	172.16.9.1/28
	State	40	172.16.1.65/30
PIX2	AdminDMZ	0	172.16.1.2/28
	WebDMZ	10	172.16.3.2/24
	ServiceDMZ	20	172.16.4.2/24
	SecureData	60	172.16.5.2/24
	Management	80	172.16.6.2/24
	Internal	100	172.16.9.2/28
	State	40	172.16.1.65/30

Конфигурирование уровней безопасности и имен на каждом интерфейсе:

...
nameif ethernet0 AdminDmz security0
nameif ethernetl WebDMZ securityl0
nameif ethernet2 ServiceDMZ security20
nameif ethernet3 SecureData security60
nameif ethernet4 Management security80
nameif ethernet5 Internal security 100
nameif ethernet6 State security40

Интерфейс State используется только для обеспечения режима failover. Команды настройки маршрутизации здесь не показаны. *Пароли:*

...
enable password GHjiiuUIIH67JH encrypted
passwd Huhu&*8h9h encrypted

Конфигурирование NAT. Внутренние межсетевые экраны не используют трансляцию адресов, но таблица трансляции адресов NAT все же требуется для организации доступа в подсети с разными уровнями безопасности. Команда global не используется, так как реальной трансляции не происходит. Для разрешения доступа через интерфейс с низким уровнем безопасности со стороны интерфейсов с более высоким уровнем безопасности используется команда nat. Эта команда применяется только на тех интерфейсах, компьютерам которых требуется доступ к компьютерам, находящимся за интерфейсами с меньшим уровнем безопасности:

...
nat (internal) 0 172.16.16.0. 255.255.248.0
nat (internal) 0 172.16.32.0. 255.255.224.0
nat (Management) 0 172.16.6.0. 255.255.255.0
nat (SecureData) 0 172.16.5.0. 255.255.255.0

Для обеспечения доступа из интерфейсов с более высоким уровнем безопасности используется команда static:

...

static (Management, AdminDMZ) 172.16.6.0 172.16.6.0 netmask 255.255.255.0
static (Management, WebDMZ) 172.16.6.0 172.16.6.0 netmask 255.255.255.0
static (Management, ServiceDMZ) 172.16.6.0 172.16.6.0 netmask 255.255.255.0
static (Management, SecureData) 172.16.6.0 172.16.6.0 netmask 255.255.255.0
static (SecureData, WebDMZ) 172.16.5.0 172.16.5.0 netmask 255.255.255.0
static (Internal, Management) 172.16.16.0 172.16.16.0 netmask 255.255.248.0
static (Internal, ServiceDMZ) 172.16.16.0 172.16.16.0 netmask 255.255.248.0

Конфигурация списков контроля доступа. Для прохождения трафика необходимо сконфигурировать списки контроля доступа для каждого интерфейса.

Межсетевые экраны PIX отличаются от Check Point тем, что требуют создания списков контроля доступа для каждого интерфейса. Используется табл. 4.6.

Таблица 4.6. Списки контроля доступа

Источник	IP-источника	Получатель	IP-получателя	Сервис
AdminDMZ				
Административные интерфейсы proxy-серверов	172.16.1.8/30	Cisco SIMS	172.16.6.25/32	Syslog (UDP 514)
Административные интерфейсы балансировщиков нагрузки	172.16.1.12/30	Cisco SIMS	172.16.6.25/32	Syslog (UDP 514)
Внешние межсетевые экраны	172.16.1.4/30	Консоль Check Point	172.16.6.13/32	FW1-Out, UDP 259
Пограничные маршрутизаторы	70.70.70.16/30	HPOV	172.16.6.33/32	SNMP-Trap (UDP 162)
Административные интерфейсы внешних межсетевых экранов	172.16.1.4/30	HPOV	172.16.6.33/32	SNMP-Trap (UDP 162)
Административные интерфейсы proxy-серверов	172.16.1.8/30	HPOV	172.16.6.33/32	SNMP-Trap (UDP 162)
Административные интерфейсы балансировщиков нагрузки	172.16.1.12/30	HPOV	172.16.6.33/32	SNMP-Trap (UDP 162)
Пограничные маршрутизаторы	70.70.70.16/30	Сервер времени	172.16.6.41/32	NTP (UDP 123)
Административные интерфейсы внешних межсетевых экранов	172.16.1.4/30	Сервер времени	172.16.6.41/32	NTP (UDP 123)
Административные интерфейсы proxy-серверов	172.16.1.8/30	Сервер времени	172.16.6.41/32	NTP (UDP 123)
Административные интерфейсы балансировщиков нагрузки	172.16.1.12/30	Сервер времени	172.16.6.41/32	NTP (UDP 123)
Пограничные маршрутизаторы	70.70.70.16/30	Сервер Cisco ACS	172.16.6.21/32	TACACS+(TCP 49)

Продолжение табл. 4.6

Источник	IP-источника	Получатель	IP-получателя	Сервис
WebDMZ				
Серверы промежуточного уровня	172.16.3.64/29	Файл-серверы	172.16.5.32/30	CIFS (TCP 445)
Серверы промежуточного уровня	172.16.3.64/29	DNS-серверы	172.16.5.52/30	DNS (TCP/UDP 53)
Серверы промежуточного уровня	172.16.3.64/29	Контроллеры домена	172.16.5.48/30	IKE (UDP 500)
Серверы промежуточного уровня	172.16.3.64/29	Контроллеры домена	172.16.5.48/30	AH (IP 51)
Web-ферма 1	172.16.3.16/29	DNS-серверы	172.16.5.52/30	DNS (TCP/UDP 53)
Web-ферма 1	172.16.3.16/29	Контроллеры домена	172.16.5.48/30	IKE (UDP 500)
Web-ферма 1	172.16.3.16/29	Контроллеры домена	172.16.5.48/30	AH (IP 51)
Web-ферма 2	172.16.3.24/29	DNS-серверы	172.16.5.52/30	DNS (TCP/UDP 53)
Web-ферма 2	172.16.3.24/29	Контроллеры домена	172.16.5.48/30	IKE (UDP 500)
Web-ферма 2	172.16.3.24/29	Контроллеры домена	172.16.5.48/30	AH (IP 51)
Web-серверы демилитаризованной зоны	172.16.3.0/24	HPOV	172.16.6.33/32	SNMP-Trap (UDP 162)
Web-серверы демилитаризованной зоны	172.16.3.0/24	Cisco VMS 2.2	172.16.6.9/32	SSL (TCP 443)
Web-серверы демилитаризованной зоны	172.16.3.0/24	Сеть данных	172.16.5.0/24	ICMP source-quench
ServiceDMZ				
Proxy-серверы	172.16.4.104/30	SIMS	172.16.6.25/32	Syslog (UDP 514)
Шлюзы VPN	172.16.4.117/32	SIMS	172.16.6.25/32	Syslog (UDP 514)
Удаленные пользователи VPN	172.16.61.0/24	Внутренний сервер OWA	172.16.17.54/32	HTTPS (TCP 443)
Удаленные пользователи VPN	172.16.61.0/24	Внутренние файл- и принт-серверы	172.16.17.32/29	HTTP (TCP 80)

Продолжение табл. 4.6

Источник	IP-источника	Получатель	IP-получателя	Сервис
Удаленные пользователи VPN	172.16.61.0/24		172.16.17.32/29	HTTPS (TCP 443)
Удаленные администраторы VPN	172.16.62.0/29	Терминальный сервер	172.16.6.45/32	SSH (TCP 22)
Удаленные администраторы VPN	172.16.62.0/29	Консоль Check Point	172.16.6.13/32	CPMI (TCP 18190)
Удаленные администраторы VPN	172.16.62.0/29	Сервер управления	172.16.6.0/24	MS-RDP (TCP 3389)
Шлюзы VPN	172.16.4.117/32	Центр сертификатов	172.16.6.17/32	LDAP (TCP 389)
Шлюзы VPN	172.16.4.117/32	Сервер Cisco ACS	172.16.6.21/32	RADIUS (UDP 1645 и 1646)
Шлюзы VPN	172.16.4.117/32	Zone Labs Integrity	172.16.6.29/32	Tcp 5054
Компьютеры	172.16.4.0/24	HPOV	172.16.6.33/32	SNMP-Trap (UDP 162)
Компьютеры	172.16.4.0/24	Сервер времени	172.16.6.41/32	NTP (UDP 132)
SecureData				
Контроллеры домена	172.16.5.48/30	Серверы промежуточного уровня	172.16.3.64/29	IKE (UDP 500)
Контроллеры домена	172.16.5.48/30	Серверы промежуточного уровня	172.16.3.64/29	AH (IP 51)
Контроллеры домена	172.16.5.48/30	Web-ферма 1	172.16.3.16/29	IKE (UDP 500)
Контроллеры домена	172.16.5.48/30	Web-ферма 1	172.16.3.16/29	AH (IP 51)
Контроллеры домена	172.16.5.48/30	Web-ферма 2	172.16.3.24/29	IKE (UDP 500)
Контроллеры домена	172.16.5.48/30	Web-ферма 2	172.16.3.24/29	AH (IP 51)
Контроллеры домена	172.16.5.48/30	Сервер времени	172.16.6.41/32	NTP (UDP 132)
DNS-серверы	172.16.5.52/30	Шлюзы DNS демилитаризованной зоны	172.16.4.112/30	DNS (TCP/UDP 53)
Сеть данных	172.16.5.0/24	HPOV	172.16.6.33/32	SNMP-Trap (UDP 162)

Окончание табл. 4.6

Источник	IP-источника	Получатель	IP-получателя	Сервис
Сеть данных	172.16.5.0/24	Web-серверы демилитаризованной зоны	172.16.2.0/24	ICMP source-quench
Management				
HPOV	172.16.6.33/32	Внутренняя сеть	172.16.0.0/16	SNMP (UDP 161)
HPOV	172.16.6.33/32	Пограничные маршрутизаторы	70.70.70.16/30	SNMP (UDP 161)
Сеть управления	172.16.6.0/24	Балансировщики нагрузки, proxy-серверы	172.16.1.8/22	SSH (TCP 22)
Сеть управления	172.16.6.0/24	Компьютеры зоны ServiceDMZ	172.6.4.96/27	SSH (TCP 22)
Сеть управления	172.16.6.0/24	Web-серверы демилитаризованной зоны	172.16.3.0/24	MS-RDP (TCP 3389)
Сеть управления	172.16.6.0/24	DNS-серверы зоны ServiceDMZ	172.16.4.112/30	MS-RDP (TCP 3389)
Сеть управления	172.16.6.0/24	Компьютеры зоны данных	172.16.5.0/24	MS-RDP (TCP 3389)
Сеть управления	172.16.6.0/24	Внутренние серверы	172.16.16.16/21	MS-RDP (TCP 3389)
Консоль Check Point	172.16.6.13/32	Внешние межсетевые экраны	172.16.1.4/30	FW1-ln (UDP 259)
Internal				
Клиентские подсети	172.16.32.0/19	Proxy-серверы DMZ	172.16.4.104/30	TCP 8080
Exchange Cluster IP	172.16.17.46/32	SMTP-шлюзы	172.16.4.108/30	SMTP (TCP 25)
Внутренние DNS	172.16.17.20/30	DNS-форвардеры	172.16.4.112/30	DNS (TCP/UDP 53)
Серверы управления контентом	172.16.16.16/21	HPOV	172.16.6.33/32	SNMP-Trap (UDP 162)
Внутренние контроллеры домена	172.16.17.16/30	Сервер времени	172.16.6.41/32	NTP (UDP 123)

Turbo ACL. Для ускорения обработки списков контроля доступа используется возможность PIX по компилированию списков контроля доступа. Включается эта возможность следующей командой: access-list compiled

Группирование объектов. Возможность группирования объектов PIX позволяет улучшить читабельность списков контроля доступа, ускорить создание похожих записей в списках контроля доступа:

...

object-group network WebDMZServers
network-object 172.16.3.16 255.255.255.248
network-object 172.16.3.24 255.255.255.248
network-object 172.16.3.64 255.255.255.248
object-group network AdminDMZNet
network-object 70.70.70.16 255.255.255.252
network-object 172.16.1.8 255.255.255.248
object-group network AdminDMZAll network-object 172.16.1.4 255.255.255.252
group-object AdminDMZNet

object-group network WindowsTS group-object WebDMZServers
network-object 172.16.4.112 255.255.255.252
network-object 172.16.5.0 255.255.255.0
network-object 172.16.16.16 255.255.248.0
object-group service FW1-In tcp port-object eq 256
port-object eq 258
port-object eq 18191
port-object eq 18192
port-object eq 18211
object-group service FW1-Out tcp port-object eq 256
port-object eq 257
port-object eq 18210

Списки контроля доступа для интерфейса AdminDMZ:

...

access-list AdminDMZ-ACL permit udp object-group AdminDMZNet host 172.16.6.25 eq514
access-list AdminDMZ-ACL permit top 172.16.1.4 255.255.255.252 host 172.16.6.13 object-group FWl-Out
access-list AdminDMZ-ACL permit udp 172.16.1.4 255.255.255.252 host 172.16.6.13 eq 259
access-list AdminDMZ-ACL permit udp object-group AdminDMZAll host 172.16.6.33 eql62
access-list AdminDMZ-ACL permit udp object-group AdminDMZAll host 172.16.6.41 eql23
access-list AdminDMZ-ACL permit top 70.70.70.16 255.255.255.252 host 172.16.6.21 eq 49
access-list AdminDMZ-ACL deny ip any any

Списки контроля доступа для интерфейса WebDMZ:

...

access-list WebDMZ-ACL permit top 172.16.3.64 255.255.255.248 host 172.16.5.30 eq 2002
access-list WebDMZ-ACL permit top 172.16.3.64 255.255.255.248172.16.5.32 255.255.255.252 eq 445
access-list WebDMZ-ACL permit udp object-group WebDMZServers 172.16.5.52 255.255.255.252 eq 53
access-list WebDMZ-ACL permit tcp object-group WebDMZServers 172.16.5.52 255.255.255.252 eq 53
access-list WebDMZ-ACL permit udp object-group WebDMZServers 172.16.5.48 255.255.255.252 eq 500
access-list WebDMZ-ACL permit ah object-group WebDMZServers 172.16.5.48 255.255.255.252
access-list WebDMZ-ACL permit udp object-group WebDMZServers host 172.16.6.33 eql62
access-list WebDMZ-ACL permit top 172.16.3.16 255.255.255.240 host 172.16.6.9 eq443
access-list WebDMZ-ACL permit icmp object-group WebDMZServers 172.16.5.0 255.255.255.0 source-quench

access-list WebDMZ-ACL deny ip any any

Списки контроля доступа для интерфейса ServiceDMZ:

...

access-list ServiceDMZ-ACL permit tcp 172.16.4.108 255.255.255.252 host 172.16.17.46 eq 25

access-list ServiceDMZ-ACL permit udp 172.16.4.104 255.255.255.252 host 172.16.6.25 eq 514

access-list ServiceDMZ-ACL permit udp host 172.16.4.117 host 172.16.6.25 eq 514

access-list ServiceDMZ-ACL permit tcp 172.16.61.0 255.255.255.0 host 172.16.17.54 eq 443

access-list ServiceDMZ-ACL permit tcp 172.16.62.0 255.255.255.248 host 172.16.17.54 eq 443

access-list ServiceDMZ-ACL permit tcp 172.16.61.0 255.255.255.0 172.16.17.32 255.255.255.248 eq 80

access-list ServiceDMZ-ACL permit tcp 172.16.62.0 255.255.255.248 172.16.17.32 255.255.255.248 eq 80

access-list ServiceDMZ-ACL permit tcp 172.16.61.0 255.255.255.0 172.16.17.32 255.255.255.248 eq 443

access-list ServiceDMZ-ACL permit tcp 172.16.62.0 255.255.255.248 172.16.17.32 255.255.255.248 eq 443

access-list ServiceDMZ-ACL permit tcp 172.16.62.0 255.255.255.248 host 172.16.6.45 eq 22

access-list ServiceDMZ-ACL permit tcp 172.16.62.0 255.255.255.248 host 172.16.6.13 eq 18190

access-list ServiceDMZ-ACL permit tcp 172.16.62.0 255.255.255.248 172.16.6.0 255.255.255.0 eq 3389

access-list ServiceDMZ-ACL permit tcp host 172.16.4.117 host 172.16.6.17 eq 389

access-list ServiceDMZ-ACL permit udp host 172.16.4.117 host 172.16.6.21 range 1645 1646

access-list ServiceDMZ-ACL permit tcp host 172.16.4.117 host 172.16.6.29 eq 5054

access-list ServiceDMZ-ACL permit udp 172.16.4.0 255.255.255.0 host 172.16.6.33 eq 162

access-list ServiceDMZ-ACL permit udp 172.16.4.0 255.255.255.0 host 172.16.6.41 eq 123

access-list ServiceDMZ-ACL deny ip any any

Списки контроля доступа для интерфейса SecureData:

...

access-list SecureData-ACL permit udp 172.16.5.48 255.255.255.252 object-group WebDMZServers eq 500

access-list Secure Data-ACL permit ah 172.16.5.48 255.255.255.252 object-group WebDMZServers

access-list Secure Data-ACL permit udp 172.16.5.48 255.255.255.252 host 172.16.6.41 eq 123

access-list SecureData-ACL permit udp 172.16.5.52 255.255.255.252 172.16.4.112 255.255.255.252 eq 53

access-list SecureData-ACL permit tcp 172.16.5.52 255.255.255.252 172.16.4.112

255.255.255.252 eq 53

access-list SecureData-ACL permit udp 172.16.5.0 255.255.255.0 host 172.16.6.33 eq 162

access-list WebDMZ-ACL permit icmp 172.16.5.0 255.255.255.0 172.16.3.0 255.255.255.0 source-quench

access-list SecureData-ACL deny ip any any

Списки контроля доступа для интерфейса Management:

...

access-list Management-ACL permit udp host 172.16.6.33 172.16.0.0 255.255.0.0 eq 161

access-list Management-ACL permit udp host 172.16.6.33 70.70.70.16 255.255.255.252 eq 161

access-list Management-ACL permit tcp 172.16.6.0 255.255.255.0 172.16.1.8 255.255.255.248 eq 22

access-list Management-ACL permit tcp 172.16.6.0 255.255.255.0 172.16.4.96 255.255.255.224 eq 22

access-list Management-ACL permit tcp 172.16.6.0 255.255.255.0 object-group WindowsTS eq 3389

access-list Management-ACL permit tcp host 172.16.6.13 172.16.1.4 255.255.255.252 object-group FWl-In

access-list Management-ACL permit udp host 172.16.6.13 172.16.1.4 255.255.255.252 eq 259

access-list Management-ACL deny ip any any

Списки контроля доступа для интерфейса Internal:

...

access-list Internal-ACL permit tcp 172.16.32.0 255.255.224.0 172.16.4.104 255.255.255.252 eq 8080

access-list Internal-ACL permit tcp host 172.16.17.46 172.16.4.108 255.255.255.252 eq 25

access-list Internal-ACL permit udp 172.16.17.20 255.255.255.252 172.16.4.112 255.255.255.252 eq 53

access-list Internal-ACL permit tcp 172.16.17.20 255.255.255.252 172.16.4.112 255.255.255.252 eq 53

access-list Internal-ACL permit tcp 172.16.35.0 255.255.255.248 host 172.16.5.30 eq 2002

access-list Internal-ACL permit tcp 172.16.36.0 255.255.255.248 172.16.5.32 255.255.255.252 eq 445

access-list Internal-ACL permit udp 172.16.16.16 255.255.248.0 host 172.16.6.33 eq 162

access-list Internal-ACL permit udp 172.16.17.16 255.255.255.252 host 172.16.6.41 eq 123

access-list Internal-ACL deny ip any any

Включение списков контроля доступа:

...

access-group AdminDMZ-ACL in interface AdminDMZ

access-group WebDMZ-ACL in interface WebDMZ

access-group ServiceDMZ-ACL in interface ServiceDMZ

access-group SecureData-ACL in interface SecureData

access-group Management-ACL in interface Management
access-group Internal-ACL in interface Internal

Настройка TACACS+. TACACS+ используется для централизованного управления аутентификацией и авторизацией доступа к межсетевым экранам. Определяем IP-адрес сервера TACACS+ и пароль для аутентификации:

...
aaa-server TACACS+ (Management) host 172.16.6.21 F$!19Ty timeout 5

Используемый метод аутентификации применяется для консольного доступа:

...
aaa authentication serial console TACACS+

Предупреждающий баннер:

...
banner login «This is a private computer system for authorized use only.
All access is logged and monitored. Violators could be prosecuted».

«Ежедневное» сообщение, выводимое в первую очередь при попытке получения доступа к межсетевому экрану:

...
banner motd «This is a private computer system for authorized use only.
All access is logged and monitored. Violators could be prosecuted».

Сообщение, выводимое при входе в непривилегированный (EXEC) режим:

...
banner exec «Any unauthorized access will be vigorously prosecuted».

Настройка встроенной системы IDS. Cisco PIX имеет встроенную систему обнаружения вторжений. Хотя по количеству сигнатур система уступает устройствам серии Cisco IDS 4200, все же имеет смысл сконфигурировать ее для отсылки сообщений в случае атак:

...
ip audit info action alarm
ip audit attack action alarm

Защита системы аутентификации. Для защиты от атак на переполнение системы аутентификации используется следующая опция:

...

floodguard enable

Защита от атак с подменой адреса. Для защиты от атак с подменой адреса используется возможность проверки правильности адреса отправителя uRPF:

...

ip verify reverse-path interface AdminDmz
ip verify reverse-path interface WebDMZ
ip verify reverse-path interface ServiceDMZ
ip verify reverse-path interface SecureData
ip verify reverse-path interface Management
ip verify reverse-path interface Internal

Конфигурирование межсетевых экранов PIX для работы в режиме горячего резервирования. Настройка осуществляется следующим образом:

1. Выключить резервный межсетевой экран.
2. Синхронизировать время на обоих межсетевых экранах:

...

ntp authentication-key 1 md5 For$Ntp
ntp authenticate
ntp trusted-key 1
ntp server 172.16.6.41 key 1 source Management

3. Подключить failover-кабель к обоим межсетевым экранам.
4. Необходимо сконфигурировать только основной межсетевой экран.
5. В отличие от VRRP или HSRP Cisco PIX не требует дополнительного IP-адреса для режима failover.
6. Включить режим failover:

...

failover
failover link State

7. Определить IP-адреса для интерфейсов:

...

failover ip address AdminDMZ 172.16.1.2
failover ip address WebDMZ 172.16.3.2
failover ip address ServiceDMZ 172.16.4.2
failover ip address SecureData 172.16.5.2
failover ip address Management 172.16.6.2
failover ip address Internal 172.16.9.2
failover ip address State 172.16.1.66

8. Включить резервный межсетевой экран. Проверить функционирование.

Дополнительные настройки безопасности. С целью ограничения доступа и

использования защищенного протокола для управления сконфигурирован SSH. Для этого сначала создается пара ключей:

```
...
ca generate rsa key 1024
ca save all
```

Далее отключается Telnet:

```
...
ssh 172.16.6.0 255.255.255.0 Management
ssh timeout 15
no telnet
```

Журналирование событий межсетевого экрана. Журналирование событий межсетевого экрана является критически важным для надежного функционирования сети. Межсетевые экраны сконфигурированы для отправки сообщений на сервер Cisco SIMS:

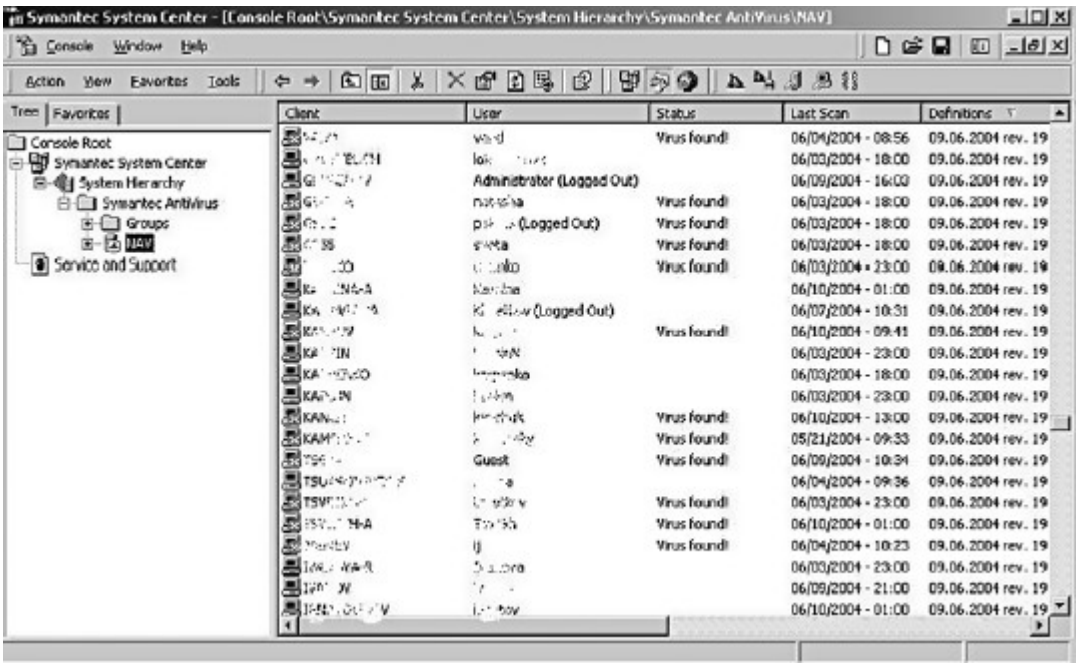
```
...
logging buffered warnings
logging host Management 172.16.6.25
logging trap informational
logging timestamp
logging on
```

Конфигурирование SNMP. Межсетевой экран конфигурируется для отправки trap только к SNMP-серверу:

```
...
snmp-server community TopoE6?%HU
snmp-server host 172.16.6.33 Management trap
snmp-server enable traps
logging on
```

4.3.6. Настройка корпоративной системы защиты от вирусов

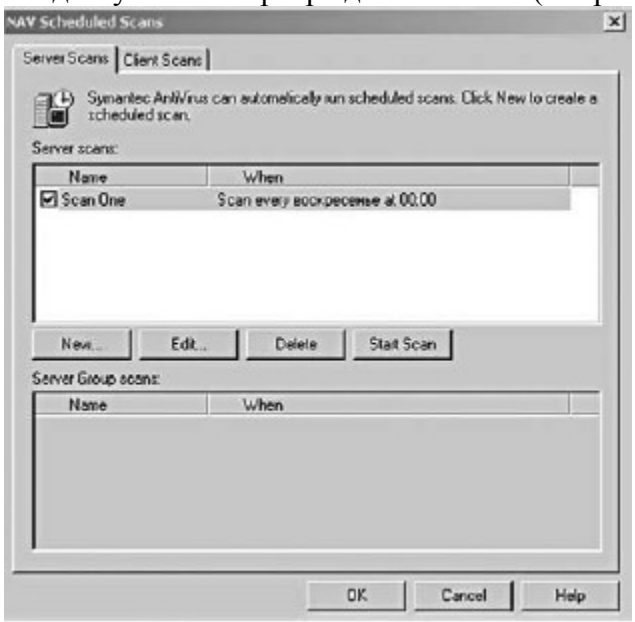
Все серверы и рабочие станции внутренней сети компании защищены с помощью Symantec Antivirus Corporate Edition v.8.1. Политики управляются централизованно с использованием Symantec System Center (см. рис. 4.11).



...

Рис. 4.11. Symantec System Center

Сканирование самого антивирусного сервера осуществляется в нерабочий день (воскресенье) для увеличения доступности сервера для клиентов (см. рис. 4.12).



...

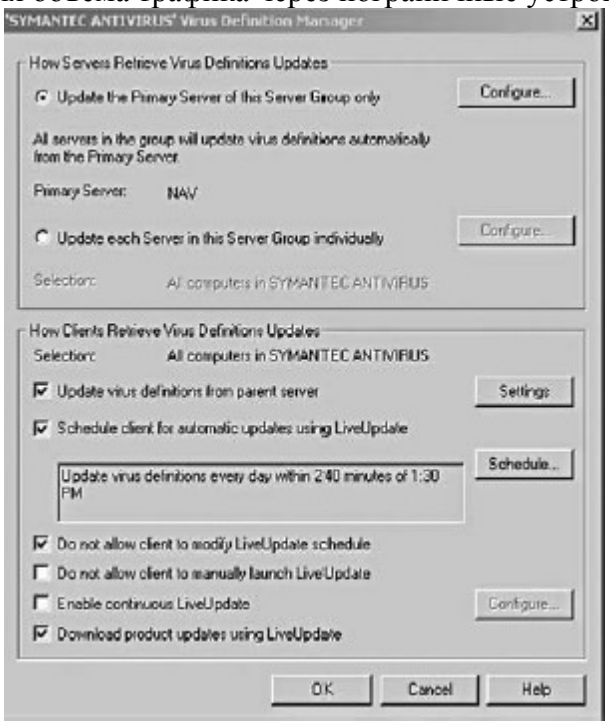
Рис. 4.12. Сканирование антивирусного сервера

Сканирование клиентов осуществляется один раз в неделю (см. рис. 4.13).

...

Рис. 4.13. Сканирование клиентов

Все обновления загружаются на сервер и только потом устанавливаются на клиентов. Это сделано для уменьшения объема трафика через пограничные устройства (см. рис. 4.14).

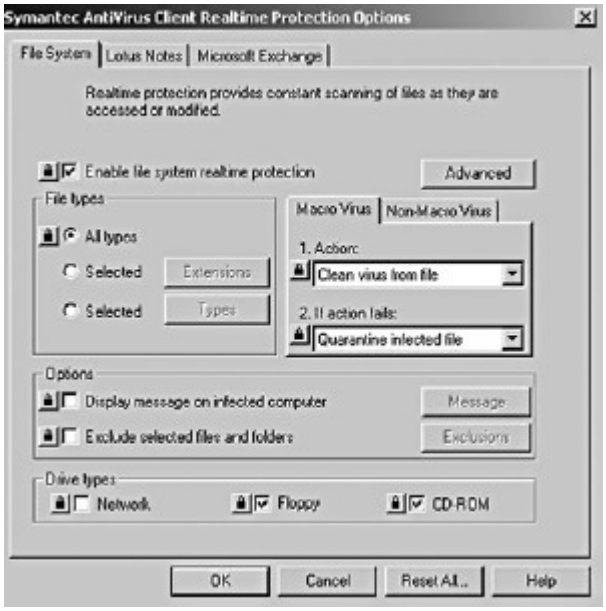


...

Рис. 4.14. Загрузка обновлений на сервер

Для увеличения защищенности клиентов включена опция Real-time protection и проверяются все типы файлов на наличие вирусов, в том числе на FDD и CD-ROM (см. рис.

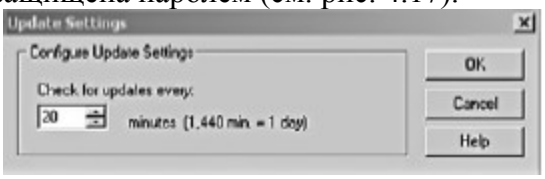
4.15).



...

Рис. 4.15. Проверка файлов на наличие вирусов

Наличие обновлений проверяется каждые 20 минут (см. рис, 4.16). Для предупреждения действий сотрудников, желающих отключить антивирусное программное обеспечение или удалить его, включена опция, запрещающая останавливать сервис, а возможность деинсталляции защищена паролем (см. рис. 4.17).



...

Рис. 4.16. Проверка наличия обновлений

...

Рис. 4.17. Запрещение остановки сервиса

4.4. Дальнейшие шаги по совершенствованию правил безопасности

Шаг 1. Производительность межсетевых экранов. Проверить, позволяет ли пропускная способность внешних межсетевых экранов обрабатывать весь объем трафика. Для увеличения пропускной способности можно мигрировать на схему Check Point Firewall-1 Clustering с модулем High Availability. Можно также использовать продукты для балансировки нагрузки межсетевых экранов таких фирм, как F5, Alteon, Foundry, Radware. Следует задать соответствующие правила безопасности.

Шаг 2. VPN-аутентификация. Хотя настроена двухфакторная IKE-аутентификация с использованием сертификатов, хранящихся на Aladdin eToken USB и Cisco ACS RADIUS, но все равно остается слабое звено в виде паролей пользователей. Чтобы избежать этого, можно использовать однократные пароли, такие, как RSA Security SecurlD. Cisco ACS легко интегрируется с этим продуктом. Необходимо определить правила безопасности.

Шаг 3. Избыточность Cisco ACS. Сервер Cisco ACS играет важную роль в аутентификации пользователей VPN. Хотя сервис функционирует на аппаратной платформе, поддерживающей полное резервирование, но все равно существует вероятность отказа. Поэтому рекомендуется установить второй сервер Cisco ACS и настроить репликацию конфигурации.

Шаг 4. Избыточность VPN-концентратора. Хотя в данный момент доступ через VPN не является критически важным, но при изменении этого требования может понадобиться покупка дополнительно концентратора. Если не будет возможности купить такую же модель, можно остановиться на модели Cisco VPN 3005 для первичной замены в случае выхода из строя основного концентратора. Следует задать правила безопасности.

Шаг 5. Избыточность сервера syslog. Сервер – центральная и единственная точка сбора всех журналов, и его доступность является критически важной для функционирования сети. Рекомендуется организовать кластеризацию программного обеспечения сервера и определить правила безопасности.

Шаг 6. Избыточность инфраструктуры компании. Для повышения отказо– и катастрофоустойчивости инфраструктуры компании рекомендуется создать резервный центр обработки данных и определить правила безопасности.

Приложение 1 ОЦЕНКА СОСТОЯНИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ В США

В начале 2005 года Институт компьютерной безопасности (Computer Security Institute, CSI) и Группа по компьютерным вторжениям отделения Федерального бюро расследований в Сан-Франциско (San Francisco Federal Bureau of Investigation\'s Computer Intrusion Squad) опубликовали очередное, девятое, исследование состояния информационной безопасности в США. Этот проект (www.GoCSI.com) является наиболее продолжительным в мире по времени по сравнению с аналогичными. Как изменилась динамика инцидентов в области информационной безопасности в 2004 году? Какие проблемы безопасности сегодня злободневны? Как эти проблемы безопасности проецируются на российские компании и организации? Далее представлены основные результаты исследования CSI/FBI2004 года и комментарии к ним.

Новые проблемы безопасности. Исследование CSI/FBI 2004 года наряду с хорошо известными техническими проблемами в области защиты информации выявило ряд новых проблем. К ним относятся:

• оценка требуемых затрат на защиту информации;

• оценка возврата инвестиций на защиту информации;

• определение потребностей в обучении по вопросам безопасности;

• расчет требуемого бюджета на защиту информации;

• оценка возможности аутсорсинга решения задач в области защиты информации;

• оценка влияния законодательных актов, и в частности закона Сарбейнса-Оксли 2002 года, на организацию режима информационной безопасности предприятия;

• оценка возможности внешнего страхования информационных рисков и роли аудита безопасности.

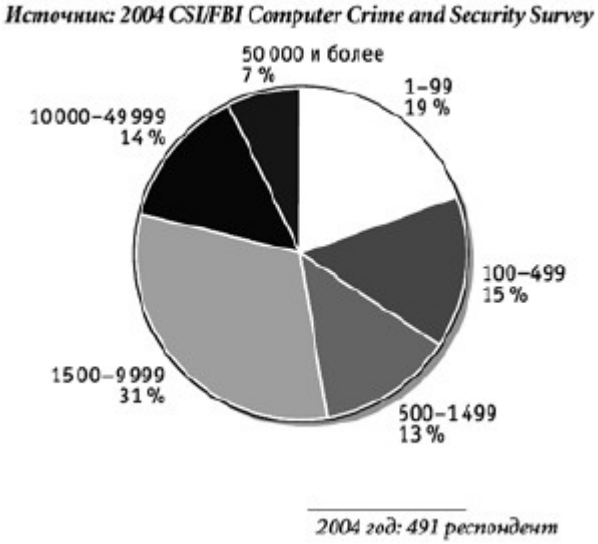
Интересно отметить, что все перечисленные проблемы так или иначе связаны с экономическими аспектами защиты информации, а также с вопросами управления информационными рисками, которые являются не менее актуальными и для российских компаний и организаций.

Состав респондентов. Результаты исследования CSI/FBI 2004 года основаны на ответах 494 респондентов из числа лиц, ответственных за организацию режима информационной безопасности на предприятии. Сводные данные по респондентам, представлявшим ведущие предприятия из различных отраслей экономики США, приведены на рис. П1.1-П1.4. Большая часть респондентов (см. рис. П1.1) была из финансового сектора экономики США (19 %), за ними следовали респонденты из области высоких технологий (13 %) и сферы производства (12 %). Респонденты из правительственных учреждений и организаций (на федеральном и местном уровне) составили 13 %, а на долю респондентов из учебных заведений пришлось только 7 %.

...

Рис. П1.1. Распределение респондентов по отраслям экономики США

По количеству сотрудников (см. рис. П1.2) лидируют предприятия и организации, насчитывающие от 1,5 тыс, до 9 999 работников (31 %), и с численностью сотрудников менее 100 работников (19 %). Предприятия и организации, насчитывающие 50 тыс, и более работников, составили 7 %.

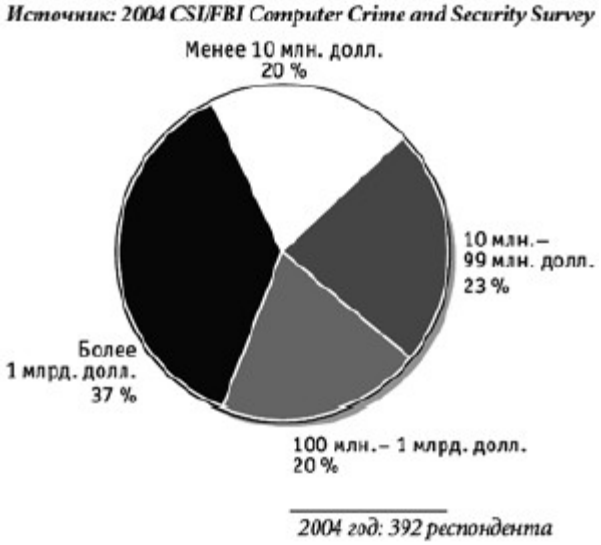


...

Рис. П1.2. Распределение респондентов по количеству сотрудников на предприятии

Данные по годовым доходам опрашиваемых предприятий и организаций представлены на рис. П1.3. Доход 57 % предприятий и организаций составил более 100 млн. долларов, включая 37 % организаций с доходом более 1 млрд. долларов. Доход 20 % предприятий и организаций составил менее 10 млн. долларов. Новыми для исследования 2004 года стали данные по занимаемым должностям респондентов на предприятии (см. рис. П1.4). Как оказалось, в исследовании приняло участие 18 % руководителей высшего эшелона управления предприятиями: 4 % респондентов – президенты компаний и учреждений (CEO),

8 % – начальники служб автоматизации (CIO) и 6 % – начальники служб информационной безопасности (CISO). Большая часть респондентов (53 %) оказалась представленной менеджерами безопасности предприятий (BISO) и/или техническими специалистами в области защиты информации. При этом 9 % респондентов занимали должность системного администратора, а 19 % – другие инженерные должности.



...

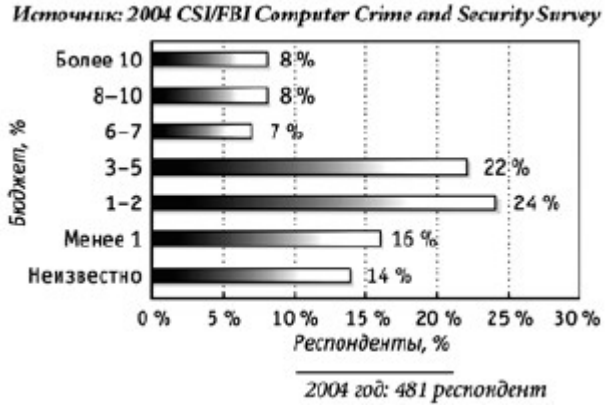
Рис. П1.3. Распределение респондентов по доходам предприятия

...

Рис. П1.4. Распределение респондентов по занимаемым должностям на предприятии

Бюджеты защиты информации. Исследование 2004 года коснулось вопроса планирования бюджета на защиту информации. Как видно на рис. П1.5, данные по бюджетам опрашиваемых предприятий и организаций на защиту информации распределились следующим образом: 46 % респондентов указали, что на защиту информации выделяется от 1 до 5 % от общего бюджета на информационные технологии; 16 % – менее 1 %; 23 % – более 5 % от бюджета на информационные технологии; 14 % респондентов указали, что

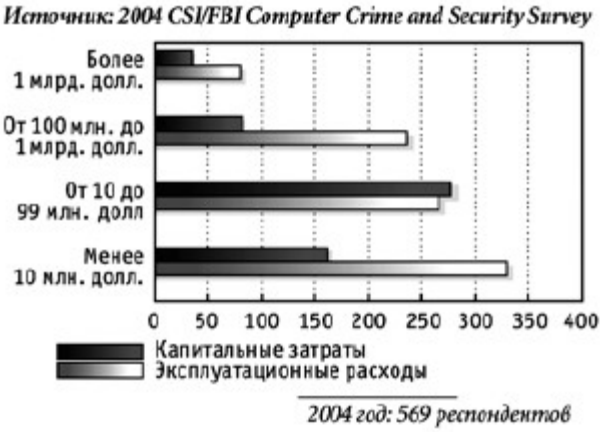
сумма бюджета на защиту информации им не известна.



...

Рис. П1.5. Планирование бюджета на защиту информации предприятия

Определение величины средних эксплуатационных расходов на защиту информации в пересчете на одного работника предприятия показало следующее (см. рис. П.1.6.). Как и следовало ожидать, подтвердилось предположение о том, что по мере роста доходов предприятий эксплуатационные и капитальные затраты на защиту информации растут менее быстрыми темпами. Например, компании с годовым оборотом менее 10 млн. долларов США тратят на одного сотрудника в среднем около 500 долларов (334 доллара эксплуатационных расходов и 163 доллара капитальных затрат), в то время как компании с годовым оборотом более 1 млрд. долларов тратят в среднем около 110 долларов на одного сотрудника (82 доллара эксплуатационных расходов и 30 долларов капитальных затрат).



...

Рис. П1.6. Средние затраты на защиту информации на одного сотрудника предприятия

Величины затрат на защиту информации в перерасчете на одного сотрудника предприятия по отраслям экономики США представлены на рис, П1.7. Как оказалось, самые большие затраты на защиту информации (608 долларов) на предприятиях транспорта (449 долларов эксплуатационных расходов и 159 долларов капитальных затрат на одного сотрудника). Далее по убыванию эксплуатационных расходов следует федеральное правительство (261 доллар), предприятия телекоммуникаций (209 долларов) и высоких

технологий (183 доллара). С точки зрения капитальных затрат на защиту информации в убывающем порядке места распределились следующим образом: в отрасли телекоммуникаций (150 долларов), в отрасли высоких технологий (83 доллара) и в федеральном правительстве (61 доллар).

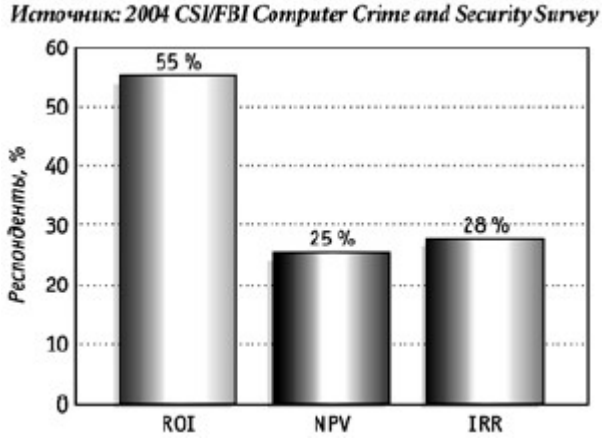
...

Рис. П1.7. Средние затраты на защиту информации на одного сотрудника предприятия по отраслям экономики США

Интересно отметить, что если федеральное правительство сообщило об одних из самых больших затратах на защиту информации на одного сотрудника, правительственные учреждения на местах тратят на одного сотрудника меньше всего (примерно 17 долларов), а правительства штатов по аналогичным затратам оказались где-то посередине (примерно 154 доллара).

На практике лицам, ответственным за организацию режима информационной безопасности, часто требуется обосновать бюджеты на создание и сопровождение корпоративной системы защиты информации. В академических кругах и во время проведения профессиональных форумов по безопасности, а также на страницах периодических изданий часто ведется дискуссия о целесообразности расчета экономических показателей эффективности инвестиций на защиту информации. Результаты исследования CSI/FBI 2004 года показали, что для определения эффективности инвестиций на защиту информации компании используют ряд экономических показателей, таких, как коэффициент возврата инвестиций (ROI или ROSI), показатели внутренней нормы доходности (IRR) и чистой текущей стоимости (NPV). Например, участников исследования 2004 года попросили обозначить по шкале из семи баллов готовность компаний использовать показатели ROI, IRR и NPV для количественной оценки экономической эффективности затрат на защиту информации. При этом ответы 1, 2 или 3 истолковывались как неготовность к использованию названных экономических показателей; ответ 4 – затруднение в ответах; ответ 5, 6 или 7 – готовность к использованию указанных показателей. Как оказалось (см. рис. П1.8), 55 % респондентов используют показатель ROI, 28 % – показатель IRR и 25 % – показатель NPV. Таким образом, показатель ROI при всех своих ограничениях по сравнению с NPV и IRR является наиболее популярным. Использование NPV и/или IRR вызывает

некоторое удивление, так как в периодической печати не раз заявлялось о малой пригодности методов традиционного экономического анализа в области защиты информации.

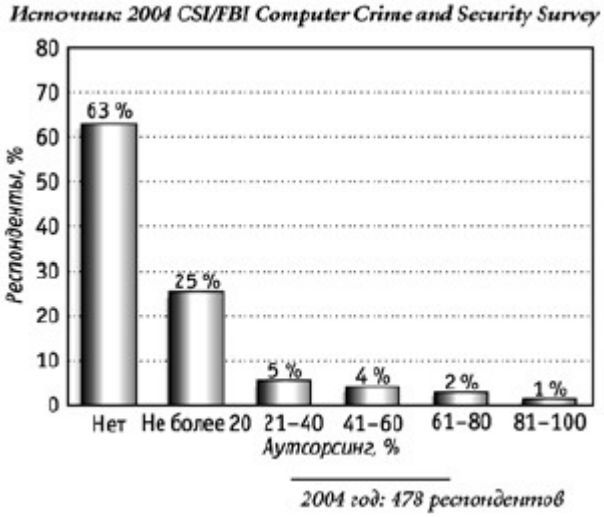


...

Рис. П1.8. Данные по использованию экономических показателей ROI, NPV и IRR

Исследование CSI/FBI 2004 года затронуло ряд новых проблем безопасности, в частности аутсорсинга работ по защите информации (подразумевающего передачу части функций по защите информации сторонним организациям), а также страхования остаточных информационных рисков предприятия.

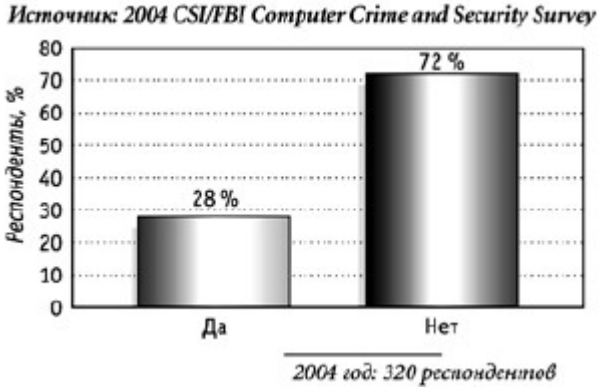
Текущее исследование показало, что аутсорсинг работ по защите информации не является столь широко распространенным явлением, как аутсорсинг работ в области традиционных информационных технологий. Лишь 12 % респондентов указали, что их организации передают сторонним организациям более 20 % функций безопасности (см. рис. П1.9). При этом 63 % респондентов указали, что их организации в настоящее время не занимаются и не планируют заниматься аутсорсингом функций безопасности. Достаточно интересно будет проследить динамику развития аутсорсинга функций безопасности в будущих исследованиях CSI/FBI.



...

Рис. П1.9. Данные по аутсорсингу функций безопасности

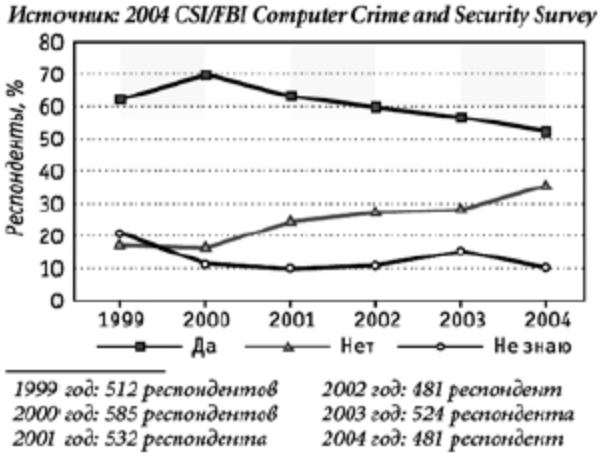
Как свидетельствует рис, П1.10, практика внешнего страхования остаточных информационных рисков также находится на этапе становления. Постепенно предприятия начинают понимать, что зрелость современных технологий защиты информации, таких, как антивирусная защита, защита от НСД, межсетевое экранирование и VPN, обнаружение вторжений и аномалий и пр., не могут полностью устранить информационные риски предприятия. Поэтому обращение к услугам внешнего страхования для покрытия остаточных информационных рисков и снижения прогнозируемых финансовых потерь выглядит вполне естественным шагом. Пока страховые компании не располагают представительными статистическими данными по инцидентам безопасности для обоснованного определения тарифов страхования информационных рисков, но уже пытаются предлагать страховые полисы. В целом же исследование 2004 года позволило определить (см. рис. П1.10), что только менее 30 % респондентов воспользовались услугами внешнего страхования. В дальнейшем также интересно проследить динамику обращения предприятий к услугам внешнего страхования информационных рисков.



...

Рис. П1.10. Данные по внешнему страхованию информационных рисков

Характеристика инцидентов безопасности. Исследование 2004 года показало (см. рис. П1.11) сохранение тенденции 2000 года сокращения общей частоты успешных атак на информационные системы. Доля респондентов, ответивших, что на предприятии столкнулись с несанкционированным использованием компьютерных систем, за последние 12 месяцев сократилась до 53 % (это наименьший процент с 1999 года). Доля респондентов, ответивших, что случаев несанкционированного использования компьютерных систем не было, увеличилась до 35 %, в то время как доля респондентов, которым не известно, имело ли место такое несанкционированное использование, снизилась до 11 %.



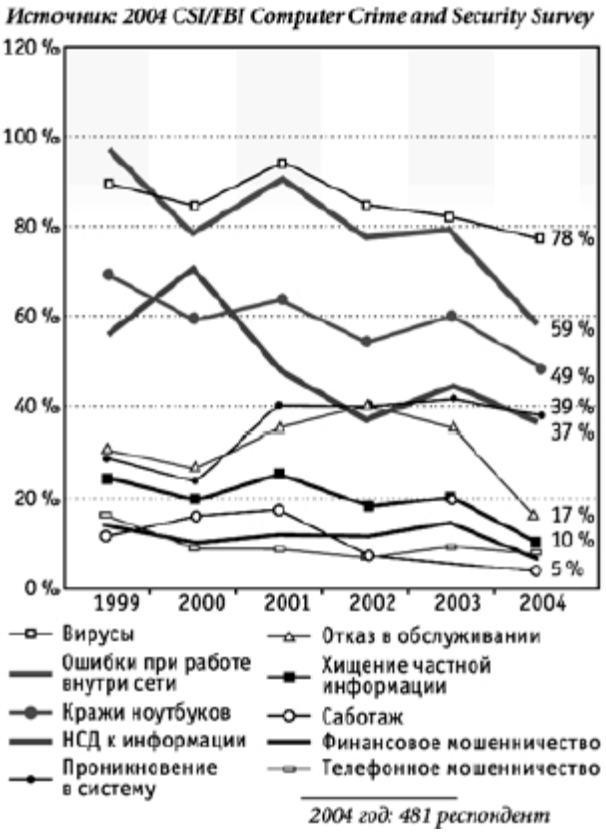
...

Рис. П1.11. Данные по несанкционированному использованию компьютерных систем

Таблица П1.1. Характеристика инцидентов безопасности в 2004 году

Кол-во инцидентов, %	1–5	6–10	более 10	Не знаю
2004	47 %	20 %	12 %	22 %
2003	38 %	20 %	16 %	26 %
2002	42 %	20 %	15 %	23 %
2001	33 %	24 %	11 %	31 %
2000	33 %	23 %	13 %	31 %
1999	34 %	22 %	14 %	29 %
Кол-во внешних угроз, %	**1–5**	**6–10**	**более 10**	**Не знаю**
2004	52 %	9 %	9 %	30 %
2003	46 %	10 %	13 %	31 %
2002	49 %	14 %	9 %	27 %
2001	41 %	14 %	7 %	39 %
2000	39 %	11 %	8 %	42 %
1999	43 %	8 %	9 %	39 %
Кол-во внутренних угроз, %	**1–5**	**6–10**	**более 10**	**Не знаю**
2004	52 %	6 %	8 %	34 %
2003	45 %	11 %	12 %	33 %
2002	42 %	13 %	9 %	35 %
2001	40 %	12 %	7 %	41 %
2000	38 %	16 %	9 %	37 %
1999	37 %	16 %	12 %	35 %

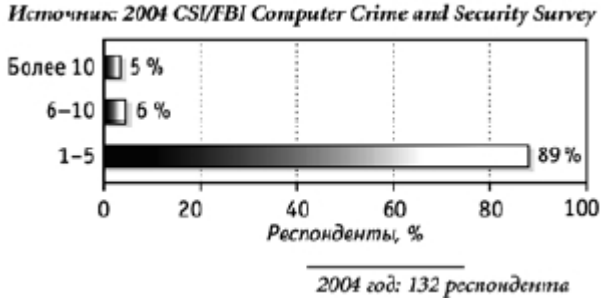
Приведенная здесь таблица наглядно демонстрирует, что количество инцидентов безопасности постепенно снижается. При этом угрозы безопасности равномерно распределились на внешние и внутренние. Эта таблица также показывает, что доля респондентов, фиксирующих за год от 6 до 10 инцидентов безопасности, судя по всему, стабилизировалась на уровне 20 %, в то время как доля респондентов, фиксирующих количество инцидентов безопасности за год от одного до пяти, увеличилась до 47 %. В 2004 году впервые зафиксирован самый низкий процент (12 %) респондентов, оценивающих, что их организация столкнулась за год более чем с десятью инцидентами безопасности.



...

Рис. П1.12. Характеристика атак или злоупотреблений в 2004 году

Рис. П1.12. показывает, что общее количество атак на компьютерные системы или выявленное злоупотребление этими системами медленно, но вполне устойчиво уменьшается.



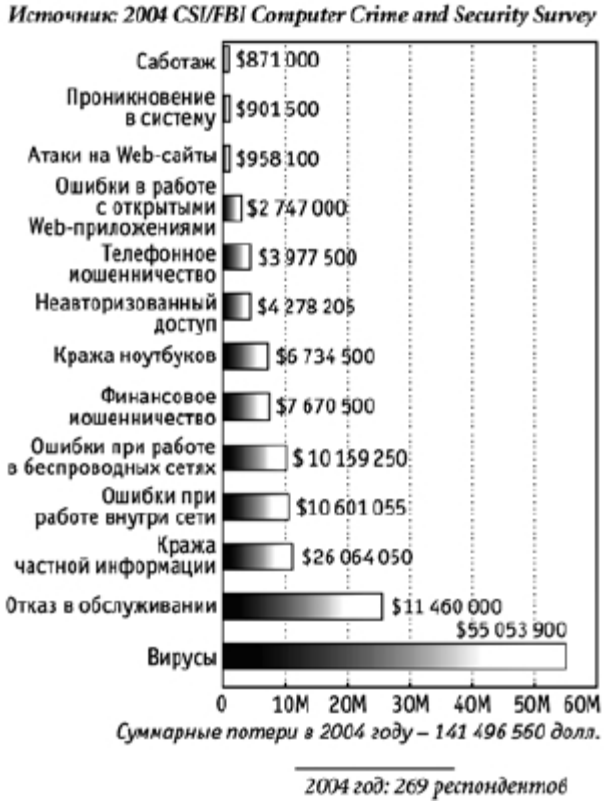
...

Рис. П1.13. Данные по происшествиям на Web-сайтах предприятий США

Как видно на рис. П1.13, на большинстве предприятий в 2004 году столкнулись с происшествиями на Web-сайтах. При этом 5 % респондентов сообщили о том, что их организации столкнулись более чем с десятью происшествиями на Web-сайтах. Подавляющее большинство (89 %) респондентов указали, что в течение года их организации столкнулись с происшествиями на Web-сайтах числом от одного до пяти.

Анализ убытков предприятий и организаций США (см. рис. П1.14) из-за инцидентов безопасности в 2004 году позволяет сделать следующие выводы. Во-первых, реальная история подсчета убытков свидетельствует о том, что общие потери (в расчете на одного

респондента) сократились. Общие потери предприятий в 2004 году составили 141 496 560 долларов по сравнению с 201 797 340 долларами в 2003 году. Во-вторых, как и в предыдущих исследованиях, респонденты часто были не готовы оценить потери в денежном эквиваленте. В исследовании 2004 года только 269 респондентов из 494 смогли предоставить количественные данные об убытках в долларах. В-третьих, впервые на первое место по приносимым убыткам вышли вирусные атаки, опередив хищения частной информации, которые влекли наибольшие убытки на протяжении последних пяти лет.



...

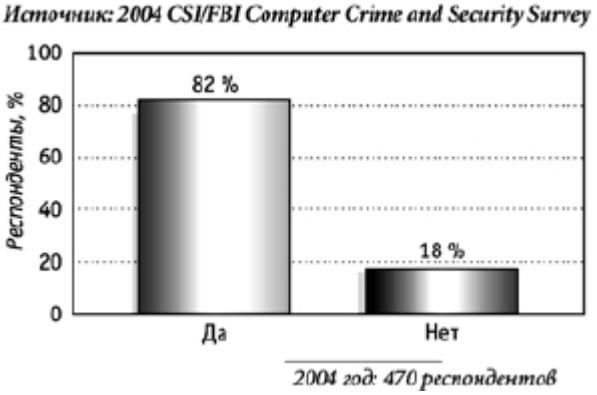
Рис. П1.14. Данные по убыткам из-за инцидентов безопасности в 2004 году

Технологии безопасности. В ходе исследования 2004 года респондентам был задан вопрос о том, какие технологии и технические средства безопасности используются в компании. Ответы показали (см. рис. П1.15), что 99 % респондентов используют на предприятии антивирусное программное обеспечение; 98 % – межсетевые экраны; 68 % – системы обнаружения вторжений (это на 5 % меньше по сравнению с исследованием 2003 года); 45 % – системы предупреждения вторжений, которые определяют и блокируют злоумышленную деятельность в сети в реальном масштабе времени; 71 % – контрольные листы доступа; 56 % – парольную защиту; 35 % – смарт-карты и электронные брелки с паролями; 11 % – биометрические средства защиты от НСД; 64 % – криптографические средства защиты информации; 42 % – технологию шифрования файлов; 30 % – инфраструктуру открытых ключей (PKI).

...

Рис. П1.15. Технологии безопасности современного предприятия

Аудит безопасности и вопросы обучения. Результаты исследования 2004 года показали (см. рис. П1.16), что 82 % предприятий регулярно проводят аудит безопасности информационных активов и компании в целом. Хотя для многих предприятий и организаций США процедура аудита безопасности пока не является общепринятой процедурой. Здесь будущие исследования помогут точно определить зависимость защищенности информационных систем предприятий от аудитов безопасности.



...

Рис. П1.16. Проводит ли ваша организация аудиты безопасности?

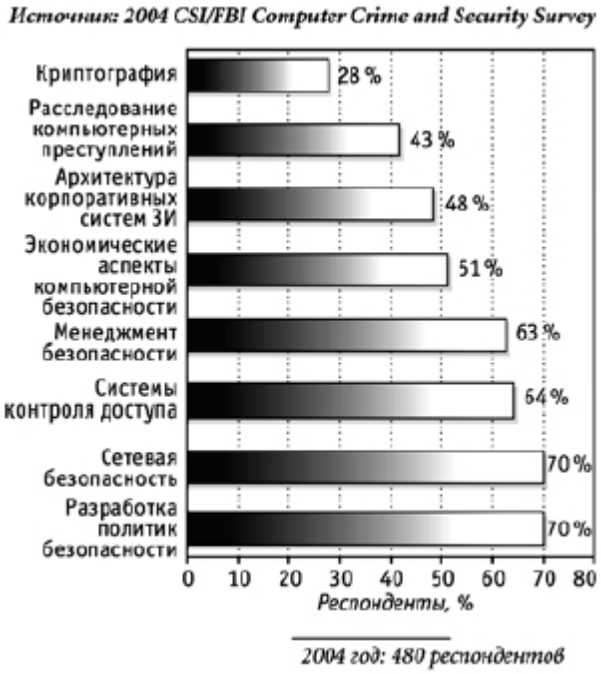
В исследовании 2004 года был поднят новый вопрос о необходимости обучения в области защиты информации. Во-первых, респондентов просили определить степень их согласия с формулировкой: «Моя организация инвестирует соответствующую сумму в знания по безопасности». Рис. П1.17 показывает, что в среднем респонденты не считают, что

их организации инвестируют достаточные средства в обучение по вопросам безопасности.

...

Рис. П1.17. Оценка достаточности инвестиций в обучение по безопасности

На рис. П1.18 представлены процентные доли респондентов, указавших на важность получения знаний по защите информации (для оценки важности обучения использовалась семибалльная шкала). Для пяти из восьми основных направлений обеспечения защиты информации обучение было признано достаточно важным. При этом обучение вопросам разработки политик безопасности и по сетевой безопасности было выделено как наиболее актуальное и полезное (70 %), далее следовало обучение по системам контроля доступа (64 %), управлению безопасностью (63 %), а также по экономическим аспектам защиты информации (51 %). Менее полезными в 2004 году оказались знания по архитектуре корпоративных систем защиты информации (47 %), расследованию компьютерных преступлений (43 %) и криптографии (28 %).



...

Рис. П1.18. Актуальность обучения по направлениям защиты информации

Обмен информацией. Исследование продемонстрировало, что большинство компаний не проявляют явной заинтересованности в обмене информацией по имевшим место инцидентам в области защиты информации. На рис. П1.19 отображена реакция опрошенных организаций на вторжения в информационные системы, начиная с 1999 года. Более 90 % респондентов указали: их организация реагирует на вторжения путем устранения недостатков в корпоративной системе защиты информации. Лишь половина респондентов указала, что их организация обменивается информацией о том или ином нарушении безопасности. Обмен информацией в процентах не увеличился за прошедшие годы и остается практически на том же уровне, что и в более ранних исследованиях. В прошлом году зафиксировано заметное снижение процентной доли компаний, которые сообщали правоохранительным органам о вторжениях в корпоративные информационные системы.

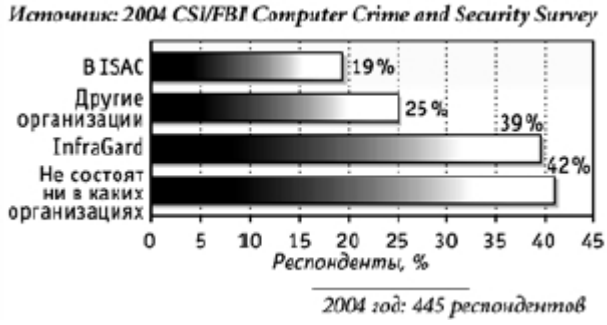
...

Рис. П1.19. Действия организаций в случаях вторжения в компьютерные системы

...

Рис. П1.20. Основные причины отказа от сообщений о вторжениях правоохранительным органам

На рис. П1.20 приведены причины, по которым организации не сообщали о вторжениях в информационные системы правоохранительным органам. Здесь отражены процентные доли респондентов, определяющих каждую сформулированную причину как очень важную (оценка важности – пять баллов и выше по семибалльной шкале) для принятия именно такого решения. Свыше 50 % респондентов (из тех, кто указал, что их организации не должны сообщать о вторжении правоохранительным органам) посчитали достаточно важной причиной падение курса акций и/или потерю репутации организации в результате огласки вторжения. Почти 35 % опрошенных в качестве важной причины назвали выгоду, которой могли бы воспользоваться конкуренты. Лишь 20 % посчитали, что использование гражданско-правовых средств судебной защиты было важной причиной для того, чтобы не сообщать о вторжении. Менее одной пятой от принявших участие в исследовании заявили, что они не знали о том, что о вторжении в корпоративную информационную систему следует сообщать правоохранительным органам. Другими словами, предприятиям хотя и известно о роли правоохранительных органов в борьбе с компьютерной преступностью, они предпочитают не сообщать о большинстве инцидентов и нарушений в области безопасности.



...

Рис. П1.21. Данные по предприятиям, входящим в организации обмена информацией об инцидентах безопасности

В ходе исследования 2004 года был предложен вопрос о том, входят ли предприятия в

какую-либо организацию обмена информацией о нарушениях и инцидентах безопасности. Результаты исследования свидетельствуют о том, что ряд компаний входят сразу в несколько групп обмена информацией (см. рис. П1.21); 42 % респондентов указали, что их организации не входят в какую-либо организацию обмена информацией; 39 % входят в InfraGard; 19 % – в ISAC и 25 % входят в другие аналогичные организации. При этом большинство компаний готовы участвовать в полномасштабном обмене информацией о нарушениях в области защиты информации, что соответствует последним выводам в теоретических работах ученых.

Влияние законодательных актов. В исследовании CSI/FBI 2004 года был включен новый вопрос о влиянии законодательных актов, и в частности закона Сарбейнса-Оксли, на организацию режима информационной безопасности предприятия. Как показано на рис. П 1.22, респонденты из числа представителей финансовых, коммунальных и телекоммуникационных отраслей экономики США считают, что закон Сарбейнса-Оксли оказал значительное влияние на организацию режима информационной безопасности в компании. В то же время респонденты из других отраслей экономики США не столь единодушны. По-видимому, для принятия окончательного решения о значении этого и других аналогичных законодательных актов для организации режима информационной безопасности на предприятии необходимо подождать результатов будущих исследований.

...

Рис. П1.22. Влияние закона Сарбейнса-Оксли на организацию режима информационной безопасности предприятия

Резюме

Результаты исследования CSI/FBI позволили выявить следующие основные тенденции и перспективы развития современных технологий защиты информации:

• в целом несанкционированное использование информационных систем снизилось, как и суммы ежегодных финансовых убытков от инцидентов, связанных с нарушением безопасности информации;

• в отличие от прошлых лет вирусные атаки и атаки типа «отказ в обслуживании» превзошли самый высокий прежний показатель – стоимость хищения частной информации.

Ущерб от вирусных атак вырос до 55 млн. долларов;

• процент организаций, сообщавших о вторжениях в компьютерные системы правоохранительным органам, в течение последнего года снизился. Основной причиной этого является опасение негативных последствий публичной огласки инцидентов безопасности, выражающихся в возможной потере имиджа и доходности компании;

• большинство организаций проводят экономическую оценку затрат и возврата инвестиций на защиту информации. При этом 55 % организаций используют показатель возврата инвестиций (ROI или ROSI), 28 % используют показатель внутренней нормы доходности (IRR) и 25 % используют показатель чистой текущей стоимости (NPV);

• свыше 80 % организаций регулярно проводят аудит безопасности информационных активов и компании в целом;

• большинство организаций не передают работы по обеспечению информационной безопасности сторонним организациям. Среди тех организаций, которые считают это возможным, процент работ по обеспечению информационной безопасности на основе аутсорсинга является весьма низким;

• законодательные акты, и в частности закон Сарбейнса-Оксли, оказывают определенное влияние на организацию режима информационной безопасности компании;

• подавляющее большинство организаций считают обучение сотрудников компании вопросам защиты информации достаточно важным элементом общей программы обеспечения безопасности. При этом респонденты исследования считают, что текущие затраты на обучение являются скорее необходимыми, чем достаточными.

Приложение 2 МЕЖДУНАРОДНЫЙ ОПРОС 2003 ГОДА ПО ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ. ОБЗОР РЕЗУЛЬТАТОВ ПО СТРАНАМ СНГ

В начале 2004 года компания «Эрнст энд Янг» опубликовала результаты своего исследования состояния информационной безопасности в СНГ (www.eu.com/russia *). В этом исследовании специалисты «Эрнст энд Янг» провели анализ и сопоставили проблемы, мнения и действия компаний стран СНГ по вопросам информационной безопасности в сравнении с ведущими мировыми компаниями. Далее рассмотрены основные результаты исследования и комментарии к ним «Эрнст энд Янг».*

Краткая справка Один из основных результатов данного опроса – вывод о том, что во всем мире компании сталкиваются с одинаковыми проблемами по информационной безопасности. Сбои в работе важнейших информационных систем компаний продолжают оставаться серьезной помехой для ведения бизнеса во всех странах мира. Несмотря на то, что такие сбои в основном связаны с проблемами программно-аппаратного комплекса и каналов связи, компании все чаще сталкиваются со сбоями, вызванными компьютерными вирусами либо злоумышленными действиями и недобросовестной работой сотрудников, что приводит к отказу в работе информационных систем. Для предотвращения этого и повышения существующего уровня защиты корпоративных систем необходимы дополнительные инвестиции в обеспечение информационной безопасности. За последние годы мы также осознали необходимость контроля и управления в этой сфере.

Многие компании используют разнообразные технические решения для защиты информационных систем. Однако в странах СНГ принятые меры не позволили достичь желаемого эффекта. Наш опрос помог выяснить, что руководители многих компаний, работающих в СНГ, менее уверены в достаточности принятых мер по обеспечению безопасности, чем их зарубежные коллеги. Некоторые из специфичных проблем, с которыми они сталкиваются, такие, как: недостаточная системная интеграция, использование устаревшей инфраструктуры и отсутствие комплексного подхода к внедрению средств обеспечения информационной безопасности, существенно затрудняют достижение приемлемого уровня информационной безопасности.

Еще одним фактором, усложняющим ситуацию, может быть нежелание использовать сторонних подрядчиков даже при отсутствии собственных специалистов и ресурсов для осуществления управления информационными рисками, требующего серьезной технической и организационной работы.

В то же время эффективное управление вопросами информационной безопасности приобретает все большее значение для компаний стран СНГ по мере их роста и продвижения на новые рынки. Инвесторам необходима уверенность в том, что для защиты бизнеса и информационных активов принимаются необходимые меры. Клиентам важно знать, что соблюдается конфиденциальность их персональных данных. Деловые партнеры ожидают, что компания будет функционировать без сбоев. Результаты нашего исследования и комментарии к ним, как мы рассчитывали, помогут улучшить стандарты информационной безопасности как в отдельных компаниях, так и в деловом сообществе СНГ в целом.

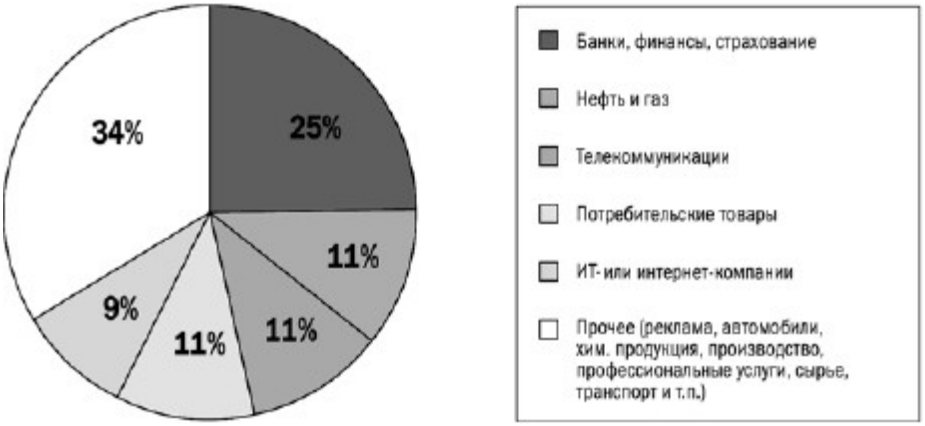
В международном опросе по информационной безопасности приняли участие более 1 400 генеральных директоров, директоров по информационным системам и других руководителей компаний из 66 стран (включая страны СНГ).

...

Рис. П2.1. Участники опроса (по странам)

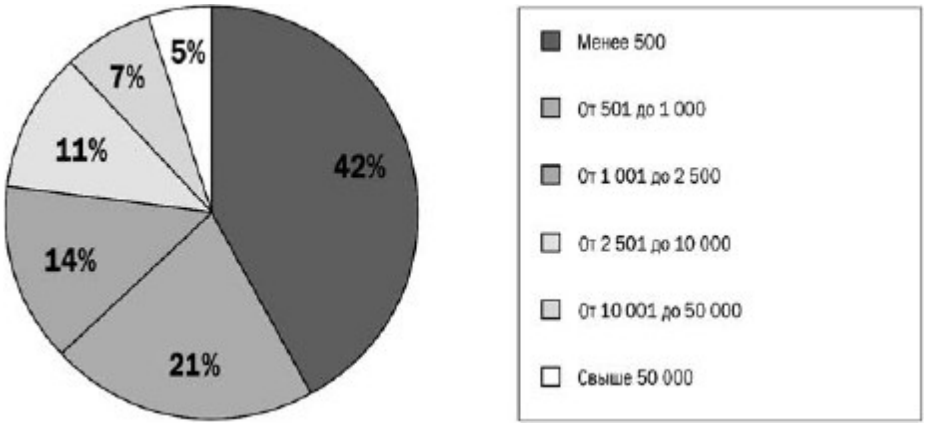
В настоящем обзоре рассматриваются ответы, полученные только от компаний, ведущих свою деятельность в СНГ. В опросе приняли участие 56 компаний, работающих в России, Украине, Казахстане и Беларуси.

Большинство компаний считает, что основную ответственность за обеспечение информационной безопасности должен нести либо директор по информационным системам (руководитель отдела ИТ), либо директор по безопасности. На самом деле, ответственность за координацию вопросов безопасности должна быть возложена на совет директоров.



...

Рис. П2.2. Участники опроса (по отраслям)



...

Рис. П2.3. Участники опроса (по количеству сотрудников)

По мере усиления зависимости компаний от информационных технологий в их повседневной деятельности даже кратковременное нарушение информационной безопасности, приведшее к сбою систем, уничтожению данных или программ, может иметь катастрофические последствия для бизнеса. Вот почему для руководства компании становится все более важным вопрос о принятии на себя всей полноты ответственности за вопросы информационной безопасности. Кроме того, компании редко докладывают совету директоров о происшествиях в области безопасности и связанных с этим вопросах. Менее 40 % участников опроса (в основном это международные компании) делают такие доклады регулярно (ежеквартально, ежемесячно или чаще).

Опрос показал, что как в СНГ, так и за рубежом ответственным за вопросы информационной безопасности, как правило, назначается руководитель ИТ-подразделений или руководитель отдела общей безопасности. Относительно небольшое число компаний в СНГ, большей частью работающих в сфере ИТ, операций с ценными бумагами и мобильной связи, сообщили, что в их компаниях за эти вопросы отвечает представитель высшего руководства (генеральный директор, финансовый директор или руководитель отдела).

Комментарий «Эрнст энд Янг»: • планирование и реализация стратегии информационной безопасности должны быть поручены представителю высшего руководства, имеющему полное представление о бизнесе организации и технических аспектах угроз и уязвимых мест в информационных системах. Тем не менее за координацию вопросов безопасности должен отвечать в конечном итоге совет директоров;

• во всем мире наблюдается рост компьютерной преступности. Чем успешнее работают компании в странах СНГ, тем больше возникает рисков в этой области. То, что в прошлом хакеры не атаковали эти компании, не означает, что и в будущем этого не произойдет. Чтобы убедить инвесторов в том, что для защиты важнейших активов компании (то есть ее стоимости) принимаются необходимые меры, совет директоров должен продемонстрировать свое внимание к вопросам информационной безопасности и руководить их решением.

Большинство участников опроса заявили о том, что их стратегия информационной безопасности приведена в соответствие с задачами бизнеса. Однако определенные однажды правила редко пересматриваются, и это вызывает сомнения в том, что они

действительно всегда соответствуют бизнес-целям. Любая стратегия информационной безопасности, чтобы стать эффективной, должна быть нацелена на минимизацию бизнес-рисков и создание конкурентных преимуществ. Исходя из наблюдений, сделанных нами в ходе опроса, большинство компаний в СНГ считают вопросы информационной безопасности важным аспектом своей деятельности. Почти две трети (62 %) участников опроса указали, что их специалисты по информационной безопасности регулярно (ежеквартально, ежемесячно или чаще) встречаются с руководителями подразделений, чтобы обсудить, каким образом меры информационной безопасности могут лучше защитить бизнес и способствовать его расширению.

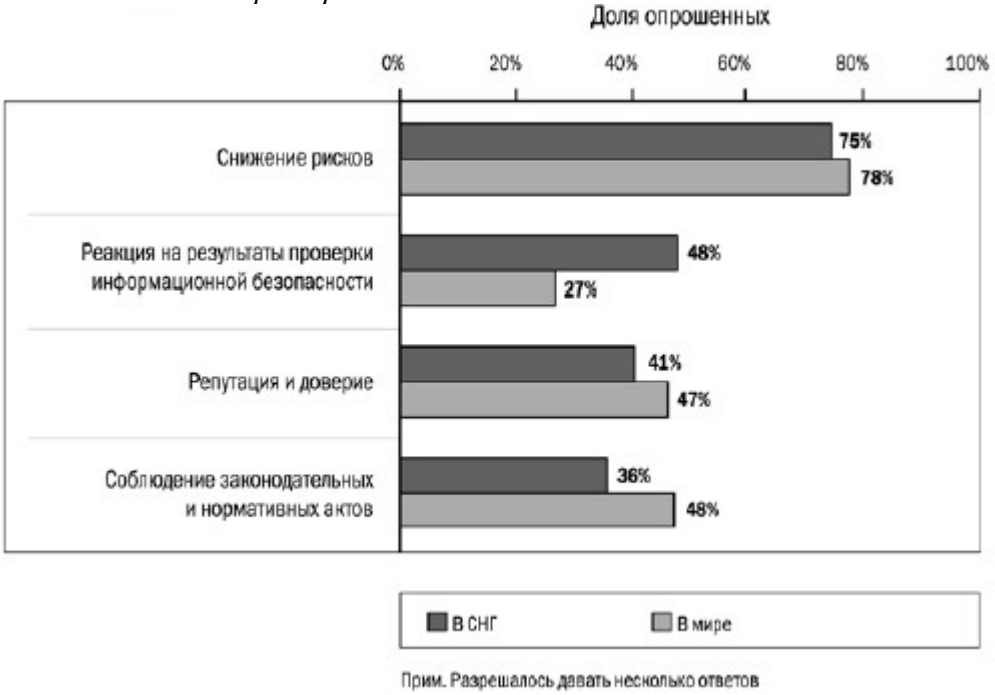
Тем не менее руководители очень многих компаний в СНГ практически не занимаются вопросами стратегии и политики информационной безопасности. В результате 66 % участников опроса высказали сомнения в том, действительно ли внедренные правила соответствуют целям бизнеса.

Комментарий «Эрнст энд Янг»: • стратегия информационной безопасности будет способствовать экономии средств только в том случае, если ее внедряют руководители различных подразделений и если она направлена на минимизацию важнейших бизнес-рисков компании. Регулярные встречи между руководством службы информационной безопасности и руководителями компании обеспечивают более полное понимание постоянно меняющихся требований к бизнесу и связанных с ними рисков;

• информационные технологии и информационная безопасность могут служить стимулом для развития бизнеса и создать конкурентное преимущество. Руководители компании должны совместно со специалистами в этих областях постоянно изучать возможности, открывающиеся в связи с новыми достижениями технологий;

• руководство компании должно регулярно пересматривать стратегию и правила информационной безопасности на предмет соответствия задачам бизнеса. Это позволит обеспечить выделение достаточного объема ресурсов компании на решение вопросов информационной безопасности, имеющих огромное значение для бизнеса.

Решения в области информационной безопасности в СНГ реализуются в основном для минимизации рисков, ликвидации уязвимых мест, защиты репутации, создания доверительных отношений с партнерами и соблюдения законодательства.



...

Рис. П2.4. Основные факторы, влияющие на принятие решений в области безопасности

Основополагающей целью большинства мероприятий по информационной безопасности является защита и расширение бизнеса компании.

Участники опроса в СНГ и за рубежом сообщают, что наиболее весомым фактором при принятии решений о внедрении новых технологий информационной безопасности является снижение рисков. Кроме того, компании в СНГ придают большое значение проверкам и оценке безопасности информационных систем с целью выявления и устранения уязвимых мест.

Нередко внедрение решений вызвано необходимостью поддержать репутацию компании и внушить партнерам уверенность в способности компании защитить свои информационные активы. О своей готовности включать в годовую отчетность данные о программах по обеспечению информационной безопасности заявили 71 % участников опроса в СНГ.

Комментарий «Эрнст энд Янг»: • прежде чем приступить к разработке стратегии информационной безопасности, компании необходимо решить, какие информационные активы имеют наиболее важное значение для ее деятельности. Основное внимание в программе должно уделяться защите этих активов от нарушения конфиденциальности, хищения или уничтожения;

• любые изменения в информационных системах и сетях приведут к появлению новых уязвимых мест. Даже при отсутствии изменений в существующем программном и аппаратном обеспечении постоянно обнаруживаются все новые уязвимые места. Этим часто пользуются хакеры для проникновения в информационные системы, поэтому компаниям необходимо научиться оперативно распознавать такие места и разрабатывать контрмеры по защите;

• успех многих компаний зависит исключительно от их репутации. Однажды случившееся нарушение в области безопасности может подорвать доверие к компании со стороны клиентов и инвесторов. Вот почему профилактические меры должны приниматься заблаговременно.

Многие компании в СНГ не уверены в достаточности принимаемых ими мер по обеспечению информационной безопасности. Сегодня большинство компаний принимают меры для защиты своих информационных систем. В ходе предыдущего опроса, проведенного «Эрнст энд Янг» в 2001 году, нами было выявлено, что многие компании стран СНГ внедрили антивирусную защиту, межсетевые экраны и системы обнаружения вторжения. Тем не менее эти меры не обеспечивают стопроцентной защиты, и в ходе опроса 2003 года было установлено, что в целом по СНГ не хватает уверенности в уровне обеспечения безопасности:

• *выявление уязвимых мест в системах;*

По сравнению с 66 % участников опроса во всем мире только 48 % участников опроса в странах СНГ заявили, что их компании могут с достаточной степенью уверенности выявить уязвимые места в своих информационных системах. Такая ситуация говорит о недостаточном внимании к этому вопросу со стороны руководства, недостаточности имеющихся средств, квалификации и опыта, а также об отсутствии правил и процедур обнаружения уязвимых мест и принятия мер по их устранению.

защита важнейшей деловой информации;

Лишь 48 % участников опроса в СНГ (по сравнению с 70 % участников опроса по всему миру) оценили свой уровень защиты важнейшей деловой информации, как соответствующий мировому уровню или достаточный. Можно сделать вывод, что многие компании в СНГ чувствуют себя уязвимыми из-за отсутствия целостного подхода к вопросам информационной безопасности.

выявление вторжений и атак на информационные системы;

Уверенность в способности своей компании обнаруживать хакерские атаки выразили 59 % участников опроса в СНГ (66 % участников опроса в мире).

обеспечение непрерывной деятельности в случае атаки.

Всего 54 % участников нашего опроса (67 % участников опроса в мире) вполне уверены в способности своей компании продолжать деятельность в случае хакерской атаки или иной экстренной ситуации. Хотя в результате прошлого опроса мы выяснили, что в большинстве компаний СНГ имеются планы обеспечения деятельности в экстренной ситуации, но они, очевидно, не являются полными, не протестированы и, соответственно, неэффективны для предотвращения сбоев в деятельности компании. В СНГ наибольшую уверенность относительно принятых мер информационной безопасности выражают компании, занимающиеся банковской деятельностью, информационными технологиями и операциями с ценными бумагами, а также работающие в нефтегазовой отрасли. Что касается общего мнения, то участники опроса и в СНГ, и во всем мире сочли, что информационная безопасность лучше всего обеспечивается в банковском секторе.

Комментарий «Эрнст энд Янг»: • лучшая защита от вторжений в информационные системы – профилактические меры. В компаниях должна присутствовать официальная процедура непрерывного анализа выявленных уязвимых мест. Необходимо регулярно проводить оценку рисков по информационной безопасности, обеспечивая комплексный и своевременный анализ уязвимости сети по отношению к внешним или внутренним вторжениям;

• после обнаружения уязвимых мест в системе следует принять меры, чтобы не допустить использования этих мест хакерами. Выбор верного решения по обеспечению безопасности может оказаться сложной задачей. Здесь важно отдавать себе отчет в том, что решение, оптимальное для одной компании, может оказаться абсолютно непригодным для другой. Выбранное решение должно обеспечивать защиту от комплекса угроз и уязвимых мест, характерных для данной компании;

• бессистемная, выборочная реализация средств безопасности не обеспечивает необходимого уровня защиты. Чтобы надежно защитить важнейшую деловую информацию, компаниям необходимо интегрировать вопросы физической и информационной безопасности в единый для всей организации свод правил, стандартов и инструкций. Стратегия безопасности проверяется на прочность в своем самом слабом звене;

• системы обнаружения вторжений (IDS) обеспечивают раннее обнаружение атак на информационные системы, давая специалистам по безопасности возможность отследить нарушителя, представить себе возможные последствия инцидента, оценить его значение, а затем принять меры, необходимые для минимизации ущерба и предотвращения атак в будущем;

• компаниям необходимо составлять планы мероприятий по обеспечению непрерывности и восстановлению своей деятельности в экстренных ситуациях, особенно если такая деятельность в значительной степени зависит от информационных систем. Этот план должен быть полным и предусматривать действия в самых различных экстренных ситуациях, он также должен регулярно проходить тестирование на предмет своей эффективности;

• компаниям необходимо проводить оценку достаточности собственных ресурсов, требуемых для выполнения всех мероприятий в области безопасности – от выявления угроз и уязвимых мест до выбора и внедрения верных решений. Независимые фирмы, основной деятельностью которых является оказание услуг в области информационных технологий и информационной безопасности, могут стать самым экономически оправданным вариантом, учитывая объем их знаний, квалификацию, опыт и объективность.

Опрос показал, что многие компании не интересуются вопросами соблюдения стандартов информационной безопасности третьими сторонами. Те компании, которые обмениваются конфиденциальной информацией по компьютерным сетям с ключевыми деловыми партнерами (независимыми подрядчиками, филиалами, поставщиками,

клиентами), ожидают, что их контрагенты обеспечат их данным такой же уровень защиты, который поддерживают они сами. Точно так же компании, постоянно осуществляющие торговые сделки через компьютерные сети, ожидают, что третьи стороны обеспечат постоянный доступ и функционирование своих информационных систем.

По оценкам значительной части участников нашего опроса в СНГ, их коллеги и деловые партнеры в состоянии гарантировать примерно такой же уровень обнаружения атак и обеспечения деятельности в случае вторжения, как и они сами. Тем не менее создается впечатление, что многие компании как в СНГ, так и во всем мире не уделяют внимания вопросу о достаточности информационной безопасности третьих сторон. Иногда этот вопрос действительно не имеет значения, например, если клиент – частное лицо или если в деловых отношениях практически не используются информационные системы. В других случаях компании, возможно, не обращают внимания на соблюдение стандартов безопасности третьими лицами просто потому, что не задумываются о последствиях, которые для них может иметь инцидент в области безопасности.

Комментарий «Эрнст энд Янг»: • компания, ведущая активный обмен информацией с деловыми партнерами через компьютерные сети и системы, подвергается серьезному риску. Такая компания должна настаивать на соблюдении минимальных стандартов информационной безопасности всеми участвующими в информационном обмене сторонами;

• компании должны представлять себе объем возможного ущерба для своей деятельности, который они могут понести в случае сбоя в работе систем третьих сторон (например, интернет-провайдера или Web-хостинга). Если такой ущерб оценивается как значительный, сторонам следует официально согласовать план мероприятий, позволяющих обеспечить непрерывность деятельности. Кроме того, компании необходимо ознакомиться с программами третьих сторон по обеспечению непрерывности деятельности и ее восстановлению в экстренных ситуациях для оценки их адекватности;

• если компании известно о том, что ее конкуренты обеспечивают более высокие стандарты информационной безопасности, то необходимо оценить, не станет ли в долгосрочной перспективе этот факт преимуществом конкурентов. Этот вопрос имеет особенно важное значение для компаний, которые занимаются электронной торговлей или работают со строго конфиденциальными данными. В таком случае преимущества по обеспечению безопасности информационной среды вполне могут оправдать затраты, связанные с инвестициями в этой области.

Обеспечение непрерывности деятельности компаний в экстренных ситуациях требует особого внимания из-за частых сбоев в работе их систем. Наше исследование показало, что перед руководителями компаний в СНГ стоят те же проблемы, связанные с отказами в работе важнейших систем, что и перед их коллегами за рубежом.

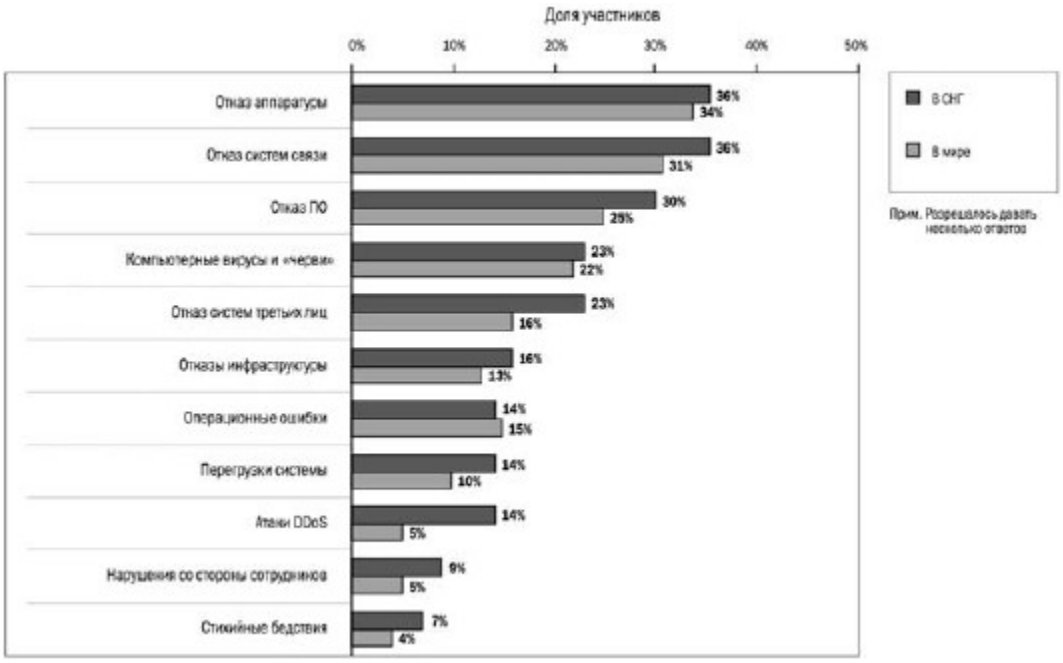
Среди участников опроса в СНГ 54 % (52 % участников опроса в мире) признали, что в прошедшем году им приходилось сталкиваться с неожиданным выходом из строя (отказом) важной системы более чем на 2 часа. Основные причины сбоя носили технический характер, то есть были связаны с отказами программного и аппаратного обеспечения, систем связи и инфраструктуры.

Однако многие отказы, о которых сообщили участники опроса, были вызваны следующими обстоятельствами:

• отказом в работе систем третьих сторон – это подтверждает необходимость оценки стандартов информационной безопасности, используемых третьими сторонами, от которых зависит деятельность компании;

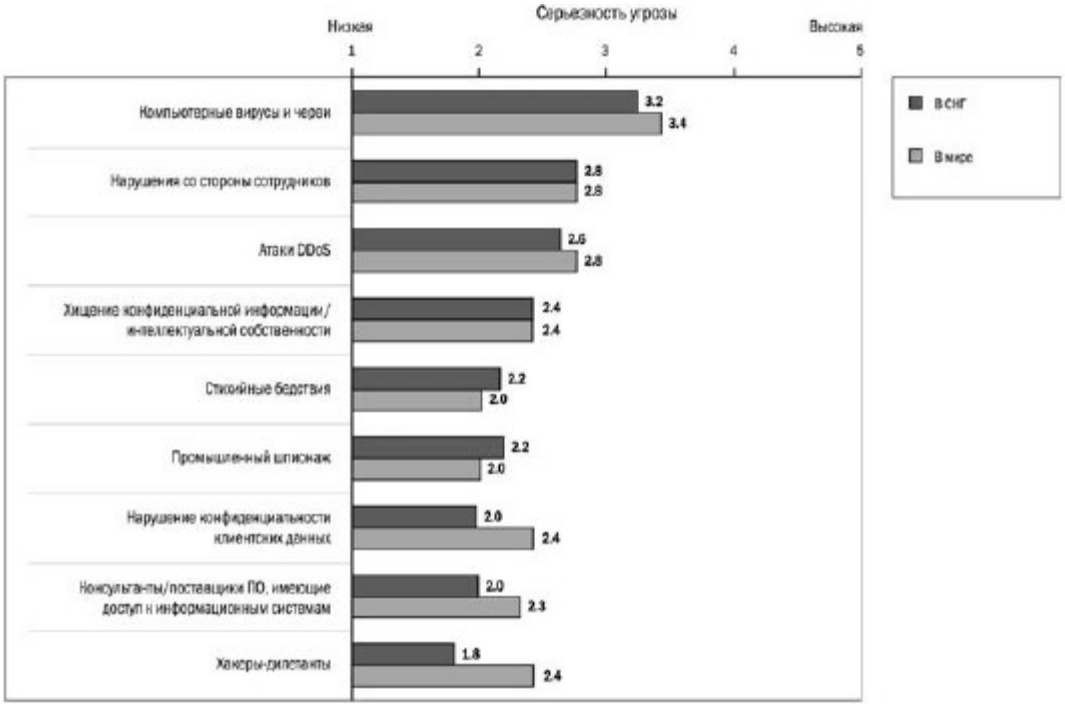
• преднамеренными атаками – вирусами и атаками с целью вызвать отказ в обслуживании (DDoS);

• человеческим фактором – операционной ошибкой (например, загрузкой неправильного программного обеспечения), системными перегрузками.



...

Рис. П2.5. Основные причины отказов важнейших систем



...

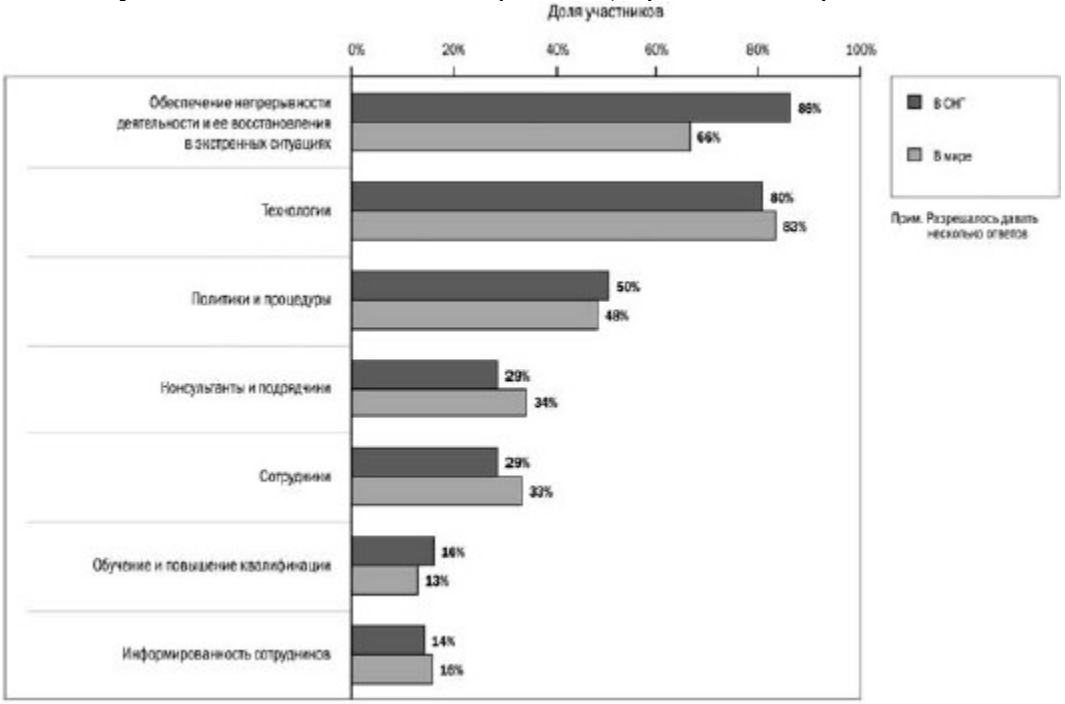
Рис. П2.6. Основные угрозы информационной безопасности (не связанные с техникой)

Но все больше компаний начинает отдавать себе отчет в значимости таких внутренних угроз, связанных с информационными системами, как нарушения в работе, вызванные действиями сотрудников. Серьезную обеспокоенность вызывают также атаки DDoS и

хищение конфиденциальной информации.

В СНГ потеря клиентских данных не считается столь серьезной проблемой, как в западных странах, в связи с тем, что законодательство об охране конфиденциальности данных практически отсутствует. Кроме того, компании в СНГ не считают серьезной угрозу доступа сторонних консультантов к информационным системам, так как не часто используют их услуги. Хакеры-дилетанты рассматриваются в качестве угрозы международными компаниями в большей степени, чем участниками опроса в СНГ, вероятно, потому, что именно известные западные компании нередко подвергались таким атакам за последние годы.

Учитывая участившиеся случаи отказов важнейших систем и причины этих отказов, многие участники опроса сообщили, что бюджет, выделяемый на обеспечение информационной безопасности, предназначен не только для совершенствования технологии, но и для работы по программам обеспечения непрерывности деятельности и ее восстановления в экстренных ситуациях. Как представляется, организационным мерам безопасности, например составлению официальных правил и процедур, а также приобретению опытных специалистов (передача некоторых функций бизнеса на субподряд, привлечение консультантов для проведения экспертизы, подбор подготовленного персонала или обеспечение обучения и повышения квалификации) придается второстепенное значение.



...

Рис. П2.7. Основные области вложения средств в информационную безопасность

В опросе по СНГ, который мы проводили в 2001 году, в качестве одной из главных проблем обеспечения информационной безопасности на должном уровне компании называли недостаточную информированность. Несмотря на это, компании по-прежнему не уделяют данному вопросу достаточного внимания. Менее 40 % участников опроса в СНГ сообщили, что они проводят регулярное обучение. Еще меньше (20 %) постоянно проводят семинары и инструктажи по информационной безопасности.

Таблица П2.1. Передача функций безопасности на субподряд

Функция передана на субподряд или будет передана в следующем году	% участников опроса в СНГ	% участников опроса в мире
Web-хостинг / Интернет-провайдер	71	58
Виртуальные выделенные сети / Удаленный доступ	36	37
Контроль за состоянием сетей и систем	18	36
Непрерывность / Восстановление деятельности	14	42
Управление сетью	13	29
Центр связи с клиентами (call center)	13	21
ИТ-инфраструктура	5	32

В СНГ довольно небольшое число компаний (по сравнению с другими странами) передает функции бизнеса на субподряд или внешнее ведение. Среди передаваемых функций большую долю занимает Web-хостинг, оказание интернет-услуг, виртуальные выделенные сети и удаленный доступ. Тем не менее контроль за состоянием информационных сетей и систем все чаще передается на субподряд, возможно, из-за неуверенности в способности обнаружить атаку собственными силами и продолжать деятельность в случае такой атаки.

Комментарий «Эрнст энд Янг»: • по мере постоянного усложнения информационных систем отдельные сбои становятся неизбежными. Иногда бывает невозможно предотвратить отказы аппаратного и программного обеспечения и систем связи, а учитывая повысившуюся вероятность террористических актов, направленных на глобальную информационную инфраструктуру, компаниям необходимо разработать эффективную программу обеспечения непрерывности деятельности и ее восстановления в экстренных ситуациях;

• во многих компаниях наблюдается непропорционально высокий объем вложений в технические средства обеспечения безопасности. Однако следует уделять больше внимания самим процессам обеспечения безопасности и человеческому фактору в этих процессах. Перечисленные ниже аспекты являются самыми важными для минимизации риска отказа систем в результате ошибки сотрудника, недостаточной информированности персонала по вопросам безопасности или в случае преднамеренной атаки:

– создание официальных процедур для проведения таких операций, как загрузка новых программных приложений и планирование системной нагрузки, позволяет избежать операционных ошибок и перегрузки систем;

– программы обучения и семинары по вопросам безопасности снижают риск того, что сотрудники сведут на нет преимущества технических средств (из-за неправильной конфигурации самого надежного межсетевого фильтра или открытия зараженного файла);

– жесткие процедуры и правила по использованию паролей и получению прав доступа уменьшают риск внутренней атаки (например, со стороны недовольного сотрудника) или со стороны деловых партнеров, имеющих санкционированный доступ в сети и системы компании.

Таблица П2.2. Бюджеты информационной безопасности

Отрасль	Бюджет на информационные системы (средний) в % от годового объема выручки	Разброс объема бюджета (отдельных компаний) в % от годового объема выручки
Высокие технологии	32	Большой разброс – от 10 до 55
Банковский сектор и финансы	13	Обычно от 5 до 10
Телекоммуникации	15	Обычно от 3 до 6
Прочие	2	Обычно от 1 до 2

Главное препятствие на пути эффективного обеспечения информационной безопасности – недостаток финансирования.

Сегодня большинство компаний хорошо осведомлены о необходимости действенных

мер по обеспечению информационной безопасности. Однако осознание важности информационной безопасности – это лишь первый шаг. Для достижения практических результатов требуются ресурсы. Компаниями, работающими в сфере высоких технологий, выделяются самые крупные бюджеты на развитие информационных систем. За ними следуют компании банковского сектора, финансовые и телекоммуникационные компании. Согласно данным опроса, главными препятствиями на пути обеспечения информационной безопасности являются другие приоритеты в распределении ресурсов и бюджетные ограничения. Компании нередко выделяют единый бюджет на удовлетворение всех потребностей по информационным системам (аппаратное и программное обеспечение, зарплата, консультанты и т. п.), при этом основная часть средств идет на повышение производительности, а вопросы информационной безопасности остаются без внимания.

Еще одна серьезная проблема – нехватка квалифицированного персонала. Причиной этого, вероятно, является ограниченный бюджет, выделяемый на его привлечение, и недостаточные вложения в программы обучения. Помимо этого, компании в СНГ довольно редко привлекают к работе независимых подрядчиков, несмотря на недостаточный опыт собственных сотрудников в решении вопросов информационной безопасности.

Комментарий «Эрнст энд Янг»: • последние 10 лет мы наблюдаем постоянное расхождение объемов финансирования в обеспечении безопасности по отношению к финансированию сферы ИТ в целом. В связи с этим у многих компаний уже сегодня может возникнуть угроза сбоя работы их систем, вторжений и вирусных атак. Единственный способ изменить эту тенденцию – решить вопросы информационной безопасности. Это означает, что стратегия информационной безопасности должна быть основана на требованиях бизнеса и руководители компании должны быть информированы о рисках и последствиях нарушения безопасности для бизнеса. (Компании, которые никогда не сталкивались в реальности с нарушением безопасности, могут провести моделирование «этичной» хакерской атаки на информационные системы, чтобы полностью представить себе, какими будут последствия и ущерб от реального инцидента.);

• экономические выгоды от внедрения комплексной структуры и соблюдения правил в области безопасности следует довести до сведения руководства компании и совета директоров. Только у них имеются полномочия отдавать распоряжения и выделять ресурсы, необходимые для укрепления информационной безопасности;

• нередко приходится видеть, как компания принимает меры по укреплению информационной безопасности только после произошедшего инцидента, причем для решения проблемы выбирается временный вариант. Такой односторонний и устаревший подход приводит к увеличению затрат и потере и без того ограниченных финансовых ресурсов. Взвешенный, инициативный, комплексный подход к обеспечению информационной безопасности в масштабах всей организации в конечном итоге часто оказывается дешевле.

Данные опроса показывают, что многие компании в СНГ не заботятся о соблюдении законодательства в области информационной безопасности. Информационная безопасность – относительно новая тема, и правительства ряда стран продолжают совершенствовать законодательство в этой сфере и разрабатывать официальные структуры поддержки, необходимые для защиты компаний и граждан от компьютерных преступлений.

Некоторые из участников нашего опроса, занимающиеся банковской деятельностью, страхованием, телекоммуникациями, операциями с ценными бумагами и управлением средствами фондов, заявили, что нормативные документы, регламентирующие вопросы безопасности, оказывают серьезное влияние на сферу их деятельности. Однако результаты нашего опроса показывают, что компании, работающие в одних и тех же отраслях, имеют совершенно разное мнение относительно масштаба такого влияния. Это является очевидным подтверждением недостаточной осведомленности и ясности относительно того, какими документами регламентируются вопросы информационной безопасности.

Среди участников опроса в СНГ 13 % признали, что они не соблюдают действующие

нормативные документы в области безопасности, а еще 27 % заявили, что не обязаны выполнять подобные требования. В действительности, принятые недавно законы налагают на компании новые обязательства по обеспечению защиты информации персонального характера (информация по клиентам и сотрудникам).

Комментарий «Эрнст энд Янг»: • во всем мире ужесточаются требования законодательства к обеспечению достаточного уровня информационной безопасности, причем многие из них распространяются и на страны СНГ. Компаниям необходимо получить консультацию профессионального юриста относительно нормативных документов, которым необходимо следовать, или государственного ведомства, куда следует обращаться по вопросам информационной безопасности.

Резюме В результате недостаточного финансирования в сфере информационной безопасности, наблюдавшегося в течение последних десятилетий, многие компании оказались не защищенными от сбоев в деятельности важнейших систем, вирусных атак и хищения конфиденциальной информации. Только теперь компании начинают осознавать насущную необходимость усиления безопасности:

• *обеспечение информационной безопасности – поддержка совета директоров;*

Обеспечение действенной системы информационной безопасности требует принятия мер в масштабах всей организации и при поддержке «на самом верху». Руководство компании и совет директоров должны быть полностью осведомлены о возможном ущербе для бизнеса и репутации компании в результате нарушения безопасности или отказа в работе систем. Варианты стратегии и политика в области безопасности должны быть направлены на защиту важнейших активов и поддержку бизнеса компании. Все перечисленные факторы имеют большое значение для обоснования необходимости выделения ресурсов и получения поддержки, без которых невозможно реализовать комплексную стратегию безопасности.

• больше внимания вопросам персонала и процедур;

Традиционно меры по обеспечению безопасности были направлены на технические аспекты, то есть приобретение и установку антивирусных программ, межсетевых фильтров и систем обнаружения вторжений. Сегодня настало время обратить внимание на обучение персонала и повышение квалификации, на мероприятия по обеспечению информированности персонала в вопросах безопасности, а также на разработку официальных процедур выявления уязвимых мест систем и управления изменениями. Эти факторы имеют огромное значение для минимизации риска в отношении того, что преимущества технических средств обеспечения безопасности могут быть сведены на нет в результате ошибки персонала или его недостаточной подготовки. Жесткая система контроля работы с паролями и правами доступа также весьма важна для предотвращения атаки изнутри компании со стороны недовольных сотрудников или деловых партнеров, имеющих прямой доступ к сетям и системам компании.

• *контроль стандартов информационной безопасности третьих сторон.*

Информационная технология проникает в каждый аспект ведения бизнеса и совершения операций. За последние годы компании и их деловые партнеры существенно увеличили объем взаимодействия через информационные системы. Сбой в системе безопасности в любой из этих организаций может подвергнуть риску целые отрасли и технологические процессы. Именно поэтому компаниям необходимо следить за тем, чтобы у основных деловых партнеров были внедрены хотя бы минимальные стандарты безопасности.

Компании должны осознать, что сегодня информационная безопасность стала аспектом бизнеса и ее важность нельзя недооценивать. Информационная безопасность – это не роскошь, а необходимость, так как именно она составляет тот фундамент, на котором строится надежная среда, позволяющая компаниям успешно работать и развиваться.

© «Эрнст энд Янг», 2003

Приложение 3 РУКОВОДСТВО ПО ИНФОРМАЦИОННОЙ

БЕЗОПАСНОСТИ ПРЕДПРИЯТИЯ (Site Security Handbook, RFC 1244)

Приводится в сокращенном варианте, с разрешения доктора физико-математических наук, профессора В.А Галатенко (автора перевода оригинального документа). Данное руководство является продуктом деятельности рабочей группы по политике информационной безопасности предприятий (SSPHWG), в которую вошли представители групп безопасности и пользовательских сервисов движения IETF (Internet Engineering Task Force). Авторами руководства являются Dave Curry (Purdue University), Sean Kirkpatrick (Unisys), Tom Longstaff (LLNL), Greg Hollingsworth (Johns Hopkins University), Jeffrey Carpenter (University of Pittsburgh), Barbara Fraser (CERT), Fred Ostapik (SRINISC), Allen Sturtevant (LLNL), Dan Long (BBN),Jim Duncan (Pennsylvania State University), Frank Byrum (DEC). Руководство содержит информацию для интернет-сообщества, оно не является стандартом, его распространение не ограничено.

Выработка официальной политики предприятия в области информационной безопасности

Краткий обзор *Организационные вопросы.* Целью разработки официальной политики предприятия в области информационной безопасности является определение правильного (с точки зрения организации) способа использования вычислительных и коммуникационных ресурсов, а также определение процедур, предотвращающих или реагирующих на нарушения режима безопасности. Чтобы достичь данной цели, следует учесть специфику конкретной организации.

Во-первых, необходимо принять во внимание цели и основные направления деятельности организации. Например, на военной базе и в университете существенно разные требования к конфиденциальности.

Во-вторых, разрабатываемая политика должна согласовываться с существующими законами и правилами, относящимися к организации. Значит, эти законы и правила необходимо выявить и принять во внимание при разработке политики.

В-третьих, если локальная сеть организации не является изолированной, вопросы безопасности следует рассматривать в более широком контексте. Политика должна освещать проблемы, возникающие на локальном компьютере из-за действий удаленной стороны, а также проблемы, причиной которых является локальный хост или удаленный пользователь.

Кто разрабатывает политику? Политика безопасности должна стать результатом совместной деятельности технического персонала, понимающего все аспекты политики и ее реализации, а также руководителей, влияющих на проведение политики в жизнь. Нереализуемая или неподдерживаемая политика бесполезна.

Поскольку политика безопасности так или иначе затрагивает всех сотрудников организации, следует позаботиться о том, чтобы у вас было достаточно полномочий для принятия решений по этим вопросам. Хотя некоторой группе (например, группе технического обслуживания) может быть поручено проведение политики в жизнь, возможно, нужна будет и группа более высокого ранга для поддержки и одобрения политики.

Кого затрагивает политика? Политика безопасности потенциально затрагивает всех пользователей компьютеров в организации, причем по нескольким аспектам. Пользователи могут отвечать за администрирование собственных паролей. Системные администраторы обязаны ликвидировать слабые места в защите и надзирать за работой всех систем.

Важно с самого начала работы над политикой безопасности правильно подобрать состав коллектива разработчиков. Возможно, на предприятии уже есть группа информационной безопасности; естественно, люди из этой группы считают безопасность своей вотчиной. Следует привлечь также специалистов по аудиту и управлению, по физической безопасности, по информационным системам и т. п. Тем самым будет подготовлена почва для одобрения политики.

Распределение ответственности. Ключевым элементом политики является доведение до каждого его обязанностей по поддержанию режима безопасности. Политика не может

предусмотреть всего, однако она обязана гарантировать, что для каждого вида проблем существует ответственный.

В связи с информационной безопасностью можно выделить несколько уровней ответственности. На первом уровне каждый пользователь компьютерного ресурса обязан заботиться о защите своего счета. Пользователь, допустивший компрометацию своего счета, увеличивает вероятность компрометации других счетов и ресурсов.

Системные администраторы образуют следующий уровень ответственности. Они должны обеспечивать защиту компьютерных систем. Сетевых администраторов можно отнести к еще более высокому уровню.

Оценка рисков *Общие положения.* Один из главных побудительных мотивов выработки политики безопасности – обеспечить уверенность в том, что деятельность по защите информации построена экономически оправданным образом. Данное положение кажется очевидным, но, вообще говоря, возможны ситуации, когда усилия прикладываются не там, где нужно. Например, много говорят и пишут о хакерах; в то же время в большинстве обзоров по информационной безопасности утверждается, что в типичной организации ущерб от внутренних, «штатных» злоумышленников значительно больше.

Процесс анализа рисков включает в себя определение того, что следует защищать, от чего защищать и как это делать. Необходимо рассмотреть все возможные риски и ранжировать их в зависимости от потенциального размера ущерба. Этот процесс состоит из множества экономических решений. Давно замечено, что затраты на защиту не должны превышать стоимости защищаемого объекта. Полное рассмотрение проблемы анализа рисков выходит за пределы данной публикации. Тем не менее в следующих пунктах будут затронуты два этапа процесса анализа рисков:

• идентификация активов,

• идентификация угроз.

Главной целью деятельности в области информационной безопасности является обеспечение доступности, конфиденциальности и целостности каждого актива. При анализе угроз следует принимать во внимание их воздействие на активы по трем названным направлениям. *Идентификация активов.* Один из этапов анализа рисков состоит в идентификации всех объектов, нуждающихся в защите. Некоторые активы (например, аппаратура) идентифицируются очевидным образом. Про другие (например, про людей, использующих информационные системы) нередко забывают. Необходимо принять во внимание все, что может пострадать от нарушений режима безопасности.

В свое время Pfleeger предложил следующую классификацию активов:

• *аппаратура* – процессоры, модули, клавиатуры, терминалы, рабочие станции, персональные компьютеры, принтеры, дисководы, коммуникационные линии, терминальные серверы, маршрутизаторы;

• *программное обеспечение* – исходные тексты, объектные модули, утилиты, диагностические программы, операционные системы, коммуникационные программы;

• *данные* – обрабатываемые, непосредственно доступные, архивированные, сохраненные в виде резервной копии, регистрационные журналы, базы данных, передаваемые по коммуникационным линиям;

• *люди* – пользователи, обслуживающий персонал;

• *документация* – по программам, по аппаратуре, системная, по административным процедурам;

• *расходные материалы* – бумага, формы, красящая лента, магнитные носители.

Идентификация угроз. После того как выявлены активы, нуждающиеся в защите, необходимо идентифицировать угрозы этим активам и размеры возможного ущерба. Это поможет понять, каких угроз следует опасаться больше всего. Это могут быть следующие угрозы:

несанкционированный доступ;

Несанкционированный доступ к компьютерным ресурсам – угроза, типичная для

большинства организаций. Несанкционированный доступ может принимать различные формы. Иногда это нелегальное использование счета другого пользователя для получения доступа к системе. В других случаях ресурсами пользуются без предварительно полученного разрешения.

Степень важности проблемы несанкционированного доступа для разных организаций не одинакова. Порой передача прав доступа неавторизованному пользователю может привести к разрушению магнитных носителей. Чаще несанкционированный доступ облегчает исполнение других угроз. Различается и степень вероятности нападения: некоторые организации (известные университеты, правительственные и военные учреждения) как бы притягивают к себе злоумышленников. Следовательно, риск несанкционированного доступа меняется от предприятия к предприятию.

нелегальное ознакомление с информацией;

Нелегальное ознакомление с информацией – другая распространенная угроза. Определите степень конфиденциальности информации, хранящейся в ваших компьютерах. Расшифровка файла паролей откроет дорогу несанкционированному доступу. Мимолетный взгляд на ваше коммерческое предложение может дать конкуренту решающее преимущество. Техническая статья способна вместить в себя годы напряженных исследований.

отказ в обслуживании.

Компьютеры и сети предоставляют своим пользователям множество ценных услуг, от которых зависит эффективная работа многих людей. Когда услуги вдруг становятся недоступными, страдает производительность труда. Отказ в обслуживании возникает по разным причинам и проявляется по-разному. Сеть может прийти в неработоспособное состояние от поддельного пакета, от перегрузки или по причине отказа компонента. Вирус способен замедлить или парализовать работу компьютерной системы. Каждая организация должна определить для себя набор необходимых сервисов и для каждого из них проанализировать последствия его недоступности.

Политические вопросы При разработке политики безопасности необходимо дать ответы на ряд вопросов, а именно:

• Кто имеет право использовать ресурсы?

• Как правильно использовать ресурсы?

• Кто наделен правом давать привилегии и разрешать использование?

• Кто обладает административными привилегиями?

• Каковы права и обязанности пользователей?

• Каковы права и обязанности системных администраторов по отношению к обычным пользователям?

• Как работать с конфиденциальной информацией?

Кто имеет право использовать ресурсы? Одним из шагов в разработке политики безопасности является определение того, кто может использовать Ваши системы и сервисы. Должно быть явно указано, кому дается право использовать те или иные ресурсы. *Как правильно использовать ресурсы?* После определения круга лиц, имеющих доступ к системным ресурсам, необходимо описать правильные и неправильные способы использования ресурсов. Для разных категорий пользователей (студентов, внешних пользователей, штатных сотрудников и т. д.) эти способы могут различаться. Должно быть явно указано, что допустимо, а что нет. Могут быть описаны также ограничения на использование определенных ресурсов. При этом вам придется специфицировать уровни доступа разных групп пользователей.

Пользователи должны знать, что они несут ответственность за свои действия независимо от применяемых защитных средств и что использовать чужие счета и обходить механизмы безопасности запрещено.

Для регламентации доступа к ресурсам нужно дать ответы на следующие вопросы:

• Разрешается ли использование чужих счетов?

• Разрешается ли отгадывать чужие пароли?

• Разрешается ли разрушать сервисы?

• Должны ли пользователи предполагать, что если файл доступен всем на чтение, то они имеют право его читать?

• Имеют ли право пользователи модифицировать чужие файлы, если по каким-либо причинам у них есть доступ на запись?

• Должны ли пользователи разделять счета?

В большинстве случаев ответы на подобные вопросы будут отрицательными. В политике могут найти отражение авторские и лицензионные права на программное обеспечение. Лицензионное соглашение с поставщиком налагает на организацию определенные обязательства; чтобы не нарушить их, необходимо приложить некоторые усилия. Кроме того, вы, возможно, захотите проинформировать пользователей, что присваивать защищенное авторскими правами программное обеспечение запрещено законом.

Точнее, вы должны довести до сведения пользователей, что копировать авторское и лицензионное программное обеспечение запрещено, за исключением явно оговоренных случаев. Они всегда могут узнать авторский/лицензионный статус программного обеспечения. В случае сомнений копировать не следует.

Политика в области правильного использования ресурсов очень важна. Если явно не указано, что запрещено, вы не сможете доказать, что пользователь нарушил политику безопасности.

Бывают исключительные случаи, когда в исследовательских целях пользователи или администраторы пытаются «расколоть» защиту сервиса или лицензионной программы. Политика должна давать ответ на вопрос, разрешены ли подобные исследования в вашей организации и каковы могут быть их рамки.

Применительно к исключительным случаям следует дать ответы на такие вопросы:

• Разрешены ли вообще подобные исследования?

• Что именно разрешено: попытки проникновения, выращивание «червей» и вирусов и т. п.?

• Какие регуляторы должны использоваться для контроля за подобными исследованиями (например, их изоляция в рамках отдельного сегмента сети)?

• Как защищены пользователи (в том числе внешние) от подобных исследований?

• Как получать разрешение на проведение исследований?

В случае, когда получено разрешение на исследование, следует изолировать тестируемые сегменты от основной сети предприятия. «Черви» и вирусы не должны выпускаться в «живую» сеть. Возможно, вы захотите заключить контракт с отдельными людьми или сторонней организацией на предмет проверки защищенности ваших сервисов. Частью проверки могут стать попытки взлома систем. Это также должно найти отражение в политике вашего предприятия.

Кто наделен правом давать привилегии и разрешать использование? Политика безопасности должна давать ответ на вопрос, кто распоряжается правами доступа к сервисам. Кроме того, необходимо точно знать, какие именно права позволено распределять. Если вы не управляете процессом наделения правами доступа к вашей системе, вы не контролируете и круг пользователей. Если вы знаете, кто отвечает за распределение прав, вы всегда сможете узнать, давались ли определенные права конкретному пользователю или он получил их нелегально.

Существует много возможных схем управления распределением прав доступа к сервисам. При выборе подходящей целесообразно принять во внимание следующие моменты:

Будут ли права доступа распределяться централизованно или из нескольких мест?

Можно установить единый распределительный пункт или передать соответствующие права подразделениям и отделам. Все зависит от того, какое соотношение между

безопасностью и удобством вы считаете допустимым. Чем сильнее централизация, тем проще поддерживать режим безопасности.

Какие методы предполагается использовать для заведения счетов и запрещения доступа?

Вы должны проверить механизм заведения счетов с точки зрения безопасности. В наименее ограничительном режиме уполномоченные лица непосредственно входят в систему и заводят счета вручную или с помощью утилит. Обычно подобные утилиты предполагают высокую степень доверия к использующим их лицам, которые получают значительные полномочия. Если вы останавливаете свой выбор на таком режиме, вам необходимо найти достаточно надежного человека. Другой крайностью является применение интегрированной системы, которую запускают уполномоченные лица или даже сами пользователи. В любом случае, однако, остается возможность злоупотреблений.

Следует разработать и тщательно документировать специальные процедуры заведения новых счетов, чтобы избежать недоразумений и уменьшить число ошибок. Нарушение безопасности при заведении счетов возможно не только по злому умыслу, но и в результате ошибок. Наличие ясных и хорошо документированных процедур внушает уверенность, что подобные ошибки не случатся. Кроме того, необходимо удостовериться, что люди, исполняющие процедуры, понимают их.

Наделение пользователей правами доступа – одна из самых уязвимых процедур. Прежде всего, следует позаботиться, чтобы начальный пароль не был легко угадываемым. Целесообразно избегать использования начальных паролей, являющихся функцией от фамилии, имени и отчества пользователя. Не стоит автоматически генерировать начальные пароли, если результат генерации легко предсказуем. Далее, нельзя разрешать пользователям до бесконечности полагаться на начальный пароль. По возможности следует принуждать пользователей менять начальный пароль при первом входе в систему. Правда, даже такая мера бессильна против людей, которые вообще не пользуются своим счетом, сохраняя до бесконечности уязвимый начальный пароль. В некоторых организациях неиспользуемые счета уничтожают, заставляя их владельцев повторно проходить процедуру регистрации.

Кто обладает административными привилегиями? Одно из решений, которое должно быть тщательно взвешено, относится к выбору лиц, имеющих доступ к административным привилегиям и паролям для ваших сервисов. Очевидно, подобный доступ должны иметь системные администраторы, но неизбежны ситуации, когда за привилегиями будут обращаться другие пользователи, что следует с самого начала предусмотреть в политике безопасности. Ограничение прав – один из способов защититься от угроз со стороны своих пользователей. Необходим, однако, сбалансированный подход, когда ограничение прав не мешает людям делать свое дело. Разумнее всего давать пользователям ровно те права, которые нужны им для выполнения своих обязанностей.

Далее, сотрудники, имеющие специальные привилегии, должны быть подотчетны некоторому должностному лицу, и это также необходимо отразить в политике безопасности предприятия. Если «привилегированные» люди перестают быть подотчетными, вы рискуете потерять контроль над своей системой и лишиться возможности расследовать случаи нарушения режима безопасности.

Каковы права и обязанности пользователей? Политика безопасности должна содержать положения о правах и обязанностях пользователей применительно к использованию компьютерных систем и сервисов предприятия. Должно быть явно оговорено, что пользователи обязаны понимать и выполнять правила безопасной эксплуатации систем. Ниже приведен перечень тем, которые целесообразно осветить в данном разделе политики безопасности:

• Каковы общие рамки использования ресурсов? Существуют ли ограничения на ресурсы и каковы они?

• Что является злоупотреблением с точки зрения производительности системы?

• Разрешается ли пользователям совместное использование счетов?

• Как «секретные» пользователи должны охранять свои пароли?

• Как часто пользователи должны менять пароли? Каковы другие аналогичные ограничения и требования?

• Как обеспечивается резервное копирование – централизованно или индивидуально?

• Как реагировать на случаи просмотра конфиденциальной информации?

• Как соблюдается конфиденциальность почты?

• Какова политика в отношении неправильно адресованной почты или отправлений по спискам рассылки, или в адрес дискуссионных групп (непристойности, приставания и т. п.)?

• Какова политика по вопросам электронных коммуникаций (подделка почты и т. п.)?

Ассоциация электронной почты (The Electronic Mail Association, EMA) подготовила статью о конфиденциальности электронной почты в организациях. Основное положение статьи состоит в том, что каждая организация должна разработать политику защиты права сотрудников на тайну. Рекомендуется, чтобы эта политика охватывала все возможные среды, а не только электронную почту. Предлагается пять критериев оценки подобной политики:

• Согласуется ли политика с существующим законодательством и с обязанностями по отношению к третьим сторонам?

• Не ущемляются ли без нужды интересы работников, работодателей или третьих сторон?

• Реалистична ли политика и вероятно ли ее проведение в жизнь?

• Затрагивает ли политика все виды передачи и хранения информации, используемые в организации?

• Объявлена ли политика заранее и получила ли она одобрение всех заинтересованных сторон?

Каковы права и обязанности системных администраторов по отношению к обычным пользователям? Должен соблюдаться баланс между правом пользователей на тайну и обязанностью системного администратора собирать достаточно информации для разрешения проблем и расследования случаев нарушения режима безопасности. Политика должна определять границы, в пределах которых системный администратор вправе исследовать пользовательские файлы с целью разрешения проблем и для иных нужд, и каковы права пользователей. Можно также сформулировать положение относительно обязанности администраторов соблюдать конфиденциальность информации, полученной при оговоренных выше обстоятельствах. Политика должна содержать ответы на несколько вопросов: • Может ли администратор отслеживать или читать пользовательские файлы при каких-либо обстоятельствах?

• Какие обязательства администратор при этом берет на себя?

• Имеют ли право сетевые администраторы исследовать сетевой трафик?

Как работать с конфиденциальной информацией? Прежде чем предоставлять пользователям доступ к вашим сервисам, следует определить, каков уровень защиты данных на вашей системе. Тем самым вы сможете определить уровень конфиденциальности информации, которую пользователи могут у вас размещать. Наверное, вы не хотите, чтобы пользователи хранили секретные сведения на компьютерах, которые Вы не собираетесь как следует защищать. Следует сообщить пользователям, какие сервисы (при наличии таковых) пригодны для хранения конфиденциальной информации. Должны рассматриваться различные способы хранения данных (на диске, ленте, файловом сервере и т. д.). Этот аспект политики должен быть согласован с правами системных администраторов по отношению к обычным пользователям (см. предыдущий пункт).

Что делать, когда политику безопасности нарушают Очевидно, что любая официальная политика, вне зависимости от ее отношения к информационной безопасности, время от времени нарушается. Нарушение может явиться следствием пользовательской небрежности, случайной ошибки, отсутствия должной информации о текущей политике или ее непонимания. Возможно также, что некое лицо или группа лиц сознательно совершают действия, прямо противоречащие утвержденной политике безопасности. Необходимо

заранее определить характер действий, предпринимаемых в случае обнаружения нарушений политики, ведь эти действия должны быть быстрыми и правильными. Следует организовать расследование, чтобы понять, как и почему нарушение стало возможным. После этого нужно внести коррективы в систему защиты. Тип и серьезность корректив зависят от характера случившегося нарушения.

Выработка ответа на нарушение политики. Политику безопасности могут нарушать самые разные лица. Некоторые из них являются своими, местными пользователями, другие нападают извне. Полезно определить сами понятия «свои» и «чужие», исходя из административных, правовых или политических положений. Эти положения очерчивают характер санкций, которые можно применить к нарушителю – от письменного выговора до привлечения к суду. Таким образом, последовательность ответных действий зависит не только от типа нарушения, но и от вида нарушителя; она должна быть продумана задолго до первого инцидента, хотя это и непросто.

Следует помнить, что правильно организованное обучение – лучшая защита. Вы обязаны поставить дело так, чтобы не только внутренние, но и внешние легальные пользователи знали положения вашей политики безопасности. Если вы будете располагать свидетельством подобного знания, это поможет вам в будущих правовых акциях, когда таковые понадобятся.

Проблемы с нелегальными пользователями, в общем, те же. Нужно получить ответы на вопросы о том, какие типы пользователей нарушают политику, как и зачем они это делают. В зависимости от результатов расследования вы можете просто заткнуть дыру в защите и удовлетвориться полученным уроком или предпочтете более жесткие меры.

Что делать, когда местные пользователи нарушают политику безопасности сторонней организации? Каждое предприятие должно заранее определить набор административных санкций, применяемых к местным пользователям, нарушающим политику безопасности сторонней организации. Кроме того, необходимо позаботиться о защите от ответных действий сторонней организации. При выработке политики безопасности следует учесть все юридические положения, применимые к подобным ситуациям.

Спецификация контактов с внешними организациями и определение ответственных. Политика безопасности предприятия должна содержать процедуры для взаимодействия с внешними организациями, в число которых входят правоохранительные органы, другие организации, команды «быстрого реагирования» (CERT, CIAC), средства массовой информации. В процедурах должно быть определено, кто имеет право на такие контакты и как именно они совершаются.

Среди прочих нужно дать ответы на следующие вопросы:

• Кто может разговаривать с прессой?

• Когда следует обращаться в правоохранительные органы?

• Если соединение выполняется из сторонней организации, имеет ли право системный администратор обратиться в эту организацию?

• Какого рода сведения об инцидентах могут выходить за пределы организации?

Детальная информация по контактам должна быть постоянно доступна вместе с ясно определенными процедурами отработки этих контактов. *Каковы обязанности по отношению к соседям и другим пользователям Интернета?* Рабочая группа по политике безопасности (Security Policy Working Group, SPWG) интернет-сообщества опубликовала документ под названием «Основы политики для безопасной работы в Интернет». В нем Интернет трактуется как совместное предприятие, в котором пользователи должны помогать друг другу в поддержании режима безопасности. Это положение следует учитывать при разработке политики предприятия. Главный вопрос состоит в том, какой информацией можно делиться с соседями. Ответ зависит как от типа организации (военная, учебная, коммерческая и т. д.), так и от характера случившегося нарушения.

Процедурные вопросы реагирования на нарушения. Помимо политических положений,

необходимо продумать и написать процедуры, исполняемые в случае обнаружения нарушений режима безопасности. Данный вопрос подробно рассматривается в следующем разделе. Для всех видов нарушений должны быть заготовлены соответствующие процедуры.

Пресекать или следить? Когда на организацию совершается нападение, грозящее нарушением информационной безопасности, стратегия ответных действий может строиться под влиянием двух противоположных подходов. Если руководство опасается уязвимости предприятия, оно может предпочесть стратегию «защититься и продолжить». Главной целью подобного подхода является защита информационных ресурсов и максимально быстрое восстановление нормальной работы пользователей. Действиям нарушителя оказывается максимальное противодействие, дальнейший доступ предотвращается, после чего немедленно начинается процесс оценки нанесенных повреждений и восстановления. Возможно, при этом придется выключить компьютерную систему, закрыть доступ в сеть или предпринять иные жесткие меры. Оборотная сторона данной медали состоит в том, что пока злоумышленник не выявлен, он может вновь напасть на эту же или другую организацию прежним или новым способом.

Другой подход, «выследить и осудить», опирается на иные философию и систему целей. Основная цель состоит в том, чтобы позволить злоумышленнику продолжать свои действия, пока организация не сможет установить его личность. Такой подход нравится правоохранительным органам. К сожалению, эти органы не смогут освободить организацию от ответственности, если пользователи обратятся в суд с иском по поводу ущерба, нанесенного их программам и данным.

Судебное преследование – не единственный возможный исход установления личности нарушителя. Если виновным оказался штатный сотрудник или студент, организация может предпочесть дисциплинарные меры. В политике безопасности должны быть перечислены допустимые варианты наказания и критерии выбора одного или нескольких из них в зависимости от личности виновного.

Руководство организации должно заранее тщательно взвесить различные возможности при выборе стратегии ответных действий. В принципе стратегия может зависеть от конкретных обстоятельств нападения. Возможен и выбор единой стратегии на все случаи жизни. Нужно принять во внимание все за и против и проинформировать пользователей о принятом решении, чтобы они в любом случае осознавали степень своей уязвимости.

Следующий контрольный перечень помогает сделать выбор между стратегиями «защититься и продолжить» и «выследить и осудить». При каких обстоятельствах следует предпочесть стратегию «защититься и продолжить»:

• активы организации недостаточно защищены;

• продолжающееся вторжение сопряжено с большим финансовым риском;

• нет возможности или намерения осудить злоумышленника;

• неизвестен круг пользователей;

• пользователи неопытны, а их работа уязвима;

• пользователи могут привлечь организацию к суду за нанесенный ущерб.

При каких обстоятельствах следует предпочесть стратегию «выследить и осудить»: • активы и системы хорошо защищены;

• имеются хорошие резервные копии;

• угроза активам организации меньше потенциального ущерба от будущих повторных вторжений;

• имеет место согласованная атака, повторяющаяся с большой частотой и настойчивостью;

• организация притягивает злоумышленников и, следовательно, подвергается частым атакам;

• организация готова идти на риск, позволяя продолжить вторжение;

• действия злоумышленника можно контролировать;

• доступны развитые средства отслеживания, так что преследование нарушителя имеет

хорошие шансы на успех;

• обслуживающий персонал обладает достаточной квалификацией для успешного выслеживания;

• руководство организации желает осудить злоумышленника;

• системный администратор знает, какого рода информация обеспечит успешное преследование;

• имеется тесный контакт с правоохранительными органами;

• в организации есть человек, хорошо знающий соответствующие законы;

• организация готова к искам собственных пользователей по поводу программ и данных, скомпрометированных во время выслеживания злоумышленника.

Толкование политики безопасности. Важно определить, кто будет интерпретировать политику безопасности. Это может быть отдельное лицо или комитет. Вне зависимости от того, насколько хорошо она написана, политика безопасности время от времени нуждается в разъяснении, а заодно и в пересмотре. *Гласность политики безопасности.* После того как положения политики безопасности записаны и одобрены, необходимо начать активный процесс, гарантирующий, что политика воспринята и обсуждена. Почтовую рассылку нельзя признать достаточной мерой. Прежде чем политика вступит в силу, следует отвести время для дискуссий, чтобы все заинтересованные пользователи могли высказать свое мнение и указать на недостатки политики. В идеале политика должна соблюдать баланс между безопасностью и производительностью труда.

Целесообразно провести собрания, чтобы выслушать пожелания пользователей и заодно убедиться в правильном понимании ими предложенной политики. (Творцы политики порой бывают несколько косноязычны.) В собраниях должны участвовать все – от высшего руководства до младших специалистов. Безопасность – забота общая.

Помимо усилий по оглашению политики на начальном этапе, необходимо постоянно напоминать о ней. Опытные пользователи нуждаются в периодических напоминаниях, новичкам ее нужно разъяснять, вводя в курс дела. Прежде чем допускать сотрудника к работе, разумно получить его подпись под свидетельством о том, что он прочитал и понял политику безопасности. В ситуациях, чреватых судебным разбирательством после нарушения политики, бумага с подписью может оказаться весьма кстати.

Выработка процедур для предупреждения нарушений безопасности Политика безопасности определяет, что нуждается в защите. В данной главе обсуждаются процедуры безопасности, специфицирующие, каким образом политика будет проводиться в жизнь.

Политика безопасности определяет, что следует защищать Политика безопасности отвечает на вопрос *что:* что следует защищать, что является самым важным, что за свойства у защищаемых объектов, что за подход к проблемам безопасности избран.

Сама по себе политика безопасности не говорит, *как* защищаются объекты. Ответы на вопросы *как* дают процедуры безопасности, рассматриваемые в данной главе. Политика безопасности оформляется в виде высокоуровневого документа, описывающего общую стратегию. Процедуры безопасности должны в деталях специфицировать шаги, предпринимаемые организацией для собственной защиты.

Политика безопасности должна включать в себя общую оценку рисков по отношению к наиболее вероятным угрозам и оценку возможных последствий осуществления этих угроз Частью процесса оценки рисков является составление списка активов, нуждающихся в защите. Данная информация необходима для выработки экономически эффективных (практичных) процедур.

Заманчиво начать разработку процедур безопасности, отправляясь от защитных механизмов: «На всех компьютерах нашей организации должны вестись регистрационные журналы, модемы обязаны выполнять обратный дозвон, а всем пользователям необходимо выдать интеллектуальные карточки». Однако подобный подход может повести к массированной защите областей с небольшим риском и к недостаточной защите

действительно уязвимых участков. Если же начать с политики и описанных ею рисков, можно быть уверенным, что процедуры обеспечивают достаточный уровень защиты для всех активов.

Выявляя возможные проблемы Чтобы определить риски, необходимо выявить уязвимые места. Одна из целей политики безопасности состоит в том, чтобы прикрыть слабости и тем самым уменьшить риск для максимально возможного числа активов. В последующих пунктах представлены наиболее типичные слабости. Данный перечень ни в коей мере нельзя считать исчерпывающим. Кроме того, следует учитывать, что обычно у каждой организации имеется несколько уникальных, присущих только ей уязвимых мест.

Точки доступа. Точки доступа обычно используются авторизованными пользователями для входа в систему. Наличие большого числа точек доступа увеличивает риск нелегального доступа к компьютерам организации и другим сетевым ресурсам.

Связь с внешними сетями открывает доступ к ресурсам организации всем лицам, подключенным к этим внешним сетям. Обычно сетевое соединение обеспечивает доступ к большому числу сервисов, каждый из которых может быть скомпрометирован.

Коммутируемые линии, в зависимости от конфигурации, могут дать доступ только к входному порту одной системы или ко всей сети, если они подключены к терминальному серверу.

Терминальные серверы сами по себе могут стать источником проблем, поскольку зачастую они лишены средств проверки подлинности пользователей. Нередко злоумышленники для сокрытия своих действий используют именно терминальные серверы, соединяясь с ними по местному телефону и уже через них выходя в локальную сеть. Некоторые терминальные серверы сконфигурированы таким образом, что к ним можно получить доступ по Telnet, находясь вне локальной сети, и затем выполнить Telnet во внешний мир, что существенно затрудняет отслеживание злоумышленников.

Неправильно сконфигурированные системы. Значительная часть «дыр» в защите приходится на неправильно сконфигурированные системы. Современные операционные системы и сопутствующее им программное обеспечение стали настолько сложными, что для досконального изучения деталей их работы нужно брать отдельного специалиста на полную ставку. Зачастую системные администраторы не являются такими специалистами, поскольку просто выбираются из числа имеющихся сотрудников.

Отчасти в неправильной конфигурации повинны поставщики, поскольку в целях упрощения процесса установки они выбирают начальные конфигурации, которые при определенных условиях являются небезопасными.

Программные ошибки. Программное обеспечение никогда не станет безошибочным. Обычным методом несанкционированного доступа является использование ошибок в защитных средствах. Частичным решением проблемы является получение информации об обнаружении подобных ошибок и внесение соответствующих исправлений в программы. Об ошибках необходимо сообщать поставщику, чтобы исправления вносились и распространялись централизованно.

Внутренние враги. Штатные сотрудники могут составлять значительную угрозу для информационной безопасности организации. Зачастую они имеют непосредственный доступ к аппаратным компонентам компьютеров и сетевых устройств. Наличие такого доступа облегчает компрометацию большинства систем. Так, в случае настольных рабочих станций, нетрудно получить привилегии суперпользователя. В случае локальной сети можно отслеживать всю передаваемую информацию, в том числе и конфиденциальную.

Выбор регуляторов для практической защиты активов После того как выяснено, что нуждается в защите и оценены риски, грозящие активам, необходимо решить, как реализовать средства защиты. Регуляторы и защитные механизмы следует выбирать так, чтобы успешно и в то же время экономически эффективно противостоять угрозам, выявленным в процессе анализа рисков. Нет смысла тратить большие суммы денег и без нужды ограничивать доступ пользователей там, где риск нападения невелик.

Выбор подходящего набора регуляторов безопасности. Выбранные вами регуляторы представляют собой реальное воплощение вашей политики безопасности. Они образуют первую (и главную) линию обороны. В этой связи особенно важно, чтобы регуляторы в совокупности составляли правильный набор. Если наибольшую угрозу для вашей системы составляют внешние злоумышленники, то, как правило, нет смысла использовать биометрические устройства для аутентификации обычных, внутренних пользователей. Если, с другой стороны, основная опасность состоит в неавторизованном использовании вычислительных ресурсов внутренними пользователями, вы, вероятно, захотите воспользоваться очень строгими процедурами автоматического учета совершаемых действий.

Доверяйте здравому смыслу. Здравый смысл – лучшее средство формирования политики безопасности. Тщательная проработка схем и механизмов безопасности – занятие увлекательное и в определенной степени необходимое, но едва ли имеет смысл тратить деньги и время на такую проработку, если без внимания остались простые регуляторы. Например, как бы тщательно ни была продумана система, построенная на основе существующих средств безопасности, один пользователь с плохо выбранным паролем способен поставить под удар всю организацию.

Используйте несколько стратегий защиты активов Другой метод защиты активов состоит в использовании нескольких стратегий.

При подобном подходе, если одна линия обороны оказывается прорванной, в дело вступает другая стратегия, то есть активы не остаются беззащитными. Комбинация нескольких несложных стратегий зачастую позволяет построить более надежную защиту, чем один, даже очень сложный, метод. Так, дополнением к традиционному механизму входа в систему могут служить модемы с обратным дозвоном, и число подобных примеров многоуровневой защиты активов можно умножать. Правда, с комбинированием стратегий легко переборщить, поэтому следует постоянно помнить, что же, собственно, защищается.

Физическая безопасность Давно известно, что если не обеспечена физическая защита, говорить о других аспектах информационной безопасности не имеет смысла. Имея физический доступ к машине, злоумышленник может остановить ее, перевызвать в привилегированном режиме, заменить диск или изменить его содержимое, внедрить «Троянского коня» или предпринять любое число других нежелательных акций, предотвратить которые крайне трудно.

Критически важные коммуникационные каналы, серверы и другие ключевые элементы должны быть сосредоточены в физически защищенных областях. Некоторые механизмы безопасности (например, сервер аутентификации Kerberos) выполняют свои функции только при условии физической защищенности.

Если вы не можете физически обезопасить машины, не следует слепо доверять им. Целесообразно ограничить доступ с менее защищенных машин в более защищенные. Особенно рискованно предоставлять незащищенным хостам право доверительного доступа (как в ОС UNIX посредством удаленных команд типа rsh).

Необходимо строго контролировать доступ к физически защищенным машинам или претендующим на звание таковых. Помните, что у технического и обслуживающего персонала, как правило, есть ключи от комнат.

Процедуры выявления неавторизованной деятельности Для обнаружения большинства видов неавторизованного использования компьютерных систем существуют несложные процедуры, применяющие стандартные средства операционных систем или опирающиеся на инструментарий, свободно доступный из различных источников.

Отслеживание использования систем. Системный мониторинг может выполняться как администратором, так и специально написанными программами. Мониторинг включает в себя просмотр различных частей системы в поисках чего-нибудь необычного. Некоторые простые способы решения данной задачи будут рассмотрены ниже.

Отслеживание использования систем очень важно выполнять на постоянной основе.

Бессмысленно выделять для мониторинга один день в месяце, поскольку нарушения режима безопасности зачастую длятся всего несколько часов. Только поддерживая постоянную бдительность, можно рассчитывать на своевременную реакцию на нарушения.

Инструменты для отслеживания использования систем. В данном пункте описываются инструменты и методы, позволяющие выявлять неавторизованное использование систем:

ведение регистрационных журналов;

Большинство операционных систем сохраняют в регистрационных файлах массу информации.

Регулярный анализ этих файлов обычно является первой линией обороны при определении неавторизованного использования систем:

– сравните текущий список активных пользователей с предыдущими записями о входах в систему. Большинство пользователей каждый день входят в систему и выходят из нее приблизительно в одно и то же время. Вход в «ненормальное» время может свидетельствовать об использовании системного счета злоумышленником;

– во многих системах накапливаются учетные записи с целью последующего выставления счетов. Эти записи также можно использовать для определения типичного профиля использования системы. Необычные записи могут быть следствием неавторизованной активности;

– обычно в системах существуют средства накопления регистрационной информации (например, syslog в ОС UNIX). Проверьте эту информацию на предмет необычных сообщений об ошибках, генерируемых программным обеспечением. Например, большое число неудачных попыток входа в течение короткого промежутка времени может свидетельствовать о попытках подобрать пароль;

– с помощью команд операционной системы, выводящих список выполняемых в данный момент процессов, можно выявить пользователей, запустивших программы, к которым они не имеют права обращаться, равно как и неавторизованные программы, запущенные нарушителем.

программы отслеживания;

Другие средства мониторинга можно сконструировать, комбинируя различные, на первый взгляд не связанные между собой, стандартные механизмы операционной системы. Например, контрольный список прав доступа к файлам и их владельцев в ОС UNIX нетрудно получить с помощью команд find и Is и сохранить как эталон. Затем периодически можно порождать новые списки и сравнивать их с эталоном (в ОС UNIX для этого имеется команда diff). Несовпадения, возможно, свидетельствуют о несанкционированных изменениях. Дополнительные средства доступны от третьих фирм-поставщиков и от организаций, распространяющих свободное программное обеспечение.

прочие средства.

Для отслеживания работы систем с целью выявления нарушений режима безопасности можно использовать и другие средства, даже если это не является их основным назначением. Например, сетевые мониторы способны обнаружить и зарегистрировать соединения от неизвестных организаций.

Меняйте расписание мониторинга. Задача системного мониторинга не такая страшная, как могло бы показаться. Системные администраторы могут выполнять многие команды, используемые для мониторинга, периодически в течение дня, заполняя ими паузы (например, во время телефонного разговора). Это лучше, чем действовать строго по расписанию, При частом выполнении команд вы быстрее привыкнете к «нормальным» результатам и будете легче обнаруживать аномалии. Кроме того, варьируя время мониторинга, вы сделаете свои действия менее предсказуемыми для злоумышленников. Например, если злоумышленник знает, что каждый день в 17:00 проверяется, все ли вышли из системы, он просто переждет момент проверки и войдет позже. Но он не может предсказать, когда системный администратор выполнит команду вывода списка активных

пользователей. Тем самым риск быть обнаруженным для злоумышленника существенно возрастает. Несмотря на достоинства, которыми обладает постоянный мониторинг, некоторые злоумышленники могут знать о стандартных регистрационных механизмах атакуемых систем. В результате возможно активное противодействие и выведение этих механизмов из строя. Таким образом, обычное отслеживание полезно для обнаружения нарушителей, но оно не гарантирует безопасности вашей системы, как не гарантирует оно и безошибочного выявления неавторизованных действий.

Что делать при подозрениях на неавторизованную деятельность В дополнение к политике необходимо выписать процедуры реагирования на вторжения. Ответы на следующие вопросы должны стать частью процедур безопасности:

• Кто имеет право решать, что именно делать?

• Следует ли обращаться в правоохранительные органы?

• Должна ли ваша организация сотрудничать с другими предприятиями в попытках выследить нарушителя?

Независимо от того, предпочтете ли вы пресекать действия нарушителя или следить за ним, вам необходимо держать наготове соответствующие инструменты, предварительно научившись ими пользоваться. Не ждите вторжения, чтобы овладеть методами отслеживания действий злоумышленников, вам будет не до того.

Оглашая политику безопасности Чтобы политика безопасности действительно работала, ее необходимо довести до сведения пользователей и системных администраторов. Ниже объясняется, что и как следует говорить этим людям.

Обучая пользователей. Пользователи должны знать, как правильно использовать компьютерные системы и как защитить себя от неавторизованных лиц. Существует несколько способов такой защиты:

правильное использование системных счетов и/или рабочих станций;

Всем пользователям необходимо разъяснить, что подразумевается под «правильным» использованием системных счетов и рабочих станций. Проще всего это сделать, когда пользователь получает новый счет и, одновременно, брошюру с текстом политики безопасности. Политика использования обычно должна определять, разрешается ли применять счет или рабочую станцию для личных надобностей (ведение домашней бухгалтерии, подготовка писем), для извлечения доходов, для игр и т. д. В политике могут также содержаться положения, касающиеся лицензионных вопросов. Например, многие университеты имеют учебные лицензии, явным образом запрещающие коммерческое использование систем.

процедуры администрирования счета и/или рабочей станции;

Каждому пользователю необходимо объяснить, как правильно администрировать счет и/или рабочую станцию. В частности, пользователь должен усвоить, как защищать файлы, как выходить из системы или блокировать терминал либо рабочую станцию и т. п. По большей части подобная информация содержится в документации для новичков, поставляемой вместе с операционной системой, хотя во многих организациях предпочитают делать свои дополнения, учитывающие местную специфику.

Если компьютеры вашей организации открыты для модемного доступа по коммутируемым линиям, необходимо проинформировать пользователей об опасностях, присущих подобным конфигурациям. Например, прежде чем получить право на модемный доступ, пользователи должны усвоить, что следует сначала выходить из системы и только потом вешать трубку.

В свою очередь наличие доступа к системе через локальные или глобальные сети несет с собой свой набор проблем безопасности, которые нужно довести до сведения пользователей. Файлы, придающие статус доверенных удаленным хостам или пользователям, должны быть изучены досконально.

выявление нелегального использования счета;

Пользователям необходимо объяснить, как выявлять случаи нелегального

использования их счетов. Если при входе в систему выдается время предыдущего входа, пользователи должны его контролировать на предмет согласованности со своими прошлыми действиями.

Командные интерпретаторы некоторых операционных систем (например, C-shell в ОС UNIX) поддерживают историю выполнения команд. Целесообразно время от времени заглядывать в историю, чтобы проверять, не пользовались ли данным счетом другие лица для выполнения своих команд.

процедуры доклада о проблемах.

Должны быть разработаны процедуры, позволяющие пользователям докладывать о замеченных проблемах, связанных с неправильным использованием счета или с другими аспектами безопасности. Пользователям следует сообщить имя и телефон администратора безопасности или соответствующий адрес электронной почты (например, security).

Обучая администраторов хостов. Во многих организациях компьютерные системы администрируются самыми разными людьми. Эти люди должны знать, как защищать свою систему от атак и неавторизованного использования и как сообщать о случаях успешного проникновения в назидание коллегам. Для этого применяются следующие процедуры: *процедуры администрирования счетов;*

Администрирование счетов требует осторожности. При начальной установке системы с дистрибутива следует проверить элементы файла паролей, соответствующие «стандартным» счетам, заведенным поставщиком. Многие поставщики заводят счета для административного и обслуживающего персонала вообще без паролей или с общеизвестными паролями. Следует или дать новые пароли, или аннулировать ненужные счета.

Иметь счета без паролей очень опасно, поскольку они открывают свободный доступ в систему. Даже счета, при входе по которым запускается не командный интерпретатор, а другая программа (например, программа вывода списка активных пользователей), могут быть скомпрометированы, если установки выполнены некорректно. Опасны и средства «анонимной» передачи файлов (FTP), позволяющие пользователям всей сети входить в вашу систему для перекачки файлов из (обычно) защищенных дисковых областей. Вы должны тщательно взвесить выгоды от наличия счета без пароля в сравнении с риском несанкционированного доступа к системе.

Если операционная система поддерживает «теневые» файлы паролей (хранение паролей в отдельных файлах, доступных только привилегированным пользователям), ими нужно обязательно воспользоваться. В число таких систем входят UNIX System V, SunOS 4.0 или старше и некоторые другие. Поскольку зашифрованные пароли оказываются недоступны обычным пользователям, нападающий не сможет скопировать их на свою машину, чтобы на досуге заняться их раскрытием.

Отслеживайте использование привилегированных счетов (root в ОС UNIX или MAINT в VMS). Как только привилегированный пользователь увольняется или перестает нуждаться в привилегиях, следует изменить пароли всех привилегированных счетов.

процедуры конфигурационного управления;

При установке с дистрибутива операционной системы или дополнительного программного продукта необходимо тщательно проверить результирующую конфигурацию. Многие процедуры установки исходят из предположения надежности всех пользователей в организации, оставляя файлы общедоступными для записи или иным способом компрометируя безопасность.

Тщательной проверке должны подвергаться и сетевые сервисы. Часто поставщики в стандартной конфигурации предполагают надежность всех внешних хостов, что едва ли разумно, если речь идет о глобальной сети, такой, как Интернет.

Многие злоумышленники собирают информацию о слабостях конкретных версий систем. Чем старее версия, тем более вероятно наличие в ее защите известных ошибок, исправленных поставщиком в более поздних выпусках. В этой связи необходимо сопоставить риск от сохранения старой версии (с «дырами» в безопасности) и стоимость

перехода на новое программное обеспечение (включая возможные проблемы с продуктами третьих фирм). Из тех же соображений оценивается и целесообразность постановки «заплат», предоставляемых поставщиком, но с учетом того обстоятельства, что заплаты к системе безопасности, как правило, закрывают действительно серьезные дыры.

Другие исправления, полученные по электронной рассылке или аналогичным образом, обычно следует вносить, но только после тщательной проверки. Никогда не вносите исправления, если не уверены, что понимаете все последствия. Всегда есть опасность, что «исправление» предлагает злоумышленник, дабы открыть себе доступ в вашу систему.

процедуры сохранения и восстановления;

Невозможно переоценить важность хорошей стратегии резервного копирования. Наличие копии файловой системы не только выручит вас в случае поломки аппаратуры или нечаянного удаления данных, но и защитит от последствий несанкционированных изменений, внесенных злоумышленником. Без копии, действуя только по методу «максимального правдоподобия», трудно вернуть к первоначальному состоянию все то, что было злонамеренно модифицировано.

Резервные копии, особенно ежедневные, могут быть полезны и для прослеживания действий злоумышленника. Анализируя старые копии, нетрудно выяснить, когда система была скомпрометирована в первый раз. Нарушитель мог оставить следы в виде файлов, впоследствии удаленных, но оставшихся на копии. Резервные копии – это и материал для правоохранительных органов, расследующих компьютерные преступления.

Хорошая стратегия состоит в том, чтобы делать полную копию не реже одного раза в месяц. Частичные (или «инкрементальные») должны делаться не реже двух раз в неделю, а в идеале – каждый день. Предпочтительно использовать команды, специально предназначенные для сохранения файловых систем (dump в случае ОС UNIX или BACKUP на VMS), а не просто команды копирования файлов, поскольку первые обеспечивают возможность восстановления целостного состояния.

процедуры доклада о проблемах.

Как и пользователи, администраторы должны располагать конкретными процедурами доклада о проблемах, связанных с информационной безопасностью. Для больших конфигураций обычно заводят список электронной рассылки, в котором перечисляются все системные администраторы организации. Можно также организовать группу быстрого реагирования по типу CERT или «горячую» линию, обслуживаемую группой поддержки.

Ресурсы для предупреждения нарушений безопасности В этом разделе обсуждаются программные, аппаратные и процедурные ресурсы, которые могут быть использованы для поддержки вашей политики безопасности.

Сетевые соединения и межсетевые экраны. Противопожарные перегородки (firewalls) устанавливают в зданиях, чтобы воспрепятствовать проникновению пламени в защищаемые области. В русском языке получил распространение также термин «брандмауэр», обозначающий устройство аналогичного назначения в автомобиле. Оно защищает салон в случае возгорания двигателя. Применительно к компьютерным вопросам мы будем использовать термин «межсетевой экран». Аналогично, секретариат или приемная являются точками контроля за доступом посетителей в другие части офиса. Подобную технологию можно распространить и на информационную систему предприятия, особенно если речь идет о сетевых соединениях.

Некоторые сети соединяются только с другими сетями той же организации и не имеют выхода во внешний мир. Подобные организации менее уязвимы для угроз извне, хотя злоумышленник все же может воспользоваться коммуникационными каналами (например, коммутируемыми телефонными линиями). С другой стороны, многие организации связаны с другими предприятиями через глобальные сети, такие, как Интернет. Над подобными организациями нависают все опасности, типичные для сетевых сред.

Перед подключением к внешним сетям следует взвесить все «за» и «против». Разумно сделать доступными из внешнего мира только хосты, не хранящие критичной информации,

изолируя жизненно важные машины (например, с данными о финансовых или материальных ценностях). Если необходимо включиться в глобальную сеть, рассмотрите возможность ограничения доступа к вашей локальной сети через один хост. Иными словами, все информационные потоки из вашей локальной сети и в нее должны проходить через один хост, играющий роль противопожарной перегородки между вашей организацией и внешним миром. Эту экранирующую систему необходимо строго контролировать, защищать паролями, а функциональные возможности, доступные внешним пользователям, следует ограничить. С помощью такого подхода ваша организация сможет ослабить некоторые внутренние регуляторы безопасности в локальной сети, сохраняя прочно защищенный передний край.

Заметьте, что даже при наличии межсетевого экрана его компрометация может привести к компрометации всей прикрываемой локальной сети. Ведутся работы по созданию экранирующих систем, которые, даже будучи скомпрометированы, все же защищают локальную сеть.

Конфиденциальность. Конфиденциальность, то есть обеспечение скрытности или секретности, – одна из главных практических целей информационной безопасности. Большинство современных операционных систем предоставляют различные механизмы, которые дают пользователям возможность контролировать распространение информации. В зависимости от своих нужд организация может защищать все, может, напротив, все считать общедоступным или занимать место где-то в середине спектра, что большинство организаций и делает (во всяком случае, до первого нарушения режима безопасности).

Как правило, с информацией могут несанкционированно ознакомиться в трех местах: там, где она хранится (на компьютерных системах), там, где она передается (в сети), и там, где хранятся резервные копии (на лентах).

В первом случае для защиты используются права доступа к файлам, списки управления доступом и/или аналогичные механизмы. В последнем случае можно применить физическое ограничение доступа к лентам (например, заперев их в сейф). И во всех случаях помощь способны оказать криптографические средства:

шифрование (аппаратное и программное);

Шифрование – это процесс преобразования информации из читабельной формы в нечитабельную. Коммерчески доступны несколько криптографических пакетов, где шифрование реализовано аппаратно или программно. Аппаратное шифрование значительно быстрее программного; однако это достоинство может обернуться и недостатком, так как криптографические устройства могут стать объектом атаки злоумышленника, пожелавшего расшифровать вашу информацию методом грубой силы.

Преимущество криптографических методов состоит в том, что даже после компрометации других средств управления доступом (паролей, прав доступа к файлам и т. п.) информация остается для злоумышленника бесполезной. Естественно, ключи шифрования и аналогичные атрибуты должны защищаться не менее тщательно, чем файлы паролей.

Передаваемую по сети информацию могут перехватить. Для защиты от этой угрозы существует несколько методов, начиная от простого шифрования файлов перед передачей (шифрование из конца в конец) и кончая использованием специального сетевого оборудования, шифрующего всю передаваемую информацию без вмешательства пользователя (секретные каналы). Интернет в целом не использует секретные каналы, поэтому, если возникает необходимость, приходится использовать шифрование из конца в конец.

стандарт шифрования данных (Data Encryption Standard, DES);

Пожалуй, на сегодняшний день DES является наиболее употребительным механизмом шифрования. Существует ряд аппаратных и программных реализаций этого механизма, а некоторые компьютеры поставляются вместе с программной версией. DES преобразует обычный текст в шифрованный посредством специального алгоритма и «затравки»,

называемой ключом. До тех пор пока пользователь хранит (или помнит) ключ, он может вернуть текст из шифрованного состояния в обычное.

Одна из потенциальных опасностей любой системы шифрования состоит в необходимости помнить ключ, с помощью которого текст был зашифрован (это напоминает проблему с паролями, обсуждаемую в других разделах). Если ключ записать, он станет менее секретным. Если его забыть, расшифровка становится практически невозможной.

Большинство вариантов ОС UNIX предоставляют команду des, позволяющую шифровать данные с помощью DES-алгоритма.

crypt;

Как и команда des, команда crypt ОС UNIX позволяет шифровать информацию. К сожалению, алгоритм, использованный в реализации crypt, весьма ненадежен (он заимствован из шифровального устройства Enigma времен Второй мировой войны), так что файлы, зашифрованные данной командой, нетрудно расшифровать за несколько часов. Пользоваться командой crypt не рекомендуется, за исключением особо тривиальных случаев.

конфиденциальная почта (Privacy Enhanced Mail, PEM).

Обычно электронная почта передается по сети в открытом виде (то есть прочитать ее может каждый). Такое решение, конечно, нельзя назвать идеальным. Конфиденциальная почта предоставляет средства для автоматического шифрования электронных сообщений, так что лицо, осуществляющее прослушивание в узле распределения почты, не сможет (легко) эти сообщения прочитать. В настоящее время разрабатывается и распространяется по Интернету несколько пакетов конфиденциальной почты.

Группа по конфиденциальности интернет-сообщества разрабатывает протокол, предназначенный для использования в реализациях конфиденциальной почты.

Аутентификация источника данных. Обычно мы принимаем на веру, что в заголовке электронного сообщения отправитель указан правильно. Заголовок, однако, нетрудно подделать. Аутентификация источника данных позволяет удостоверить подлинность отправителя сообщения или другого объекта, подобно тому, как нотариус заверяет подпись на официальном документе. Цель достигается с помощью систем шифрования с открытыми ключами. Шифрование с открытыми ключами отличается от систем с секретными ключами несколькими моментами. Во-первых, в системе с открытыми ключами применяются два ключа – открытый, который каждый может использовать (иногда такой ключ называют публичным), и секретный, известный только отправителю сообщения. Отправитель использует секретный ключ для шифрования сообщения (как и в случае DES). Получатель, располагая открытым ключом отправителя, может впоследствии расшифровать сообщение.

В подобной схеме открытый ключ позволяет проверить подлинность секретного ключа отправителя. Тем самым более строго доказывается подлинность самого отправителя. Наиболее распространенной реализацией схемы шифрования с открытыми ключами является система RSA. Она использована и в стандарте Интернета на конфиденциальную почту (PEM).

Целостность информации. Говорят, что информация находится в целостном состоянии, если она полна, корректна и не изменилась с момента последней проверки «цельности». Для разных организаций важность целостности данных различна. Например, для военных и правительственных организаций сохранение режима секретности гораздо важнее истинности информации. С другой стороны, для банка важна прежде всего полнота и точность сведений о счетах своих клиентов.

На целостность системной информации влияют многочисленные программно-технические и процедурные механизмы. Традиционные средства управления доступом обеспечивают контроль над тем, кто имеет доступ к системной информации. Однако не всегда эти механизмы сами по себе достаточны для обеспечения требуемого уровня целостности. Рассмотрим некоторые дополнительные средства:

контрольные суммы;

В качестве простейшего средства контроля целостности можно использовать утилиту, которая подсчитывает контрольные суммы для системных файлов и сравнивает их с предыдущими известными значениями. В случае совпадения файлы, вероятно, не изменились; при несовпадении можно утверждать, что кто-то изменил их некоторым неизвестным способом.

Оборотной стороной простоты и легкости реализации является ненадежность механизма контрольного суммирования. Целенаправленный злоумышленник без труда добавит в файл несколько символов и получит требуемое значение суммы.

Особый тип контрольных сумм, называемый циклическим контролем (Cyclic Redundancy Check, CRC), обладает гораздо большей надежностью. Его реализация лишь немногим сложнее, зато обеспечивается более высокая степень контроля. Тем не менее и он может не устоять перед злоумышленником.

Контрольные суммы можно использовать для обнаружения фактов изменения информации, однако они не обеспечивают активной защиты от внесения изменений. По этой причине следует применять другие механизмы, такие, как управление доступом и криптография.

криптографические контрольные суммы.

Криптографические контрольные суммы (называемые также имитовставками) вычисляются следующим образом. Файл делится на порции, для каждой из них подсчитывается контрольная сумма (CRC), а затем эти частичные суммы складываются. При подходящей реализации данный метод гарантирует практически стопроцентное обнаружение изменений файлов, несмотря на возможное противодействие злоумышленника. Недостаток метода состоит в том, что он требует значительных вычислительных ресурсов, так что его разумно применять лишь тогда, когда требуется максимально возможный контроль целостности.

Другой сходный механизм, называемый односторонней хеш-функцией (или кодом обнаружения манипуляций – Manipulation Detection Code, MDC), может быть использован также для уникальной идентификации файлов. Идея состоит в том, что никакие два разных исходных файла не дадут одинаковых результатов, так что при модификации файла хеш-функция изменит значение. Односторонние хеш-функции допускают эффективную реализацию на самых разных системах, что превращает стопроцентное обнаружение изменений файлов в реальность. (Одним из примеров эффективной односторонней хеш-функции является Snefru, доступная по USENET и Интернету.)

Заметим, что помимо обсуждаемых имеются и другие механизмы обеспечения целостности, такие, как совместный контроль со стороны двух лиц и процедуры проверки целостности. К сожалению, их рассмотрение выходит за рамки данного документа.

Ограничение сетевого доступа. Протоколы, доминирующие в Интернете, – IP (RFC 791), TCP (RFC 793) и UDP (RFC 768) – предусматривают наличие управляющей информации, которой можно воспользоваться для ограничения доступа к определенным хостам или сетям организации. Заголовок IP-пакета содержит сетевые адреса как отправителя, так и получателя. Далее, протоколы TCP и UDP поддерживают понятие «порта», идентифицирующего оконечную точку коммуникационного маршрута (обычно это сетевой сервер). В некоторых случаях может быть желательным запретить доступ к конкретным TCP– или UDP-портам, а быть может, даже к определенным хостам или сетям.

К управляющей информации относятся:

шлюзовые маршрутные таблицы;

Один из простейших способов предотвращения нежелательных сетевых соединений состоит в удалении определенных сетей из шлюзовых маршрутных таблиц. В результате хост лишается возможности послать пакеты в эти сети. (В большинстве протоколов предусмотрен двусторонний обмен пакетами даже при однонаправленном информационном потоке, поэтому нарушения маршрута с одной стороны, как правило, бывает достаточно.)

Подобный подход обычно применяется в экранирующих системах, чтобы не открывать

локальные маршруты для внешнего мира. Правда, при этом зачастую запрещается слишком много (например, для предотвращения доступа к одному хосту закрывается доступ ко всем системам сети).

фильтрация пакетов маршрутизатором.

Многие коммерчески доступные шлюзовые системы (которые более правильно называть маршрутизаторами) предоставляют возможность фильтрации пакетов, основываясь не только на адресах отправителя или получателя, но и на их комбинациях. Этот подход может быть использован, чтобы запретить доступ к определенному хосту, сети или подсети из другого хоста, сети или подсети. Шлюзовые системы некоторых поставщиков (например, Cisco Systems) поддерживают еще более сложные схемы, допуская более детальный контроль над адресами отправителя и получателя. Посредством масок адресов можно запретить доступ ко всем хостам определенной сети, кроме одного. Маршрутизаторы Cisco Systems реализуют также фильтрацию пакетов на основе типа IP-протокола и номеров TCP– или UDP-портов.

Для обхода механизма фильтрации злоумышленник может воспользоваться «маршрутизацией отправителем». Возможно отфильтровать и такие пакеты, но тогда под угрозой окажутся некоторые законные действия (например, диагностические).

Системы аутентификации. Аутентификация – это процесс проверки подлинности «личности», проводимый в интересах инстанции, распределяющей полномочия. Системы аутентификации могут включать в себя аппаратные, программные и процедурные механизмы, которые дают возможность пользователю получить доступ к вычислительным ресурсам. В простейшем случае частью механизма аутентификации является системный администратор, заводящий новые пользовательские счета. На другом конце спектра находятся высокотехнологичные системы распознавания отпечатков пальцев и сканирования роговицы потенциальных пользователей. Без доказательного установления личности пользователя до начала сеанса работы компьютеры вашей организации будут уязвимы, по существу, для любых атак. Обычно пользователь доказывает свою подлинность системе, вводя пароль в ответ на приглашение. Запросно-ответные системы улучшают парольную схему, предлагая ввести элемент данных, известный и компьютерной системе, и пользователю (например, девичью фамилию матери и т. п.):

Kerberos;

Система Kerberos, названная по имени мифологического пса, охранявшего врата ада, является набором программ, используемых в больших сетях для проверки подлинности пользователей. Разработанная в Массачусетском технологическом институте, она опирается на криптографию и распределенные базы данных и дает возможность пользователям распределенных конфигураций начинать сеанс и работать с любого компьютера. Очевидно, это полезно в учебном или аналогичном ему окружении, когда большое число потенциальных пользователей могут инициировать подключение с любой из множества рабочих станций. Некоторые поставщики встраивают Kerberos в свои системы.

Заметим, что, несмотря на улучшения в механизме аутентификации, в протоколе Kerberos остались уязвимые места.

интеллектуальные карты.

В некоторых системах для облегчения аутентификации применяются интеллектуальные карты (небольшие устройства размером с калькулятор). Здесь подлинность пользователя подтверждается обладанием определенным объектом. Одна из разновидностей такой системы включает в себя новую парольную процедуру, когда пользователь вводит значение, полученное от интеллектуальной карты. Обычно хост передает пользователю элемент данных, который следует набрать на клавиатуре карты. Интеллектуальная карта высвечивает на дисплее ответ, который, в свою очередь, нужно ввести в компьютер. Только после этого начинается сеанс работы. Другая разновидность использует интеллектуальные карты, высвечивающие меняющиеся со временем числа. Пользователь вводит текущее число в компьютер, где аутентификационное программное

обеспечение, синхронизированное с картой, проверяет корректность введенного значения.

Интеллектуальные карты обеспечивают более надежную аутентификацию по сравнению с традиционными паролями. С другой стороны, использование карт сопряжено с некоторыми неудобствами, да и начальные затраты довольно велики.

Типы процедур безопасности ***Проверка системной безопасности***

Частью нормальной деловой жизни многих бизнесменов являются ежегодные финансовые проверки. Проверки безопасности – важная часть функционирования любой компьютерной среды. Элементом таких проверок должна стать ревизия политики безопасности и защитных механизмов, используемых для проведения политики в жизнь.

Проводите плановые учения. Конечно, не каждый день или каждую неделю, но периодически нужно проводить плановые учения, чтобы проверить, адекватны ли выбранные процедуры безопасности предполагаемым угрозам. Если главной угрозой вы считаете стихийное бедствие, на учении могут проверяться механизмы резервного копирования и восстановления. С другой стороны, если вы опасаетесь прежде всего вторжения в систему сторонних злоумышленников, можно устроить учебную атаку, проверив тем самым эффективность политики безопасности.

Учения – хороший способ выяснения результативности политики и процедур безопасности. С другой стороны, они отнимают много времени и нарушают нормальную работу. Важно сопоставлять выгоды от учений и неизбежно связанные с ними потери времени.

Проверяйте процедуры. Если решено не устраивать плановых учений, проверяющих сразу всю систему безопасности, следует как можно чаще проверять отдельные процедуры. Проверьте процедуру резервного копирования, чтобы убедиться, что вы можете восстановить данные с лент. Проверьте регистрационные журналы, чтобы удостовериться в их полноте и т. п.

При проведении проверок необходимо с максимальной тщательностью подбирать тесты политики безопасности. Важно четко определить, что тестируется, как проводится тестирование и какие результаты ожидаются. Все это нужно документировать и включить в основной текст политики безопасности или издать в качестве дополнения.

Важно протестировать все аспекты политики безопасности, процедурные и программно-технические, с упором на автоматизированные механизмы проведения политики в жизнь. Должна быть уверенность в полноте тестирования каждого средства защиты. Например, если проверяется процесс входа пользователя в систему, следует явно оговорить, что будут пробоваться правильные и неправильные входные имена и пароли.

Помните, что существует предел разумности тестирования. Цель проверок состоит в получении уверенности, что политики безопасности корректно проводятся в жизнь, а не в «доказательстве абсолютной правильности» системы или политики. Важно убедиться, что разумные и надежные средства защиты, предписанные политикой, обеспечивают должный уровень безопасности.

Процедуры управления счетами Процедуры управления счетами важны для предотвращения несанкционированного доступа к вашей системе. В этой связи в политике безопасности необходимо дать ответы на следующие вопросы:

• Кто может иметь счет на данной системе?

• Как долго можно иметь счет без обновления запроса?

• Как из системы удаляются старые счета?

Помимо определения круга возможных пользователей, необходимо решить, для чего каждый из них имеет право использовать систему (например, допускается ли применение в личных целях). Если имеется подключение к внешней сети, то ее или ваше руководство могут установить правила пользования этой сетью. Следовательно, для любой политики безопасности важно определить подходящие процедуры управления счетами как для администраторов, так и для пользователей. Обычно системный администратор отвечает за заведение и ликвидацию счетов и осуществляет общий контроль за использованием системы.

До некоторой степени, управление счетом – обязанность каждого пользователя, в том смысле, что он должен следить за всеми системными сообщениями и событиями, которые могут свидетельствовать о нарушении политики безопасности. Например, выдаваемое при входе в систему сообщение с датой и временем предыдущего входа необходимо переправить «куда следует», если оно не согласуется с прошлыми действиями пользователя.

Процедуры управления паролями Политика управления паролями важна для поддержания их секретности. Соответствующие процедуры могут варьироваться от эпизодических просьб или приказаний пользователю сменить пароль до активных попыток этот пароль подобрать с последующим информированием владельца о легкости данного мероприятия. Другая часть политики управления описывает, кто может распространять пароли – имеет ли право пользователь сообщать свой пароль другим?

Независимо от политики процедуры управления должны быть тщательно продуманы и подробно регламентированы, чтобы избежать раскрытия паролей. Критичным является выбор начальных паролей. Бывают случаи, когда пользователи вообще не работают в системе и, следовательно, не активируют счета. Значит, начальный пароль не должен быть очевидным. Никогда не присваивайте счетам пароли по умолчанию, каждый раз придумывайте новый пароль. Если существует печатный список паролей, его необходимо хранить подальше от посторонних глаз в надежном месте. Впрочем, лучше вообще обойтись без подобного списка.

Выбор пароля. Пожалуй, пароли – наиболее уязвимая часть любой компьютерной системы. Как бы ни была защищена система от атак по сети или по коммутируемым линиям, от «Троянских коней» и аналогичных опасностей, она может быть полностью скомпрометирована злоумышленником, если тот получит к ней доступ из-за плохо выбранного пароля. Важно сформировать хороший свод правил выбора паролей и довести его до каждого пользователя. По возможности, следует модифицировать программное обеспечение, устанавливающее пароли, чтобы оно в максимальной степени поддерживало эти правила.

Приведем один набор простых рекомендаций по выбору паролей:

• не используйте в качестве пароля производные от входного имени (само имя, обращенное, записанное прописными буквами, удвоенное имя и т. п.);

• не используйте в качестве пароля свое имя, отчество или фамилию;

• не используйте имя супруги (супруга) или детей;

• не используйте другую ассоциированную с вами информацию, которую легко узнать (номера документов и телефонов, марку автомобиля, домашний адрес и т. п.);

• не используйте чисто цифровой пароль или пароль из повторяющихся букв;

• не используйте слов, содержащихся в словаре английского или иного языка, в других списках слов;

• не используйте пароль менее чем из шести символов;

• используйте пароли со сменой регистра букв;

• используйте пароли с небуквенными символами (цифрами или знаками пунктуации);

• используйте запоминающиеся пароли, чтобы не пришлось записывать их на бумаге.

• используйте пароли, которые вы можете ввести быстро, не глядя на клавиатуру.

Методы выбора пароля в соответствии с приведенными рекомендациями могут состоять в следующем: • возьмите одну-две строки из песни или стихотворения и составьте пароль из первых букв последовательных слов;

• составьте последовательность из чередующихся согласных и гласных (одной или двух подряд) букв длиной семь-восемь символов. Получится бессмысленное, но легко произносимое и, следовательно, запоминающееся слово;

• выберите два коротких слова и соедините их, вставив в середину знак пунктуации.

Пользователей нужно убедить в необходимости регулярно менять пароли, обычно раз в три-шесть месяцев. Это позволяет поддерживать уверенность в том, что даже если злоумышленник подберет один из паролей, он в конце концов потеряет доступ к системе,

равно как рано или поздно потеряет актуальность нелегально полученный список паролей. Многие системы дают администратору возможность заставлять пользователей менять пароли по истечении срока годности; если вам доступно соответствующее программное обеспечение, его нужно задействовать. Некоторые системы программным образом вынуждают пользователей регулярно менять пароли. Компонентом многих из подобных систем является генератор паролей. Он предлагает пользователю на выбор несколько вариантов; самостоятельно придумывать пароли не разрешается. У таких систем есть как достоинства, так и недостатки. С одной стороны, генерация защищает от выбора слабых паролей. С другой – если генератор не настолько хорош, чтобы порождать запоминающиеся пароли, пользователям придется их записывать, чтобы не забыть.

Процедуры смены паролей. То, как организована смена паролей, существенно для их безопасности. В идеале у пользователей должна быть возможность менять пароли в оперативном режиме. (Имейте в виду, что программы смены паролей – излюбленная мишень злоумышленников.)

Бывают, однако, исключительные случаи, когда действовать нужно осторожно. Пользователь может забыть пароль и лишиться тем самым возможности входа в систему. Стандартная процедура состоит в присваивании пользователю нового пароля. При этом важно убедиться, что запрашивает смену и получает новый пароль реальный человек. Одна из стандартных уловок злоумышленников – позвонить или послать сообщение системному администратору и запросить новый пароль. Перед выдачей нового пароля нужно применить какую-либо внешнюю форму проверки подлинности пользователя. В некоторых организациях пользователи должны лично явиться к администратору, имея при себе удостоверение.

Иногда нужно изменить много паролей. Если система скомпрометирована злоумышленником, он мог украсть файл паролей. В подобных обстоятельствах разумно изменить все пароли. В организации должны быть заготовлены процедуры для быстрого и эффективного выполнения такой работы. Конкретный способ действий может зависеть от серьезности проблемы. В случае выявленной атаки, наносящей ущерб, вы можете принудительно блокировать все счета и присвоить пользователям новые пароли, прежде чем они смогут вновь войти в систему. В некоторых организациях пользователям рассылаются сообщения с просьбой изменить пароль, возможно, с указанием срока исполнения. Если пароль в оговоренное время не меняют, счет блокируется.

Пользователи должны знать стандартные процедуры управления паролями, применяемые при нарушениях режима безопасности. Один из хорошо известных мошеннических приемов, о котором сообщила группа реагирования на нарушения информационной безопасности (Computer Emergency Response Team, CERT), состоит в рассылке пользователям сообщений, вроде бы от имени местного системного администратора, с предложением изменить пароль на новое, сообщаемое тут же, значение. Конечно, сообщения рассылали не администраторы, а злоумышленники, пытающиеся таким образом получить доступ к счетам. Пользователей следует предупредить о необходимости докладывать администраторам обо всех подозрительных запросах, аналогичных упомянутому.

Процедуры конфигурационного управления Обычно конфигурационное управление применяют в процессе разработки программного обеспечения. Однако оно, несомненно, в равной степени применимо и в операционном смысле. Действительно, поскольку многие системные программы предназначены для проведения в жизнь политики безопасности, необходимо иметь уверенность в их корректности. Иными словами, нельзя допускать произвольных изменений системных программ (таких, как ОС). Как минимум, процедуры должны определять, кто имеет право изменять системы, при каких обстоятельствах и как эти изменения следует документировать.

В некоторых организациях конфигурационное управление разумно применять и к физическому конфигурированию аппаратуры. Вопросы поддержания правильных и

авторизованных аппаратных конфигураций должны получить соответствующее освещение в вашей политике безопасности.

Нестандартные конфигурации. Иногда полезно внести в конфигурацию небольшие нестандартности, чтобы противостоять «стандартным» атакам, применяемым некоторыми злоумышленниками. В число нестандартных частей может входить оригинальный алгоритм шифрования паролей, необычное расположение конфигурационных файлов, а также переписанные или функционально ограниченные системные команды.

К сожалению, нестандартные конфигурации не свободны от недостатков. Внесение изменений усложняет сопровождение систем, поскольку необходимо написать дополнительную документацию, особым образом устанавливать новые версии программного обеспечения. Обычно в штате организации приходится держать специалиста «по нестандартностям».

Вследствие отмеченных недостатков нестандартные конфигурации, как правило, используются лишь на экранирующих системах. Межсетевые экраны модифицируются нестандартным образом, поскольку они являются предполагаемым объектом атак, а конфигурация внутренних систем, расположенных за «противопожарной перегородкой», остается стандартной.

Реакция на нарушение безопасности ***Обзор***

В данном разделе излагаются соображения, применимые к ситуациям, когда происходит нарушение информационной безопасности отдельного компьютера, сети, организации или корпоративной среды. Основное положение состоит в том, что враждебные действия, будь то атака внешних злоумышленников или месть обиженного сотрудника, необходимо предусмотреть заранее. Ничто не может заменить предварительно составленного плана восстановительных работ.

Традиционная информационная безопасность, хотя и имеющая весьма важное значение для общеорганизационных защитных планов, как правило, концентрируется вокруг защиты от атак и, до некоторой степени, вокруг их обнаружения. Обычно почти не уделяют внимания мерам, предпринимаемым, когда атака уже идет. В результате поспешных, непродуманных действий могут быть затруднены выявление причины инцидента, сбор улик для расследования, подготовка к восстановлению системы и защита ценной информации.

Имейте план, которому будете следовать во время инцидента. Частью реакции на нарушения безопасности является предварительная подготовка ответных мер. Под этим понимается поддержание должного уровня защиты, так что ущерб даже от серьезного инцидента будет ограниченным. Подготовка включает в себя составление руководства по мерам реагирования на инциденты и плана восстановительных работ. Наличие отпечатанных планов способно устранить многие двусмысленности, возникающие во время инцидента, и ведет к серии более точных и основательных ответов. Далее, частью защиты является выработка процедуры извещения об инциденте, чтобы каждый знал, кто кому звонит и по каким номерам. Целесообразно устраивать «учебные тревоги», когда сотрудники службы безопасности, системные администраторы и руководители отрабатывают реакцию на инциденты.

Отработка эффективных ответов на инциденты важна по многим причинам. Главнейшая из них – чисто человеческая: предотвращение угрозы жизням людей. Некоторые компьютерные системы критически важны для сохранения жизней (например, системы жизнеобеспечения в больницах или комплексы, участвующие в управлении движением воздушных судов).

Еще одно существенное достоинство предварительной подготовки, о котором часто забывают, носит экономический характер. Содержание технического и управленческого персонала, ответственного за реакцию на инциденты, требует значительных ресурсов, которые с выгодой можно было бы употребить на другие нужды. Если персонал обучен эффективным приемам реагирования, обслуживание инцидентов будет отнимать меньше времени.

Третье достоинство – обеспечение защиты секретной, критически важной или частной информации. Весьма опасно то, что компьютерный инцидент может разрушить невосстановимую информацию. Эффективная реакция на инциденты минимизирует эту опасность. Когда речь идет о секретной информации, следует учесть и включить в план соответствующие правительственные постановления.

Четвертое достоинство касается связей с прессой. Сведения о компьютерном инциденте могут повредить репутации организации у нынешних или потенциальных клиентов. Эффективная реакция на инцидент уменьшает вероятность нежелательной огласки.

Наконец, упомянем правовой аспект. Можно представить себе ситуацию, когда организация подвергается судебному преследованию, поскольку один из принадлежащих ей узлов был использован для атаки на сеть. С аналогичными проблемами могут столкнуться люди, реализующие заплаты или надстройки, если те оказались неэффективными и не смогли предотвратить ущерб или сами стали причиной ущерба. Знание уязвимых мест операционных систем и типичных приемов атаки, а также принятие превентивных мер поможет избежать конфликтов с законом.

Порядок изложения в данном разделе можно использовать в качестве плана. Данный раздел организован таким образом, что его содержание может послужить отправной точкой при написании политики безопасности, касающейся реакции на инциденты. В политике должны быть освещены следующие темы:

• обзор (цели, преследуемые политикой безопасности в плане реакции на инциденты;.

• оценка (насколько серьезен инцидент);

• извещение (кого следует известить об инциденте);

• ответные меры (что следует предпринять в ответ на инцидент);

• правовой аспект (каковы правовые последствия инцидента);

• регистрационная документация (что следует фиксировать до, во время и после инцидента).

Каждая из перечисленных тем важна при общем планировании реакции на инциденты. Далее будут сформулированы рекомендации по формированию политики безопасности, касающейся реакции на инциденты. *Возможные цели и побудительные мотивы эффективной реакции на инциденты.* Как и во всякой деятельности по планированию, в первую очередь необходимо уяснить преследуемые цели. Эти цели следует упорядочить в порядке убывания важности. Итоговый список, конечно, будет разным для разных организаций. Ниже приведен один из возможных вариантов:

• гарантировать целостность критически важных (для сохранения человеческих жизней) систем;

• сохранить и восстановить данные;

• сохранить и восстановить сервисы;

• выяснить, почему инцидент стал возможен;

• предотвратить развитие вторжения и будущие инциденты;

• избежать нежелательной огласки;

• найти виновников;

• наказать нарушителей.

Важно заранее определить приоритеты действий, совершаемых во время инцидента. Бывают столь сложные случаи, когда невозможно одновременно принять все необходимые ответные меры; без учета приоритетов тут не обойтись. Хотя, как всегда, шкала приоритетов зависит от организации, следующий список может послужить отправной точкой при выработке иерархии ответных мер: • первый приоритет – защитить жизнь и здоровье людей; при всех обстоятельствах защита человеческих жизней должна стоять на первом месте;

• второй приоритет – защитить секретные и/или критически важные данные (в соответствии с правительственными или организационными нормами);

• третий приоритет – защитить прочие данные, включая частную, научную и

управленческую информацию, поскольку потеря данных обходится дорого с точки зрения ресурсов, затраченных на их накопление;

• четвертый приоритет – предотвратить повреждение систем (потерю и изменение системных файлов, повреждение дисководов и т. п.), чтобы избежать дорогостоящих простоев и восстановлений;

• пятый приоритет – минимизировать урон, нанесенный вычислительным ресурсам; во многих случаях лучше выключить систему или отсоединить ее от сети, чем подвергать риску информацию, программное обеспечение или аппаратуру.

Важным следствием определения приоритетов является то, что после человеческих жизней и интересов государственной безопасности наиболее ценным активом обычно являются данные, а не программное или аппаратное обеспечение. Хотя нежелательны любые потери, системы можно заменить; в то же время потерю или компрометацию данных (особенно секретных), как правило, нельзя допускать ни при каких обстоятельствах.

Как уже отмечалось, частью реакции на инциденты является предварительная подготовка ответных мер. Для каждой машины и системы должна существовать и выполняться процедура резервного копирования. Наличие копий в значительной степени устраняет потери даже после серьезных инцидентов, поскольку исключаются массовые потери данных. Далее, ваши системы должны иметь безопасную конфигурацию. Под этим понимается устранение слабостей, проведение эффективной политики управления паролями, а также использование других процедур, разъясняемых ниже.

Руководство по местной политике безопасности и юридическим положениям. Любой план реагирования на инциденты должен составляться на основе политики безопасности и юридических положений. Правительственные и частные организации, имеющие дело с секретной информацией, должны следовать дополнительным правилам.

Политика, разработанная вашей организацией применительно к реакции на нарушения режима безопасности, позволит оформить ответные меры. Например, нет особого смысла создавать механизмы для отслеживания нарушителей, если ваша организация не собирается после поимки предпринимать против них какие-либо действия. На ваши планы может влиять политика других организаций. Например, телефонные компании обычно сообщают информацию для прослеживания звонков только правоохранительным органам.

Оценка *А что на самом деле?* На этой фазе точно выясняется характер проблем. Конечно, многие, если не большинство, проявлений, часто приписываемых вирусным инфекциям или вторжениям злоумышленников, являются следствием обычных отклонений, таких, как аппаратные сбои. Чтобы понимать, действительно ли имеет место нарушение режима безопасности, полезно приобрести и использовать специальное программное обеспечение. Например, широко доступные программные пакеты могут оказать существенную помощь в выявлении вируса, проникшего в Macintosh. Весьма полезна и регистрационная информация, особенно применительно к сетевым атакам. При подозрениях на вторжение чрезвычайно важно сделать моментальный снимок системы. Многие инциденты порождают целую цепь событий, и снимок системы, сделанный на начальной стадии, может оказаться полезнее других мер для установления сути проблемы и источника опасности. Наконец, важно завести регистрационную книгу. Запись системных событий, телефонных разговоров, временных меток и т. д. способна ускорить и систематизировать процесс идентификации проблемы, послужить основой последующих действий по нейтрализации инцидента.

Имеется ряд отчетливых признаков, или «симптомов», инцидента, заслуживающих особого внимания:

• крахи системы;

• появление новых пользовательских счетов (например, необъяснимым образом создался счет RUMPLESTILTSKIN) или необычайная активность со стороны пользователя (счета), практически не подававшего признаков жизни в течение нескольких месяцев;

• новые файлы (обычно со странными именами, такими, как data.xx или к);

• рассогласования в учетной информации (например, на UNIX-системах это может проявляться как сокращение файла /usr/admin/lastlog, что вызывает сильные подозрения в присутствии нарушителя);

• изменения в размерах и датах файлов (например, пользователя MS-DOS должно насторожить внезапное удлинение. EXE-файла более чем на 1 800 байт);

• попытки записи в системные файлы (например, системный администратор замечает, что привилегированный пользователь VMS пытается изменить RIGHTSLIST.DAT);

• модификация или удаление данных (например, начали исчезать файлы);

• отказ в обслуживании (например, системные администраторы и все остальные пользователи оказались выброшенными из UNIX-системы, которая перешла в однопользовательский режим);

• необъяснимо низкая производительность системы (например, необычно плохое время отклика системы);

• аномалии (например, на экране терминала вдруг появляется слово GOTCHA или раздаются частые и необъяснимые звуковые сигналы);

• подозрительные пробы (например, многочисленные неудачные попытки входа с другого узла сети);

• подозрительное «рысканье» (например, некто стал пользователем root UNIX-системы и просматривает файл за файлом).

Ни один из этих признаков не может служить бесспорным доказательством нарушения режима безопасности, точно так же, как реальный инцидент обычно не сопровождается всем набором симптомов. Если, однако, вы заметили какой-либо из перечисленных признаков, следует подозревать нарушение и действовать соответственно. Не существует формулы, позволяющей с абсолютной достоверностью обнаруживать инциденты. Пожалуй, единственным исключением являются антивирусные пакеты. Если они говорят, что вирус есть, им можно верить. В такой ситуации лучше всего воспользоваться помощью других технических специалистов и сотрудников службы информационной безопасности и сообща решить, действительно ли инцидент имеет место.

Масштабы инцидента. Идентификации инцидента сопутствует выяснение его масштабов и возможных последствий. Для эффективного противодействия важно правильно определить границы инцидента, Кроме того, оценка возможных последствий позволит установить приоритеты при выделении ресурсов для принятия ответных мер. Без выяснения масштабов и возможных последствий события трудно определить, как именно нужно действовать.

Для определения масштабов и возможных последствий следует воспользоваться набором критериев, подходящих для конкретной организации и имеющихся связей с внешним миром. Вот некоторые из них:

• затрагивает ли инцидент несколько организаций;

• затрагивает ли инцидент многие компьютеры вашей организации;

• находится ли под угрозой критически важная информация;

• какова стартовая точка инцидента (сеть, телефонная линия, локальный терминал и т. д.);

• знает ли об инциденте пресса;

• каков потенциальный ущерб от инцидента;

• каково предполагаемое время ликвидации инцидента;

• какие ресурсы требуются для ликвидации инцидента.

Возможные типы извещений Когда вы убедились, что нарушение режима безопасности действительно имеет место, следует известить соответствующий персонал. Чтобы удержать события под контролем и с технической, и с эмоциональной точек зрения очень важно, кто и как будет извещен.

Внятность. Прежде всего, любое извещение, направленное своему или стороннему

сотруднику, должно быть внятным. Это значит, что любая фраза об инциденте (идет ли речь об электронном сообщении, телефонном звонке или факсе) обязана быть ясной, точной и полной. Всякий «туман» в извещении, направленном человеку, от которого вы ждете помощи, отвлечет его внимание и может привести к недоразумениям. Если предлагается разделение труда, полезно снабдить каждого участника информацией о том, что делают другие. Это не только уменьшит дублирование, но и позволит человеку, занятому определенной работой, знать, где получить дополнительные сведения, чтобы справиться со своей частью проблемы.

Правдивость. Другой важный аспект извещений об инциденте – правдивость. Попытки скрыть отдельные моменты, сообщая ложную или неполную информацию, способны не только помешать принятию эффективных ответных мер; они могут привести даже к ухудшению ситуации. Это тем более верно в случае, когда об инциденте узнали журналисты. Если имеет место достаточно серьезный инцидент, привлекший внимание прессы, то, скорее всего, любая сообщенная вами ложная информация не получит подтверждения из других источников. Это бросит тень на организацию и испортит отношения с журналистами, а значит, и с общественностью.

Выбор языка. Язык, которым написано извещение, существенным образом влияет на восприятие информации об инциденте. Если вы используете эмоциональные обороты, вы усиливаете ощущение опасности и ожидание неблагоприятного завершения инцидента. Важно сохранять спокойствие и в письменных, и в устных извещениях.

Другим моментом, связанным с выбором языка, является извещение нетехнического и внешнего персонала. Важно точно описать инцидент, без лишней тревоги и непонятных фраз. Хотя неспециалистам объяснить суть дела труднее, зачастую это более важно. Нетехническое описание может понадобиться для высшего руководства, прессы или сотрудников правоохранительных органов. Важность подобных извещений нельзя недооценивать. От этого зависит, получит ли инцидент адекватное решение или приведет к еще более серьезным последствиям.

Извещение конкретных лиц. Кого извещать во время и после инцидента? На этот предмет можно рассмотреть несколько категорий лиц:

• персонал в точках контакта (техническая и административная группы, группа реагирования, органы дознания, другие правоохранительные органы, производители, поставщики услуг). Необходимо определить, кто отвечает за извещения в адрес каждой из перечисленных контактных групп;

• более широкое сообщество (пользователи);

• другие организации, вовлеченные в инцидент.

Следует заранее установить, кого извещать из центральной точки контакта организации. Список лиц в каждой из выбранных категорий поможет сэкономить массу времени в случае нарушения режима безопасности. В суете инцидента, когда срочные дела накладываются друг на друга, очень трудно выяснять, где и кого можно отыскать. Кроме лиц, отвечающих за определенные аспекты реакции на инциденты, в извещении нуждаются другие организации, которых нарушение затронуло или может затронуть. Пользователям зачастую также полезно знать об инциденте. Им разумно направить отчет о нарушении (если этот отчет решено сделать открытым).

Связи с общественностью – пресс-релизы. Один из самых важных вопросов – когда, кто и насколько подробно должен оповестить общественность через прессу. При этом следует учитывать несколько моментов. Во-первых, если в организации существует пресс-центр, важно задействовать именно его. Сотрудники пресс-центра имеют опыт общения с журналистами, и это поможет сохранить лицо организации во время и после инцидента. С сотрудниками пресс-центра можно говорить откровенно, они сами буферизуют предназначенную для прессы информацию, а вы в это время сможете заниматься инцидентом.

Если пресс-центра нет, следует тщательно взвешивать сообщаемые прессе сведения.

Когда информация конфиденциальна, разумно ограничиться минимумом данных обзорного характера. Весьма возможно, что все сообщенное прессе быстро дойдет до виновника инцидента. С другой стороны, как отмечалось выше, введение прессы в заблуждение может оказаться бумерангом, наносящим больший вред, чем разглашение конфиденциальной информации.

Хотя заранее сложно определить, насколько детальные сведения стоит сообщать прессе, разумно учесть следующие соображения:

• избегайте технических деталей. Детальная информация об инциденте может привести к повторению подобных нарушений или даже помешать организации расследовать текущий случай;

• избегайте предположений. Предположения о виновнике инцидента и его побудительных мотивах могут оказаться ошибочными, что способно усугубить ситуацию;

• работайте с профессионалами из правоохранительных органов, чтобы обеспечить защиту улик. Если в деле участвуют следственные органы, убедитесь, что собранные улики не стали достоянием прессы;

• избегайте интервью, если вы не готовы к ним. Помните, что журналисты попытаются вытянуть из вас максимум информации, в том числе конфиденциальной;

• не позволяйте прессе отвлекать ваше внимание от реакции на инцидент. Постоянно помните, что успешная борьба с нарушением – дело первостепенной важности.

Чьей помощью воспользоваться? В мире существует довольно много групп реагирования на нарушения информационной безопасности (например, CERT, CIAC). Аналогичные группы имеются во многих важных правительственных агентствах и больших корпорациях. Если у вашей организации есть контакты с подобной группой, с ней необходимо связаться в первую очередь и как можно раньше. Такие группы отвечают за координацию реакции на инциденты нескольких организаций или более крупных сообществ. Даже если кажется, что нарушение затрагивает только одну организацию, информация, доступная через группу реагирования, способна помочь успешной борьбе с нарушением. При выработке политики, касающейся реакции на инциденты, может быть принято решение о создании собственной группы реагирования по типу существующих, отвечающей перед организацией за борьбу с нарушениями информационной безопасности. Если группа создана, ей необходимо наладить взаимодействие с аналогичными структурами – во время инцидента налаживать доверительные отношения гораздо труднее.

Ответные меры Важная тема, которой мы пока не касались, – это реальные меры, предпринимаемые для борьбы с нарушением. Их можно подразделить на следующие основные категории: сдерживание, ликвидация, восстановление, «разбор полетов».

Сдерживание. Цель сдерживания – ограничить атакуемую область. Например, важно как можно быстрее приостановить распространение «червя» в сети. Обязательной частью сдерживания является принятие решений (останавливать ли систему, отсоединять ли ее от сети, отслеживать ли ее работу и события в сети, устанавливать ли ловушки, отключать ли некоторые сервисы, такие, как удаленная пересылка файлов в ОС UNIX и т. д.). Иногда подобные решения очевидны. Если риску подвергается секретная, конфиденциальная или частная информация, систему нужно остановить. В некоторых случаях стоит пойти на риск, связанный с нанесением системе определенного ущерба, если поддержание ее работы способно помочь в идентификации злоумышленника.

Сдерживание должно выполняться с использованием предварительно выработанных процедур. Ваша организация должна определить приемлемые границы рисков при борьбе с нарушениями и предложить соответствующие стратегические и тактические решения. Наконец, на стадии сдерживания должны извещаться заранее выбранные инстанции.

Ликвидация. После обнаружения инцидента необходимо в первую очередь позаботиться о его сдерживании. Когда эта задача решена, можно приступать к ликвидации. В этом вам может помочь программное обеспечение. Например, существуют программы, ликвидирующие вирусы в небольших системах. Если нарушитель создал какие-либо файлы,

самое время их удалить. В случае вирусной инфекции важно вычистить все диски, содержащие зараженные файлы. Убедитесь в чистоте резервных копий. Многие системы, подвергавшиеся вирусным атакам, время от времени заражаются повторно только потому, что не производится систематическая очистка резервных носителей.

Восстановление. Когда инцидент ликвидирован, наступает время восстановления, то есть приведения системы в нормальное состояние. В случае сетевых атак важно установить заплаты, ликвидирующие использованные системные слабости.

«Разбор полетов». Одну из самых важных стадий реакции на инциденты, о которой тем не менее почти всегда забывают, можно назвать «разбором полетов». Данная стадия важна потому, что она позволяет всем причастным лицам извлечь уроки из инцидента, чтобы в будущем в аналогичных ситуациях действовать эффективнее. В процессе «разбора полетов» служба информационной безопасности объясняется перед руководством и систематизирует информацию, необходимую для юридических акций.

Самый важный элемент данной стадии – анализ случившегося. Что именно и когда произошло? Насколько хорошо сработал персонал? Какая срочная информация понадобилась в первую очередь и как ее быстрее всего можно было получить? Что в следующий раз нужно делать по-другому? Постинцидентный отчет ценен как руководство к действию в аналогичных случаях. Составление хронологии событий (с указанием точного времени) важно и с юридической точки зрения. Необходимо также в кратчайшие сроки получить денежную оценку ущерба, нанесенного инцидентом: утраченных программ и файлов, повреждений аппаратуры, потерь времени на восстановление измененных файлов, реконфигурацию атакованных систем и т. п. Эта оценка может послужить основанием для последующего официального расследования.

Единая точка контакта. Когда инцидент в разгаре, важно решить, кто координирует действия множества специалистов. Принципиальной ошибкой была бы организация нескольких точек контакта, которые не в состоянии наладить согласованное управление событиями, а лишь увеличивают общую неразбериху, вызывая своими указаниями напрасную или неэффективную затрату усилий.

Человек, находящийся в единой точке контакта, может быть, а может и не быть руководителем работ по борьбе с нарушением. В принципе речь идет о двух разных ролях, для которых нужно подобрать «исполнителей». Руководитель работ принимает решения (например, он интерпретирует политику безопасности применительно к происходящим событиям). На него возлагается ответственность за реакцию на инцидент. Напротив, непосредственная функция точки контакта состоит в координации усилий всех сторон, вовлеченных в ликвидацию инцидента.

В точке контакта должен находиться специалист, техническая подготовка которого позволяет ему успешно координировать действия системных администраторов и пользователей. Нередко управленческая структура организации такова, что администратор множества ресурсов не имеет достаточной технической подготовки и не знает деталей функционирования компьютеров, но тем не менее отвечает за их использование.

Другая важная функция точки контакта – поддержание связей с правоохранительными органами и другими внешними организациями, когда возникает нужда в согласованных действиях нескольких инстанций.

Наконец, если предусматриваются правовые действия, такие, как расследование, сотрудник, обслуживающий точку контакта, может представлять организацию в суде. Если свидетелей несколько, их показания трудно координировать, а это ослабляет позиции обвинения и затрудняет наказание нарушителя. Сотрудник точки контакта может представить суду собранные улики, минимизируя тем самым число прочих свидетелей. Как показывает опыт, чем больше свидетелей рассказывает об одном и том же, тем меньше вероятность, что суд им поверит.

Регистрационная документация Целесообразно документировать все детали, связанные с инцидентом. В результате вы получите информацию, незаменимую для

восстановления хода событий. Детальное документирование в конечном итоге ведет к экономии времени. Если, например, не зафиксировать телефонный звонок, вы, скорее всего, забудете почти все, что вам сообщили. В результате придется звонить еще раз и повторно получать информацию. При этом будет потрачено и ваше, и чужое время, что едва ли можно считать приемлемым. Фиксация деталей поможет и при проведении расследования. Далее, документирование инцидента позволяет оценить размер нанесенного ущерба (что необходимо и вашему руководству, и правоохранительным органам) и организовать «разбор полетов», из которого можно извлечь полезные уроки.

Как правило, на ранних стадиях инцидента невозможно определить, понадобится ли расследование, поэтому вы должны вести документацию так, как будто собираете улики для судебного разбирательства. Необходимо зафиксировать по крайней мере следующее:

• все системные события (приобщите к документации системный регистрационный журнал);

• все ваши действия (с указанием времени);

• все телефонные переговоры (имя собеседника, дата, время и содержание разговора).

Самый простой способ сохранить документацию – записывать все в регистрационную книгу. Это избавит вас от поиска среди разрозненных листов бумаги и предоставит в случае необходимости централизованный, упорядоченный по времени источник информации. Большая часть записанных сведений может понадобиться в случае судебного рассмотрения. Таким образом, если вы начали подозревать, что инцидент приведет к расследованию, или когда расследование уже началось, необходимо регулярно (например, ежедневно) относить в архив подписанные вами копии страниц регистрационной книги вместе с другими необходимыми носителями информации, чтобы сохранить их в надежном месте. Разумно потребовать квитанцию о сдаче документации на хранение, с подписью и датой. Если всего этого не сделать, суд может не принять Ваших показаний. *Выработка мер, предпринимаемых после нарушения* ***Обзор***

После ликвидации нарушения режима информационной безопасности необходимо предпринять ряд действий, а именно:

• произвести переучет системных активов, то есть тщательно проверить, как инцидент повлиял на состояние систем;

• уроки, извлеченные из инцидента, должны найти отражение в пересмотренной программе обеспечения безопасности, чтобы не допустить повторения аналогичного нарушения;

• произвести новый анализ риска с учетом информации, полученной вследствие инцидента;

• должно быть начато следствие против виновников инцидента, если это признано необходимым.

Перечисленные шаги направлены на обеспечение комитета по политике безопасности предприятия обратной связью, чтобы политика оперативно пересматривалась и подправлялась.

Устранение слабостей Устранить все слабости, сделавшие возможным нарушение режима безопасности, весьма непросто. Ключевым моментом здесь является понимание механизма вторжения. В некоторых случаях разумно как можно быстрее отключить доступ ко всей системе или к некоторым из ее функциональных возможностей, а затем поэтапно возвращать ее в нормальное состояние. Учтите, что полное отключение доступа во время инцидента заметят все пользователи, в том числе и предполагаемые виновники; системные администраторы должны помнить об этом. Естественно, ранняя огласка может помешать следствию. Однако продолжение инцидента порой чревато увеличением ущерба, усугублением ситуации или даже привлечением к административной или уголовной ответственности.

Если установлено, что вторжение стало возможным вследствие дефектов аппаратного или программного обеспечения, следует как можно быстрее уведомить производителя (или

поставщика), а также группу реагирования CERT. Настоятельно рекомендуется включить в текст политики безопасности соответствующие телефонные (факсовые) номера, а также адреса электронной почты. Чтобы можно было оперативно уяснить суть проблемы, дефект нужно описать максимально детально (включая информацию о его использовании нарушителем).

После вторжения к системе в целом и к каждому компоненту следует относиться с подозрением. В первую очередь это касается системных программ. Ключевым элементом восстановления скомпрометированной системы является предварительная подготовка. Сюда входит вычисление контрольных сумм для всех лент, полученных от поставщика (желательно, чтобы алгоритм вычисления контрольных сумм был устойчив к попыткам взлома). Взяв полученные от поставщика ленты, нужно начать анализ всех системных файлов, доводя до сведения всех вовлеченных в ликвидацию инцидента лиц информацию обо всех найденных отклонениях. Порой бывает трудно решить, с какой резервной копии восстанавливаться; помните, что до момента обнаружения инцидент мог продолжаться месяцы или даже годы и что под подозрением может быть работник предприятия или иное лицо, располагавшее детальным знанием системы или доступом к ней. Во всех случаях предварительная подготовка позволит определить, что можно восстановить. В худшем случае самым благоразумным решением будет переустановка системы с носителей, полученных от поставщика.

Извлекайте уроки из инцидента и всегда корректируйте политику и процедуры безопасности, чтобы отразить изменения, необходимость которых выявил инцидент.

Оценивая ущерб. Прежде чем начинать восстановительные работы, необходимо уяснить истинные размеры ущерба. Возможно, на это уйдет много времени, но зато появится понимание природы инцидента и будет заложена база для проведения расследования. Лучше всего сравнивать текущее состояние с резервными копиями или с лентами, полученными от поставщика; еще раз напомним: предварительная подготовка – ключевой элемент восстановления. Если система поддерживает централизованное ведение регистрационного журнала (как правило, так и бывает), перемещайтесь по журналу назад и отмечайте аномалии.

Если ведется учет запускаемых процессов и времени сеансов, попытайтесь определить типичные профили использования системы. В меньшей степени способна пролить свет на инцидент статистика доступа к дискам. Учетная информация может дать богатую пищу для анализа инцидента и официального расследования.

Восстановительные работы. После оценки ущерба следует разработать план восстановительных работ. Как правило, лучше всего восстанавливать сервисы в порядке поступления заявок от пользователей, чтобы минимизировать причиняемые неудобства. Помните, что наличие подходящих процедур восстановления крайне важно; сами эти процедуры специфичны для каждой организации.

Возможно, придется вернуться к начальному состоянию системы с последующей ее настройкой. Чтобы облегчить действия даже в таком, наихудшем, случае, храните записи о начальных установках системы и обо всех внесенных изменениях.

Анализ ситуации. После того как система вроде бы приведена в «безопасное» состояние, в ней, возможно, продолжают таиться дыры или даже ловушки. На фазе «разбора полетов» система должна быть тщательно обследована, чтобы выявить проблемы, упущенные при восстановлении. В качестве отправной точки разумно воспользоваться программными средствами обнаружения слабостей конфигурации (такими, как COPS). Следует, однако, помнить, что эти средства не заменяют постоянного системного мониторинга и хороших административных процедур.

Ведите журнал безопасности. Как уже отмечалось, журнал безопасности наиболее полезен на этапе устранения уязвимых мест. В этой связи упомянем два момента. Во-первых, следует документировать процедуры, использованные для восстановления режима безопасности. В это число могут войти командные процедуры, предназначенные для

периодического запуска с целью проверки надежности системной защиты. Во-вторых, регистрируйте важные системные события. Это может помочь оценить ущерб от инцидента.

Усвоение уроков *Понимание урока.* По завершении инцидента целесообразно составить отчет, в котором описывается инцидент, способы его обнаружения, процедуры исправления ситуации, процедуры мониторинга и усвоенные уроки. Все это способствует ясному пониманию проблемы: трудно извлечь уроки из инцидента, если его причины не были поняты.

Ресурсы:

дополнительные устройства и методы обеспечения безопасности;

Безопасность – это динамический, а не статический процесс. Организации зависят от характера доступных в каждый момент времени защитных средств, устройств и методов. Слежение за новинками в области информационной безопасности поможет поставить новейшие технологии на службу интересам предприятия.

хранилище книг, списков, источников информации;

Собирайте книги, списки, источники информации и т. п. как руководства и справочники по защите систем. Все время пополняйте свое собрание. Помните, что вместе с изменениями систем меняются методы и проблемы безопасности.

сформируйте подгруппу.

Сформируйте подгруппу из числа системных администраторов, которая станет ядром службы информационной безопасности. Наличие подобного коллективного органа позволит проводить обсуждение вопросов безопасности и сопоставление различных точек зрения. Эта подгруппа может также разработать политику безопасности предприятия и периодически совершенствовать комплекс защитных мер.

Совершенствование политики и процедур *Сформируйте механизмы для изменения политики, процедур и инструментов.* Если нарушение режима безопасности стало возможным из-за плохой политики, то пока политика не скорректирована, организация обречена на повторные неприятности. После ликвидации инцидента следует подвергнуть политику и процедуры пересмотру, чтобы очертить круг изменений, необходимых для недопущения аналогичных случаев. Даже если нарушений нет, разумно периодически пересматривать политику и процедуры, поскольку меняется сама современная компьютерная среда.

Процедуры доклада об инцидентах. Необходимо отладить процедуру доклада об инцидентах, чтобы иметь их детальное описание вместе с принятыми мерами. Каждый инцидент должен разбираться подгруппой информационной безопасности предприятия с целью уяснения его сути и выработки предложений по совершенствованию политики и процедур безопасности.

Приложение 4 ПОЛИТИКИ БЕЗОПАСНОСТИ, РЕКОМЕНДУЕМЫЕSANS

Институт SANS подготовил ряд политик безопасности, которые можно найти на сайте института (www.sans.org). К ним относятся:

1) политика допустимого шифрования,
2) политика допустимого использования,
3) руководство по антивирусной защите,
4) политика аудита уязвимостей,
5) политика хранения электронной почты,
6) политика использования электронной почты компании,
7) политика использования паролей,
8) политика оценки рисков,
9) политика безопасности маршрутизатора,
10) политика обеспечения безопасности серверов,

11) политика виртуальных частных сетей,
12) политика беспроводного доступа в сеть компании,
13) политика автоматического перенаправления электронной почты компании,
14) политика классификации информации,
15) политика в отношении паролей для доступа к базам данных,
16) политика безопасности лаборатории демилитаризованной зоны,
17) политика безопасности внутренней лаборатории,
18) политика экстранета,
19) политика этики,
20) политика лаборатории антивирусной защиты.

1. Политика допустимого шифрования

Цель

Основной задачей этой политики является определение разрешенных к использованию алгоритмов шифрования. Политика обеспечивает гарантии соблюдения федеральных законов и юридического разрешения для распространения и использования технологий шифрования за пределами США.

Область действия Политика обязательна для всех сотрудников компании.

Суть политики Для шифрования должны быть использованы испытанные стандартные алгоритмы типа DES, Blowfish, RSA, RC5 и IDEA. Эти алгоритмы могут быть использованы в приложениях, разрешенных к применению в компании. Например, PGP производства NAI применяет комбинацию IDEA и RSA или Diffie-Hellman, в то время как SSL – шифрование RSA. Ключи для симметричного шифрования должны иметь длину как минимум 56 бит. Ключи для асимметричного шифрования должны иметь длину, соответствующую аналогичной стойкости. Требования к длине ключей должны пересматриваться в компании ежегодно.

Использование других алгоритмов шифрования разрешено, если это рекомендовано квалифицированной группой экспертов и получено разрешение отдела информационной безопасности. Экспорт технологий шифрования за пределы США ограничен экспортными законами. Резиденты за пределами США, использующие шифрование, обязаны ориентироваться на законы стран, в которых они находятся.

Ответственность К любому сотруднику, нарушившему эту политику, могут быть применены дисциплинарные меры, вплоть до увольнения.

Термины и определения *Симметричное шифрование* – метод шифрования, при котором один и тот же ключ используется и для шифрования, и для дешифрования.

Асимметричное шифрование – метод шифрования, при котором один ключ используется для шифрования, а другой – для дешифрования.

2. Политика допустимого использования Основной задачей издания этой политики отделом информационной безопасности является не наложение ограничений на установленную в компании культуру открытости, доверия и целостности, а защита сотрудников и партнеров компании от преднамеренных и непреднамеренных противоправных действий со стороны других людей. Системы компании, связанные с Интернетом/интранетом/экстранетом, включая компьютерное оборудование, программное обеспечение, операционные системы, системы хранения данных, учетные записи для доступа к электронной почте, к Web-ресурсам, являются собственностью компании. Эти системы должны использоваться только с деловой целью в интересах компании и ее клиентов.

Цель Цель этой политики состоит в определении допустимого использования компьютерного оборудования в компании. Эти правила предназначены для защиты компании и ее сотрудников, чтобы не подвергать их рискам, включая вирусные атаки, взлом систем, и не допускать возникновения юридических проблем.

Область действия Политика обязательна для всех сотрудников, подрядчиков, консультантов, временных сотрудников и других работающих в компании, включая весь персонал сторонних компаний, пользующихся информационными системами или

оборудованием компании. Положения этой политики относятся и ко всему оборудованию, которое является собственностью компании или взято ею в аренду.

Суть политики Общие вопросы использования и владения:

• администраторы корпоративной сети стремятся обеспечить разумный уровень конфиденциальности передаваемых сотрудниками данных, а сотрудники должны знать, что данные, которые они создают в корпоративных системах, являются собственностью компании. Из-за необходимости обеспечения безопасности корпоративной сети компании, руководство не может гарантировать конфиденциальность информации, хранимой на любом устройстве сети, принадлежащем компании;

• сотрудники ответственны за использование ресурсов компании в личных целях. Отделы ответственны за создание руководящих документов по использованию ресурсов компании в личных целях. При отсутствии таких политик сотрудникам следует руководствоваться требованиями и положениями политик более высокого уровня, в случае возникновения вопросов необходимо обращаться к своему непосредственному начальнику;

• отдел информационной безопасности рекомендует, чтобы любая информация, которую сотрудники считают важной, была зашифрована. В качестве руководства по классификации информации и ее защите используйте политику по защите информации отдела информационной безопасности. По вопросам шифрования сообщений электронной почты и документов используйте ознакомительные программы, разработанные отделом информационной безопасности;

• в соответствии с политикой аудита уязвимостей, определен список людей, имеющих право мониторинга оборудования, информационных систем и сетевого трафика в любое время;

• компания имеет право периодически проводить аудит корпоративной сети и информационных систем для проверки выполнения этой политики.

Безопасность и конфиденциальная информация компании: • пользовательские интерфейсы для доступа к корпоративной информации должны быть классифицированы как конфиденциальные или неконфиденциальные в соответствии с руководящими документами по вопросам конфиденциальности, которые находятся в отделе кадров. Конфиденциальной информацией могут быть списки клиентов, планы стратегического развития, торговые секреты и т. д. Сотрудники должны принять все необходимые меры, чтобы предотвратить неправомочный доступ к этой информации;

• сотрудники компании ответственны за безопасность их паролей и учетных записей. Пароли системного уровня должны изменяться один раз в квартал, пароли учетных записей сотрудников должны изменяться раз в шесть месяцев;

• при появлении у сотрудника необходимости оставить рабочее место без присмотра все серверы, портативные компьютеры и автоматизированные рабочие места должны быть защищены включением скринсейвера с паролем, активирующимся после 10 или менее минут бездействия, или путем выхода из системы (logging-off);

• шифрование используется в соответствии с политикой допустимого шифрования отдела информационной безопасности;

• поскольку информация, содержащаяся в портативных компьютерах, более уязвима, необходимо предпринимать усиленные меры безопасности;

• при использовании корпоративной электронной почты сотрудники должны указывать, что выраженные ими мнения являются только их собственными и не представляют собой точку зрения компании, кроме случаев, когда они выполняют при этом свои деловые обязанности;

• все компьютеры, используемые сотрудниками для доступа к ресурсам компании, независимо от того, являются они собственностью компании или принадлежат сотруднику, должны иметь утвержденное отделом безопасности информации антивирусное программное обеспечение с самой последней базой обновлений;

• сотрудники должны быть особенно внимательны при открытии вложений в

сообщениях электронной почты, полученных от неизвестных отправителей, так как они могут содержать вирусы, почтовые «бомбы» или программы типа «Троянский конь».

Запрещается! Список, представленный ниже, не является исчерпывающим, но здесь сделана попытка определить действия, которые попадают в категорию запрещенных:

в сфере действий в корпоративной сети • нарушения прав любого человека или компании, защищенных авторским правом, законами о торговых секретах, патентами или другим законом о защите интеллектуальной собственности, включая установку или распространение «пиратского» или другого программного обеспечения, которые не лицензировано для использования в компании;

• неправомочное копирование защищенного авторским правом материала, включая преобразование в цифровую форму и распространение фотографий из журналов, книг или других защищенных авторским правом источников, музыки и установка любого защищенного авторским правом программного обеспечения, для которого компания или данный сотрудник не имеют действующей лицензии;

• экспорт программного обеспечения, технической информации, программного обеспечения по шифрованию данных или технологии в нарушение международных или региональных экспортных законов. Перед экспортированием любого материала руководство должно проконсультироваться с соответствующими органами;

• запуск злонамеренных программ в сети или на компьютере (например, вирусов, «червей», «Троянских коней», почтовых «бомб», и т. д.);

• разглашение ваших паролей другим сотрудникам или разрешение пользоваться кому-либо вашей учетной записью или паролями. Сюда относятся и члены семьи, если работа выполняется дома;

• использование корпоративных ресурсов для создания, передачи или хранения материалов сексуального, религиозного и другого характера, не относящихся к выполнению служебных обязанностей;

• мошеннические предложения изделий, продуктов или услуг с использованием учетной записи пользователя компании;

• создание заявления о гарантиях, явных или подразумеваемых, если это не является частью обязанностей при выполнении работы;

• нарушение безопасности корпоративной сети: получение доступа к данным, к которым сотрудник не должен его иметь; регистрация на ресурсах, к которым сотруднику явно не разрешен доступ; прослушивание сетевого трафика; выполнение различных атак на ресурсы компании и т. д.;

• сканирование портов или поиск уязвимостей, если на это не получено разрешение от отдела информационной безопасности;

• выполнение любой формы мониторинга сети с перехватом данных, не направленных на компьютер сотрудника, если эта деятельность не является частью его обязанностей;

• попытки обхода систем установления подлинности или безопасности приложений, операционных систем и оборудования;

• попытки ограничения доступа сотрудников к корпоративным ресурсам, за исключением компьютера сотрудника;

• использование программ/скриптов/команд или отправки сообщений любого вида с намерением ограничить доступ или разорвать сессию другого сотрудника;

• разглашение списка сотрудников компании сторонним организациям или лицам;

в сфере, связанной с передачей информации в электронном виде • посылка сообщений электронной почты с незапрашиваемой получателем информацией (junk-mail) или рекламного материала кому-либо без его просьбы (спам электронной почты);

• любая форма преследования через электронную почту, телефон или пейджер;

• неправомерное использование или подделывание заголовков почтовых сообщений;

• подслушивание сообщений электронной почты других сотрудников;

• создание или отправление «цепочек писем» или других писем по схеме типа

«пирамида»;

• использование электронной почты других поставщиков интернет-услуг для рекламирования услуг и продуктов своей компании;

• отправка не относящихся к бизнесу сообщений большому количеству участников новостных групп (спам новостных групп).

Ни при каких обстоятельствах сотрудник компании не должен участвовать в любой деятельности, которая является незаконной по местным, федеральным или международным законам с использованием средств и ресурсов компании.

Ответственность К любому сотруднику, нарушившему эту политику, могут быть применены дисциплинарные меры, вплоть до увольнения.

Термины и определения *Спам* – неразрешенные и/или незапрашиваемые массовые отправки электронных почтовых сообщений.

3. Руководство по антивирусной защите Для предупреждения вирусного заражения рекомендуется:

• использовать на своих компьютерах рекомендованное в качестве стандарта для компании антивирусное программное обеспечение. Базы вирусных сигнатур должны обновляться регулярно;

• никогда не открывать файлы и не выполнять макросы, полученные в почтовых сообщениях от неизвестного или подозрительного отправителя. Удалять подозрительные вложения, не открывая их, и очищать корзину, где хранятся удаленные сообщения;

• удалять спам, рекламу и другие бесполезные сообщения, как описано в политике допустимого использования;

• никогда не загружать файлы и программное обеспечение из подозрительных или неизвестных источников;

• не допускать предоставления дисков в совместное использование на чтение/запись, если только это не абсолютно необходимо;

• всегда проверять дискеты на наличие вирусов;

• периодически резервировать важные данные и системную конфигурацию, хранить резервные копии в безопасном месте;

• если при тестировании в лаборатории происходит конфликт с антивирусным программным обеспечением, то можно его отключить, провести тестирование и сразу включить обратно. При отключенном антивирусном программном обеспечении не выполнять никаких приложений, которые могут привести к распространению вируса (например, почтовые программы);

• периодически проверять политику лаборатории антивирусной защиты и данное руководство на предмет обновлений, так как новые вирусы появляются почти каждый день.

4. Политика хранения электронной почты ***Цель***

Политика хранения электронной почты предназначена для помощи сотрудникам в определении, какая информация, посланная или полученная по электронной почте, должна быть сохранена и на какой срок.

По вопросам надлежащей классификации информации следует обращаться к вашему менеджеру. По вопросам, связанным с этой политикой, нужно обращаться в отдел информационной безопасности.

Вся информация, содержащаяся в сообщениях электронной почты, разделена на четыре основные категории, определяющие время хранения:

• административная корреспонденция – 4 года;

• финансовая корреспонденция – 4 года;

• общая корреспонденция – 1 год;

• недолговечная корреспонденция (хранят, пока не прочитают, потом уничтожают).

Суть политики *Административная корреспонденция.* Административная корреспонденция компании включает (но не ограничена этим) информацию об отпусках, поведении на рабочем месте и о любых юридических проблемах, например о нарушении

интеллектуальной собственности. Вся электронная почта с пометкой «Для руководства» будет рассматриваться как административная корреспонденция. Для гарантии сохранения административной корреспонденции создан почтовый ящик admin@CompanyName. при копировании сообщения на этот адрес ответственность за его хранение будет нести отдел информационных технологий.

Финансовая корреспонденция. Финансовая корреспонденция – вся информация, связанная с доходами и расходами компании. Для гарантии сохранения финансовой корреспонденции создан почтовый ящик fiscal@CompanyName. при копировании сообщения на этот адрес ответственность за его хранение будет нести отдел информационных технологий.

Общая корреспонденция. К общей корреспонденции относится информация, которая имеет отношение к взаимодействию с клиентами. Каждый сотрудник ответственен за хранение электронной почты такого типа.

Недолговечная корреспонденция. Недолговечная корреспонденция, безусловно, наиболее объемная категория, включающая личную электронную почту, запросы или рассылки, электронную почту, связанную с разработкой продуктов и услуг и т. д.

Службы мгновенного обмена сообщениями. Общая корреспонденция, проходящая через службы мгновенного обмена сообщениями, может быть сохранена с использованием функции журналирования службы или путем копирования в файл. Сообщения, проходящие через службу мгновенного обмена сообщениями, которые являются административными или финансовыми, должны быть скопированы и отправлены по электронной почте на соответствующий адрес для хранения.

Шифрование сообщений. Шифрование сообщений должно соответствовать политике обработки и хранения информации, но, вообще, информация должна храниться в незашифрованном виде.

Восстановление удаленных почтовых сообщений с использованием резервных копий. Отдел информационных технологий отвечает за поддержание резервных копий в актуальном состоянии с хранением копий за пределами компании.

Ответственность Любой сотрудник, нарушивший эту политику, может быть подвергнут дисциплинарным мерам, вплоть до увольнения.

Термины и определения *Разрешенная электронная почта* – все почтовые системы, поддерживаемые отделом информационных технологий. Если в связи с выполнением служебных обязанностей необходимо использовать адрес электронной почты вне компании, следует обратиться в отдел информационных технологий.

Разрешенное шифрование электронной почты и файлов – методы шифрования, включающие использование DES и PGP. Шифрование DES доступно во многих бесплатных программах на всех платформах. Для использования PGP в компании необходимо приобрести лицензию. За помощью в приобретении нужно обратиться в отдел информационных технологий.

Разрешенное средство мгновенного обмена сообщениями – Jabber Secure IM Client – является единственным средством мгновенного обмена сообщениями, разрешенным для использования на компьютерах компании.

Средства контроля доступа – методы электронной защиты файлов от получения к ним доступа неавторизованными сотрудниками, кроме тех, кому это разрешено владельцем ресурса.

Незащищенные каналы – все каналы связи, которые не находятся под контролем компании.

Шифрование – важная информация защищается в соответствии с политикой допустимого шифрования. Международные законы по использованию средств шифрования неоднозначны. Следуйте корпоративным руководящим документам по использованию средств криптографии и консультируйтесь с вашим менеджером и/или корпоративными юридическими службами.

5. Политика использования электронной почты компании ***Цель***

Недопущение нанесения ущерба имиджу компании, поскольку электронная почта, отправляемая с электронного почтового адреса компании, рассматривается сторонними лицами и организациями как официальное утверждение от имени компании.

Эта политика описывает порядок использования электронной почты, посылаемой с почтовых адресов компании, и должна выполняться всеми служащими, продавцами и агентами, работающими от имени компании.

Суть политики *Запрещается!* Система электронной почты компании не должна использоваться для создания или распространения любых материалов, не связанных с деятельностью компании, включая материалы националистического, сексуального, порнографического, религиозного и политического характера. Сотрудник, получивший электронное письмо такого содержания от любого работающего в компании, должен немедленно сообщить об этом своему руководителю.

Использование в личных целях. Использование ресурсов компании в личных целях приемлемо в разумных пределах, но такие электронные письма должны храниться в отдельной папке.

Отправка рекламных писем или развлекательных почтовых сообщений от имени компании запрещена. Отправка предупреждений о вирусах и любых других предупреждений, массовые отправки почтовых сообщений от имени компании должны быть одобрены руководством компании перед посылкой. Эти ограничения относятся также к переадресации почты, полученной служащим.

Мониторинг. Сотрудникам компании не следует ожидать соблюдения конфиденциальности почтовых сообщений при хранении, отсылке или приеме почты в системе электронной почты компании. Компания может контролировать почтовые сообщения без уведомления сотрудника.

Ответственность Любой сотрудник, нарушивший эту политику, может быть подвергнут дисциплинарным мерам, вплоть до увольнения.

Термины и определения *Электронная почта* – передача информации через почтовый протокол типа SMTP или IMAP. Почтовыми клиентами могут быть, например, Eudora или Microsoft Outlook.

Переадресация почты – электронная почта, полученная на почтовый адрес компании и перенаправленная на почтовый адрес, не принадлежащий компании.

Важная информация – информация, разглашение которой может повредить компании или репутации ее клиентов, или положению на рынке.

Предупреждение о вирусе – предупреждение о возможном заражении вирусом. Подавляющее большинство таких электронных сообщений является обманом и содержит информацию для запугивания или введения в заблуждение сотрудников.

Разглашение информации – намеренное или неумышленное раскрытие ограниченной для распространения информации людям, которые не должны ее знать.

6. Политика использования паролей Пароли – важный аспект компьютерной безопасности. Они являются первой линией защиты учетных записей сотрудников. Неправильно выбранный пароль может привести к проникновению злоумышленника в корпоративную сеть компании. Все сотрудники компании (включая подрядчиков и продавцов, имеющих доступ к информационным системам компании) ответственны за правильный выбор и хранение паролей (в соответствии с приведенными ниже рекомендациями).

Цель Цель этой политики состоит в том, чтобы установить стандарты по созданию устойчивых к взлому паролей, по защите этих паролей и определению частоты изменения паролей.

Область действия Все, кто имеет доступ или ответственен за предоставление доступа к любой информационной системе компании.

Суть политики *Общие вопросы:*

• все пароли уровня системы (например, для root в системах UNIX, для enable в оборудовании Cisco, для administrator в системах Windows, администраторские пароли в приложениях и т. д.) должны меняться по крайней мере один раз в квартал;

• все пароли на критичные элементы инфраструктуры (серверы, приложения, активное сетевое оборудование) должны храниться в отделе информационной безопасности;

• все пользовательские пароли (например, пароли для доступа к электронной почте, сети, персональному компьютеру, и т. д.) должны меняться по крайней мере один раз в шесть месяцев. Рекомендованный интервал – четыре месяца;

• учетные записи сотрудников, которым предоставили доступ к административным учетным записям на системах через членство в группах или посредством программ типа sudo, должны иметь пароль, отличный от всех других паролей данного пользователя;

• запрещается отправлять пароли в сообщениях электронной почты или с помощью других форм электронного обмена информацией;

• при использовании SNMP community strings не должны быть значениями по умолчанию и должны отличаться от паролей, используемых для аутентификации в интерактивном режиме. Обязательно использование хешей паролей (например, SNMPv2), если это возможно;

• все пароли должны соответствовать стандартам, приведенным ниже.

Руководства:

основные принципы выбора паролей;

Пароли используются для учетных записей сотрудников, для доступа к Web-сайтам, к электронной почте, в режим конфигурирования маршрутизатора. Так как очень небольшое число систем поддерживают использование одноразовых (one-time) паролей, каждый должен знать правила выбора защищенного от взлома пароля и неукоснительно следовать им.

Неправильно подобранные пароли имеют следующие особенности:

– содержат меньше восьми символов;

– являются словами, которые можно найти в словаре;

– представляют собой часто используемые слова: фамилии, клички домашних животных, имена друзей, сотрудников и т. д.; компьютерные термины, названия команд, сайтов, компаний, аппаратных средств, программного обеспечения, – дни рождения и другую личную информацию типа адресов и телефонных номеров; слова или числа типа aaabbb, набранные подряд несколько символов на клавиатуре, например qwerty, zyxwvuts, 123321 и т. д.; любой из вышеупомянутых паролей, записанный в обратном порядке; любой из вышеупомянутых паролей, в начале или в конце которого присутствует цифра (например, secret 1, 1 secret).

Устойчивые к взлому пароли имеют следующие особенности:

– содержат как прописные, так и строчные буквы (например, a-z,A-Z);

– имеют цифры и знаки пунктуации, например 0–9! *$ % A* * () _ + | ~-= \

– их длина составляет по крайней мере восемь алфавитно-цифровых символов;

– не являются словами из какого-либо языка, сленга, диалекта, жаргона и т. д.;

– не основаны на личной информации (фамилии, имени);

– пароли нигде не записаны и не хранятся в компьютере. Для создания легко запоминаемого, устойчивого к взлому пароля можно использовать, например, первые буквы куплета песни или другой фразы. Например, берется фраза: «This May Be One Way To Remember», и пароль может быть таким: «TmBlw2R!» или «TmblW› г ~».

...

Примечание: не используйте ни один из приведенных примеров в качестве пароля.

руководство по защите пароля;

Не используйте один и тот же пароль для доступа к ресурсам компании и для доступа к

внешним, по отношению к компании, ресурсам. Везде, где возможно, используйте разные пароли для доступа к ресурсам компании. Например, выберите один пароль для доступа к системе электронной почты и другой для своей учетной записи на компьютере. Никто, кроме вас, не должен знать ваши пароли. Все пароли являются конфиденциальной информацией.

Запрещается:

– сообщать кому-либо свой пароль по телефону;

– отправлять пароль в сообщении электронной почты;

– показывать пароль своему начальнику;

– называть пароль в присутствии других людей;

– намекать на формат пароля (например, «моя фамилия»);

– писать пароль в анкетных опросах;

– давать свой пароль членам семьи;

– давать пароль сотрудникам на время своего отпуска.

Если кто-то требует сообщить ему ваш пароль, покажите ему этот документ или сообщите сотрудникам отдела информационной безопасности. Не используйте возможность запоминания пароля приложениями (например, Eudora, Outlook, Netscape Communicator). Не записывайте пароли на бумаге и не храните их в вашем офисе. Не храните пароли в файле на компьютерной системе (включая Palm Pilot или подобные устройства) без шифрования. Пароли должны меняться по крайней мере раз в шесть месяцев (кроме паролей уровня системы, которые должны меняться ежеквартально). Рекомендованный интервал – четыре месяца. Если учетная запись или пароль, как вы подозреваете, были скомпрометированы, сообщите об инциденте в отдел информационной безопасности и измените все пароли. Подбор паролей периодически выполняется отделом информационной безопасности. Если пароль будет взломан во время одной из таких проверок, то пользователь обязан поменять его.

руководство по разработке приложений;

Разработчики приложений должны гарантировать, что их программы содержат следующие меры безопасности. Приложения:

– должны иметь возможность идентификации подлинности сотрудников, а не групп;

– не должны хранить пароли в незашифрованном виде или в любой другой форме, которая позволит получить к ним доступ;

– должны предусматривать управление ролями сотрудников так, чтобы один пользователь мог выполнять функции другого, не зная пароля этого пользователя;

– должны поддерживать TACACS+, RADIUS и/или X.509 с исправлениями безопасности для LDAP везде, где возможно.

использование паролей или ключевых фраз (passphrase) для удаленного доступа сотрудников;

Доступ к сети компании через систему удаленного доступа должен осуществляться с использованием или одноразовых (one-time) паролей, или инфраструктуры открытых ключей.

ключевая фраза (passphrase).

Ключевая фраза применяется для идентификации подлинности пользователя при использовании инфраструктуры открытых ключей. Данная фраза определяет математические отношения между публичным ключом, который известен всем, и секретным ключом, известным только пользователю. Без этой фразы пользователь не может получить доступ к секретному ключу. Ключевая фраза – это не то же самое, что пароль. Ключевая фраза – более длинная версия пароля и поэтому лучше защищена от взлома. Обычно составляется из нескольких слов. Из-за этого ключевая фраза лучше защищена от взлома методом грубой силы (brute-force). Правильно подобранная ключевая фраза достаточно длинная и содержит комбинацию прописных и строчных символов, чисел и знаков препинания. Пример: «The*?#› *@ TrafficOnThelOlWas* & #! #ThisMorning». Все правила, указанные выше для паролей, обязательны и для ключевых фраз.

Ответственность Любой сотрудник, нарушивший эту политику, может быть подвергнут дисциплинарным мерам, вплоть до увольнения.

Термины и определения *Учетная запись администратора приложения* – любая учетная запись для администрирования приложения (например, администратор базы данных Oracle).

7. Политика оценки рисков ***Цель***

Дать право отделу информационной безопасности проводить периодическую оценку рисков информационной безопасности для определения степени уязвимости и инициирования защитных процессов.

Область действия Оценка рисков может быть произведена в отношении любого объекта внутри компании или объекта за ее пределами, если компания имеет соглашения со сторонними организациями. Оценка рисков может быть произведена в отношении любой информационной системы, включая приложения, серверы или сети, любых процессов или процедур, с помощью которых эти системы администрируются и/или поддерживаются.

Суть политики Выполнение, разработка и внедрение мер по уменьшению рисков – обязанность отдела информационной безопасности и отдела, занимающегося поддержкой конкретной системы. Пользователи, ответственные за системы, должны работать совместно с отделом информационной безопасности при проведении оценки рисков и при разработке плана по их уменьшению.

Ответственность К любому сотруднику, нарушившему эту политику, могут быть применены дисциплинарные меры, вплоть до увольнения.

Термины и определения *Объект* – любое подразделение, отдел, группа или третья сторона, внутренние или внешние по отношению к компании, ответственные за поддержание и сохранность ресурсов компании.

Риск – факторы, которые могут нарушать конфиденциальность, целостность или доступность информационных ценностей или систем компании. Отдел информационной безопасности отвечает за поддержание целостности, доступности и конфиденциальности критичной информации и ресурсов и за уменьшение влияния процедур и политик безопасности на производительность компании.

8. Политика безопасности маршрутизатора ***Цель***

Этот документ описывает минимально необходимые настройки безопасности в конфигурации всех маршрутизаторов и коммутаторов, имеющих соединение с корпоративной сетью компании или управляемых специалистами компании в рамках предоставления услуг клиентам.

Область действия Затрагивает все маршрутизаторы и коммутаторы, соединяющиеся с корпоративной сетью компании. Не затрагивает маршрутизаторы и коммутаторы во внутренней сети компании и в тестовых лабораториях. Маршрутизаторы и коммутаторы в демилитаризованной зоне относятся к политике оборудования демилитаризованной зоны.

Суть политики Каждый маршрутизатор должен иметь следующие настройки конфигурации:

• на маршрутизаторе не должны создаваться никакие локальные учетные записи. Маршрутизаторы должны использовать TACACS+ для аутентификации сотрудников;

• ЕпаЬІе-пароль на маршрутизаторе должен храниться в зашифрованном виде. Маршрутизатор должен иметь enable-пароль, установленный организацией, поддерживающей маршрутизатор;

• на маршрутизаторе должны быть отключены:

– IP directed broadcast,

– входящие пакеты с недействительными адресами, например из RFC1918,

– TCP small services,

– UDP small services,

– весь source routing,

– Web-сервер маршрутизатора;

• маршрутизаторы должны использовать корпоративную стандартизированную community string SNMP;

• списки контроля доступа добавляются по мере необходимости;

• маршрутизатор должен быть включен в корпоративную систему управления сетью и иметь ответственного за него сотрудника;

• каждый маршрутизатор должен иметь следующее приглашение: «Неправомочный доступ к этому устройству сети запрещен. Вы должны иметь явное разрешение для получения доступа или конфигурирования этого устройства. Все действия, выполненные на этом устройстве, будут зарегистрированы, и нарушения этой политики могут иметь своим следствием дисциплинарные меры, о них может быть сообщено в правоохранительные органы. Конфиденциальность действий на устройстве не гарантируется».

Ответственность К любому сотруднику, нарушившему эту политику, могут быть применены дисциплинарные меры, вплоть до увольнения.

Термины и определения *Производственная сеть* – сеть, используемая в ежедневном бизнесе компании.

Лабораторная сеть – любая сеть, используемая для тестирования, демонстраций, обучения и т. д., нарушение функционирования которой не повлияет на производственную сеть.

9. Политика обеспечения безопасности серверов ***Цель***

Установить стандарты конфигураций серверов, находящихся под управлением сотрудников компании. Эффективное выполнение этой политики минимизирует неправомерный доступ к секретам и технологиям компании.

Область действия Эта политика охватывает оборудование, находящееся в собственности компании и/или используемое в ее сети. Данная политика предназначена только для оборудования, находящегося во внутренней сети компании. Стандарты по конфигурации оборудования, находящегося в демилитаризованной зоне, приведены в описании политики оборудования демилитаризованной зоны.

Суть политики *Владельцы и обязанности.* Все внутренние серверы, развернутые в сети компании, должны быть закреплены за эксплуатационной группой, которая является ответственной за администрирование систем. Стандарты конфигурации серверов устанавливаются и поддерживаются эксплуатационной группой исходя из бизнес-потребностей, одобряются они отделом информационной безопасности. Эксплуатационные группы должны отслеживать соответствие конфигурации стандартам, а в случае необходимости – реализовывать отклонения от стандартов. Каждая эксплуатационная группа определяет процесс изменения стандартов конфигурации, который должен включать в себя анализ изменений и разрешение от отдела информационной безопасности.

Требования отдела информационной безопасности:

• серверы должны быть зарегистрированы в корпоративной системе управления компании. Как минимум, должна иметься следующая информация о сервере: ответственный, местоположение оборудования и ответственный за резервное копирование; производитель оборудования и версия операционной системы; основные функции и приложения;

• информация в корпоративной системе управления компании должна своевременно обновляться;

• изменения в конфигурациях серверов должны соответствовать процедурам управления изменениями.

Основные настройки конфигурации:

• конфигурация операционной системы должна быть произведена в соответствии с установленными отделом информационной безопасности стандартами;

• неиспользуемые сервисы и приложения должны быть отключены/удалены;

• доступ к сервисам должен журналироваться и/или защищаться с использованием методов контроля доступа;

• обновления средств безопасности должны быть установлены сразу после их появления, допустимо единственное исключение, когда приложение не может быть остановлено из-за его критичности;

• доверительные отношения между системами приводят к увеличению рисков безопасности. Не используйте доверительные отношения, если есть другой метод, способный реализовать необходимые задачи;

• необходимо всегда использовать принцип наименьших привилегий;

• не следует использовать администраторскую учетную запись, если можно выполнить задачу с применением непривилегированной учетной записи;

• привилегированный доступ, если это технически возможно, должен осуществляться с помощью SSH или IPSec;

• серверы должны быть физически расположены в помещении с ограниченным доступом;

• запрещается размещать серверы в незащищенных помещениях.

Мониторинг. Все связанные с безопасностью события на критических или важных системах регистрируются, и журналы должны храниться следующим образом: • все связанные с безопасностью события хранятся в офисе как минимум 1 неделю;

• ежедневные инкрементальные резервные копии хранятся в течение 1 месяца;

• еженедельные полные резервные копии журналов хранятся в течение 1 месяца;

• ежемесячные полные резервные копии хранятся как минимум 2 года;

• о событиях, связанных с нарушением безопасности, следует немедленно сообщать в отдел информационной безопасности, который будет проводить анализ и разбор инцидентов. При необходимости будут определены корректирующие меры защиты. События, связанные с нарушением безопасности, включают: сканирование портов, доказательства неправомерного доступа к привилегированным учетным записям, аномальные события, которые не связаны с нормальным функционированием приложений, и т. д.

Соглашения: • аудит будет проводиться регулярно;

• управление проведением аудита возлагается на группу внутреннего аудита или на отдел информационной безопасности, в соответствии с политикой аудита уязвимости. Отдел информационной безопасности обрабатывает полученные данные и затем представляет их в соответствующие группы для проведения корректирующих работ;

• должны быть предприняты все меры по недопущению выхода из строя оборудования или остановки сервисов во время проведения аудита.

Ответственность К любому сотруднику, нарушившему эту политику, могут быть применены дисциплинарные меры, вплоть до увольнения.

Термины и определения *Демилитаризованная зона* – часть сети компании, внешняя по отношению к корпоративной сети.

Сервер – в рамках этой политики сервер определяется как внутренний сервер компании. Компьютеры сотрудников и оборудование лабораторий не затрагиваются этой политикой.

10. Политика виртуальных частных сетей

Цель Установить стандарты для удаленного доступа к внутренней корпоративной сети через виртуальные частные сети, построенные с использованием IPSec и L2TP.

Область действия Эта политика обязательна для всех сотрудников компании, внешних консультантов, временных и других работников, включая весь персонал сторонних организаций, использующий виртуальные частные сети для доступа в сеть компании. Эта политика применима и к реализации виртуальной частной сети с использованием IPSec-концентратора.

Суть политики Определенному перечню сотрудников компании и сотрудников сторонних организаций разрешено пользоваться услугами виртуальной частной сети, которая является сервисом, «управляемым пользователем». Это означает, что сотрудник ответственен за выбор интернет-провайдера, проведение инсталляции необходимого

программного обеспечения и оплату связанных с этим расходов. Дальнейшие детали могут быть уточнены в политике удаленного доступа.

Дополнительно следует иметь в виду:

• сотрудник, имеющий доступ в корпоративную сеть через виртуальную частную сеть, несет ответственность за недопущение доступа посторонних лиц во внутреннюю сеть компании;

• аутентификация в виртуальной частной сети происходит с использованием или однократных (one-time) паролей, или архитектуры открытых ключей с устойчивыми к взлому ключевыми фразами;

• после установления виртуальной частной сети весь трафик будет идти только через туннель, весь другой трафик будет блокироваться;

• двойные туннели запрещены, разрешено только одно сетевое соединение;

• точки терминирования трафика виртуальных частных сетей будут устанавливаться и обслуживаться группой сетевых операций;

• на всех компьютерах, получающих доступ к внутренней корпоративной сети, должно быть установлено принятое в качестве обязательного в компании антивирусное программное обеспечение с самыми последними обновлениями антивирусных баз;

• соединение через виртуальную частную сеть будет прервано в случае 30-минутного бездействия сотрудника. После этого сотрудник должен снова установить соединение. Использование ping или подобных средств для поддержания активности соединения запрещено;

• общее время непрерывного соединения ограничено 24 часами;

• владельцы компьютеров, не являющиеся сотрудниками компании, должны сконфигурировать свои компьютеры в соответствии с политиками информационной безопасности компании;

• в качестве программных и аппаратных клиентов для организации виртуальной частной сети могут выступать только утвержденные отделом информационной безопасности средства;

• при использовании технологии виртуальных частных сетей компьютеры становятся частью корпоративной сети и должны быть сконфигурированы в соответствии с политиками информационной безопасности компании.

Ответственность К любому сотруднику, нарушившему эту политику, могут быть применены дисциплинарные меры, вплоть до увольнения.

Термины и определения *IPSec-концентратор* – устройство, на котором терминируется трафик виртуальной частной сети.

11. Политика беспроводного доступа в сеть компании ***Цель***

Эта политика запрещает доступ к корпоративной сети компании через незащищенные беспроводные подключения. Доступ с использованием беспроводных устройств в сеть компании разрешен только с устройств, соответствующих требованиям этой политики или имеющих разрешение отдела информационной безопасности.

Область действия Эта политика относится ко всем устройствам с возможностью беспроводного доступа во внутреннюю сеть компании (персональным компьютерам, мобильным телефонам, персональным органайзерам и др.). Беспроводные устройства, не имеющие входа во внутреннюю сеть компании, не подпадают под действие этой политики.

Суть политики *Регистрация точек доступа и беспроводных карт.* Все беспроводные точки доступа во внутреннюю сеть компании необходимо зарегистрировать в отделе информационной безопасности и получить разрешение.

Эти точки доступа должны периодически проверяться отделом информационной безопасности на защищенность. Все беспроводные сетевые адаптеры, используемые в переносных и персональных компьютерах, должны быть зарегистрированы в отделе информационной безопасности.

Разрешенная технология. Весь беспроводной доступ во внутреннюю сеть компании

настраивается в соответствии с рекомендациями по защите производителя оборудования и лучшими практиками в этой области.

Использование шифрования и аутентификации. Все компьютеры с устройствами для беспроводного доступа должны использовать для подключения виртуальную частную сеть, сконфигурированную для блокирования незашифрованного и неаутентифицированного трафика. Для соответствия этой политике устройства должны поддерживать аппаратное шифрование «точка-точка» с длиной ключа как минимум 56 бит. Кроме того, все устройства должны иметь уникальный аппаратный адрес, который может быть зарегистрирован и журналирован, например MAC-адрес. Все соединения должны быть аутентифицированы на уровне пользователя с проверкой во внешней базе данных, например TACACS+ или RADIUS.

Установка SSID. SSID должен быть сконфигурирован таким образом, чтобы он не содержал какой-либо информации о компании, например названия компании, отдела, имени сотрудника или идентификатора продукта.

Ответственность Любой сотрудник, нарушивший эту политику, может быть подвергнут дисциплинарным мерам, вплоть до увольнения.

12. Политика автоматического перенаправления электронной почты компании ***Цель***

Недопущение преднамеренного или случайного разглашения конфиденциальной информации компании.

Область действия Эти политика описывает автоматическое перенаправление электронной почты компании и потенциально возможную непреднамеренную передачу конфиденциальной информации сотрудниками компании, вендорами и агентами, действующими от имени компании за ее пределами.

Суть политики Сотрудники должны действовать очень внимательно при отправке любых почтовых сообщений за пределы компании. Почтовые сообщения не должны автоматически перенаправляться за пределы компании, если только не получено разрешение от отдела информационной безопасности. Конфиденциальная информация (подробнее см. в описании политики классификации информации), не должна перенаправляться, кроме случаев, когда это является критически важным для бизнеса, при передаче информация должна быть зашифрована в соответствии с политикой допустимого шифрования.

Ответственность Любой сотрудник, нарушивший эту политику, может быть подвергнут дисциплинарным мерам, вплоть до увольнения.

Термины и определения *Электронное почтовое сообщение* (почтовое сообщение) – передача информации с помощью почтового протокола типа SMTP или IMAP. Почтовыми клиентами могут быть, например, Eudora или Microsoft Outlook.

Переадресация почты – электронная почта, полученная на почтовый адрес компании и перенаправленная на почтовый адрес, не принадлежащий компании.

Разглашение информации – намеренное или неумышленное раскрытие ограниченной для распространения информации людям, которые не должны ее знать.

13. Политика классификации информации

Цель Помочь сотрудникам в определении информации, которая может быть разглашена ими людям, не являющимся сотрудниками компании, и информации, которая не может быть разглашена ими за пределами компании без получения соответствующего разрешения.

Информация, описываемая в этой политике, – любая информация, хранимая или передаваемая внутри компании на бумажных, электронных и других носителях, получаемая или передаваемая посредством голоса или визуально (телефон, видеоконференция).

Все сотрудники должны ознакомиться с правилами хранения и маркирования информации, описанными в этой политике. Уровни важности информации, приведенные ниже, являются руководством и акцентируют внимание на требуемых шагах по защите конфиденциальной информации (например: конфиденциальная информация не должна оставаться без присмотра в комнатах для конференций).

Область действия Вся информация в компании делится на:

• публичную,

• конфиденциальную.

Публичная информация – информация, которая может быть объявлена публично сотрудником, уполномоченным на это, и разглашение этой информации не нанесет ущерба компании. *Конфиденциальная информация* – вся остальная информация. Необходимо понимать, что информация бывает более важной и менее важной, более важная должна быть и защищена более тщательно. К информации, которую нужно защищать очень тщательно, относятся торговые секреты, списки возможных приобретений и другая информация, от которой зависит успех компании. К конфиденциальной информации, которую тоже нужно защищать, хотя и менее тщательно, относятся списки телефонов компании, общая информация о структуре компании, списки сотрудников и т. д.

Частью конфиденциальной информации компании является конфиденциальная информация сторонней компании, с которой заключены контракты и договоры. Защита такой информации описана в «Соглашении о неразглашении» и контрактах. Информация этого типа категоризируется от очень важной до информации о самом факте работы с данной компанией.

Сотрудники компании должны следовать здравому смыслу при защите конфиденциальной информации компании. Если сотрудник сомневается в степени важности обрабатываемой им информации, он должен обратиться к своему руководителю.

Суть политики Руководства, представленные ниже, описывают шаги по защите информации с различным уровнем важности. Сотрудники должны использовать эти руководства только как общие рекомендации, так как конфиденциальная информация может, в зависимости от обстоятельств, нуждаться в большем или меньшем уровне защиты, чем описано.

Минимальная важность – основная информация о компании, некоторая техническая информация и информация о персонале:

• *руководство по маркировке для информации в электронном виде или в виде бумажных копий* (любые из этих маркировок могут быть использованы с дополнительными аннотациями в «Соглашении о конфиденциальности со сторонними организациями») – если маркировка желательна, то фраза ««Название компании» конфиденциально» должна быть размещена на видном месте. Могут быть использованы другие фразы для маркировки, например: «Собственность ‹Название компании›». Даже когда маркировка не произведена, то информация предположительно является конфиденциальной, если только явно не определена как публичная сотрудником, имеющим на это право;

• *доступ* – сотрудники компании, работники по контракту с необходимостью доступа к информации для выполнения ими работы в соответствии со своими обязанностями;

• *распространение внутри компании* – стандартные электронные письма, разрешенные к использованию методы передачи информации по электронным каналам;

• *распространение за пределы компании* – почтовые службы, разрешенные к использованию методы передачи информации по электронным каналам;

• *распространение по электронным каналам – без* ограничений, за исключением того, что информация должна быть отправлена только к разрешенным получателям;

• *хранение* – защищать от просмотра сотрудниками, не имеющими на это прав, не оставлять на столах и досках для записей. Компьютеры, на которых хранится такая информация, должны удовлетворять требованиям политик безопасности компании. Доступ к информации должен контролироваться на уровне списков доступа по пользователям, не по группам. Резервное копирование;

• *уничтожение* – информация уничтожается в специальных устройствах (для бумажных носителей) или перезаписыванием/размагничиванием (для электронных носителей);

• *ответственность за преднамеренное или непреднамеренное разглашение* –

сотрудник, нарушивший эту политику, может быть подвергнут дисциплинарным, вплоть до увольнения, или уголовным мерам наказания.

Более важная – деловая, финансовая, техническая информация и детальная информация о персонале: • *руководство по маркировке для информации в электронном виде или в виде бумажных копий* (любые из этих маркировок могут быть использованы с дополнительными аннотациями в «Соглашении о конфиденциальности со сторонними организациями») – если маркировка желательна, то фраза «‹Название компании› конфиденциально» должна быть размещена на видном месте. Могут быть использованы другие фразы для маркировки, например: «‹Название компании›. Только для внутреннего использования»;

• *доступ* – сотрудники компании, работники по контракту с подписанным «Соглашением о неразглашении» с необходимостью доступа к информации для выполнения ими своих обязанностей;

• *распространение внутри компании* – стандартные электронные письма, разрешенные к использованию методы передачи информации по электронным каналам;

• распространение за пределы компании – почтовые службы;

• *распространение по электронным каналам – без* ограничений, за исключением того, что информация должна быть отправлена только к разрешенным получателям и должна быть зашифрована или отправлена внутри зашифрованного канала передачи данных;

• *хранение* – доступ к информации должен контролироваться на уровне списков доступа по пользователям, не по группам;

• *уничтожение* – информация уничтожается в специальных устройствах (для бумажных носителей) или перезаписыванием/размагничиванием (для электронных носителей). Должно производиться надежное уничтожение и физическое разрушение носителей;

• *ответственность за преднамеренное или непреднамеренное разглашение* – сотрудник, нарушивший эту политику, может быть подвергнут дисциплинарным, вплоть до увольнения, или уголовным мерам наказания.

Очень важная – торговые секреты, маркетинговая, операционная, финансовая информация, исходные коды и техническая информация, от которой зависит успех деятельности компании: • *руководство по маркировке для информации в электронном виде или в виде бумажных копий* (любые из этих маркировок могут быть использованы с дополнительными аннотациями в «Соглашении о конфиденциальности со сторонними организациями») – с целью определения важности информации для компании используется фраза «Внутренняя ‹Название компании› зарегистрирована и ограниченного доступа», «Только для просмотра сотрудниками ‹Название компании›», «‹Название компании› конфиденциально», размещенная на видном месте;

• *доступ* – только те сотрудники и лица, не являющиеся сотрудниками компании, кто определен в списке имеющих доступ к этой информации, с подписанным «Соглашением о неразглашении»;

• *распространение внутри компании* – подпись о получении, передача в конвертах с печатью «Конфиденциально» или через разрешенные для этой цели способы передачи информации по электронным каналам;

• *распространение за пределы компании* – в защищенных от просмотра конвертах через определенные почтовые службы с росписью в получении;

• *распространение по электронным каналам – без* ограничений, за исключением того, что настоятельно рекомендуется шифровать передаваемую информацию с использованием криптостойких алгоритмов и длинных ключей шифрования;

• *хранение* – доступ к информации должен контролироваться на уровне списков доступа по пользователям, не по группам. Должна быть обеспечена физическая безопасность помещений и компьютеров, в которых хранится информация;

• *уничтожение* – строго предписывается, что информация уничтожается в

специальных промаркированных устройствах (для бумажных носителей) или перезаписыванием/размагничиванием (для электронных носителей). Должно производиться надежное уничтожение и физическое разрушение носителей;

• *ответственность за преднамеренное или непреднамеренное разглашение* – сотрудник, нарушивший эту политику, может быть подвергнут дисциплинарным, вплоть до увольнения, или уголовным мерам наказания.

Ответственность Любой сотрудник, нарушивший эту политику, может быть подвергнут дисциплинарным мерам, вплоть до увольнения.

Термины и определения *Маркировка* – разграничение владельца или ответственного за информацию.

Соответствующие меры – меры, предназначенные для минимизации рисков, связанных с внешними подключениями. Компьютеры компании, используемые конкурентами или сотрудниками, не имеющими на это прав, должны быть ограничены в доступе к информации так, чтобы в случае попытки доступа к информации риск был минимально возможным.

Подключения компании к другим компаниям – соединения должны быть сконфигурированы таким образом, чтобы доступ был разрешен только к тем приложениям и информации, которые необходимы для совместной работы.

Разрешенные электронные способы передачи – разрешенные к использованию в компании FTP-клиенты и Web-браузеры.

Разрешенная электронная почта – все почтовые системы, поддерживаемые отделом информационных технологий и разрешенные к использованию в компании.

Разрешенное шифрование почтовых сообщений и файлов – технологии включают DES и PGP. Шифрование DES доступно во многих бесплатных программах на всех платформах. Для использования PGP в компании необходимо приобрести лицензию. За помощью в приобретении обращайтесь в отдел информационных технологий.

Информационные ресурсы компании – все компьютеры, их данные и программы, так же как информация на бумажных носителях.

Перезапись/удаление – использование специальных программ для перезаписи данных, например из состава Norton Utilities, так как обычное удаление данных средствами операционной системы не приводит к удалению, а только делает их невидимыми для пользователя.

Списки доступа на уровне пользователей – метод защиты информации на электронных носителях от доступа сотрудников, не имеющих на это прав.

Незащищенные интернет-каналы – все сети, которые не находятся под полным контролем компании.

Шифрование – шифрование конфиденциальной информации, осуществляемое в соответствии с политикой допустимого шифрования. Международные проблемы использования шифрования сложны и неоднозначны. Следуйте корпоративным стандартам по экспортному контролю криптографии и консультируйтесь с вашим руководителем и/или юридической службой по связанным с этой проблемой вопросам.

Физическая безопасность – постоянное присутствие рядом с компьютером или прикрепление компьютера к объекту, который не может быть перемещен. Один из методов выполнения такой задачи – наличие ключа для блокировки доступа к компьютеру. Чтобы защитить переносной компьютер, никогда не оставляйте его без присмотра, запирайте комнату, в которой он находится, или сдавайте его в сейф на хранение.

Защищенный канал – электронные коммуникации, над которыми компания имеет полный контроль. Например, все сети компании, соединенные через защищенный канал; компьютер, соединенный с другим посредством модема, а не с использованием мобильного телефона; ISDN-соединения с домашними компьютерами сотрудников.

14. Политика в отношении паролей для доступа к базам данных ***Цель***

Политика определяет требования по обеспечению безопасности хранения и обработки

учетных записей в базах данных и паролей к ним при использовании программного обеспечения, посредством которого сотрудники получают доступ к информации, хранимой в базах данных компании. При неправильных хранении и использовании атрибутов доступа к базам данных они могут быть скомпрометированы.

Область действия Эта политика применяется ко всему программному обеспечению, с помощью которого осуществляется доступ к базам данных компании.

Суть политики *Общие положения.* Для поддержания необходимого уровня безопасности доступ посредством программного обеспечения к базе данных должен разрешаться только после соответствующей аутентификации. Атрибуты, используемые для аутентификации, нельзя размещать в коде программы в незашифрованном виде. Атрибуты доступа к базе данных не должны быть доступны через Web-сереер.

Специфические требования:

хранение учетных записей и паролей:

– учетные записи и пароли для доступа к базе данных должны храниться в файле отдельно от кода программы. Доступ к этому файлу должен быть строго ограничен;

– учетные записи и пароли для доступа к базе данных могут храниться на сервере баз данных. В этом случае хеш от пароля может храниться в выполняемом теле программы;

– учетные записи и пароли для доступа к базе данных могут храниться как часть данных на сервере аутентификации, таком, как LDAP. Аутентификация доступа к базе данных может проходить как часть общей аутентификации в системе;

– учетные записи и пароли для доступа к базе данных нельзя размещать в дереве документов Web-сереера;

– прямой доступ через аутентификацию (например, ORACLE OPSS) не должен разрешать работу с базой данных, основываясь только на аутентификации удаленного пользователя на удаленном компьютере;

– пароли и ключевые фразы, используемые для доступа, должны соответствовать требованиям политики использования паролей;

восстановление учетных записей и паролей:

– если учетная запись и пароль хранятся не в исходном коде программы, то они должны быть считаны из файла непосредственно перед использованием. Сразу после аутентификации область памяти, в которой они размещались, должна быть очищена;

– область, в которой хранятся учетная запись и пароль, должна быть физически отделена от других областей кода, то есть размещаться в отдельном файле;

– для языков программирования, которые выполняются непосредственно из исходного кода (интерпретируемые языки), файл, хранящий учетные записи и пароли, не должен размещаться в той же просматриваемой или выполняемой директории, в которой размещается код программы;

доступ к учетным записям и паролям:

– каждая программа или несколько программ, выполняющих одну функциональную задачу, должны иметь уникальную базу учетных записей и паролей. Использование одной и той же базы учетных записей и паролей для нескольких программ запрещено;

– пароли доступа к базам данных в соответствии с политикой использования паролей считаются паролями системного уровня;

– разработчики должны определить процедуру, гарантирующую, что пароли управляются и изменяются в соответствии с политикой использования паролей. Эта процедура должна включать метод ограничения знания паролей для доступа к базе данных на основе правила «необходимо знать»;

• *техники кодирования для реализации этой политики* (добавьте ссылки к различным языкам кодирования, рекомендованным в вашей компании, таким, как Perl, Java, C и C++).

Ответственность Любой сотрудник, нарушивший эту политику, может быть подвергнут дисциплинарным мерам, вплоть до увольнения.

Термины и определения *Компьютерный язык* – язык, используемый для написания

программ.

Атрибуты доступа – что-то, что вы знаете (пароль или ключевая фраза), и/или что-то, что определяет вас (учетная запись, отпечатки пальцев, сетчатка глаза).

Роль – уровень привилегий, который может быть аутентифицирован и авторизован. Уровень привилегий, на основе которого осуществляется доступ к ресурсам.

Тело выполнения – серия инструкций компьютеру, которые он выполняет для реализации логики программы.

15. Политика безопасности лаборатории демилитаризованной зоны ***Цель***

Эта политика устанавливает требования по информационной безопасности для всех сетей и оборудования, расположенных в демилитаризованной зоне. Выполнение этих требований минимизирует потенциальный риск компании от нанесения ущерба путем получения неавторизованного доступа к ресурсам компании, потери конфиденциальной информации и интеллектуальной собственности компании.

Область действия Субъекты действия этой политики – лабораторные сети и устройства компании (например, маршрутизаторы, коммутаторы, компьютеры и т. д.), которые доступны из Интернета и размещающиеся за пределами корпоративного межсетевого экрана. Сюда же входят лаборатории, находящиеся у поставщика услуг Интернета и в удаленных местах расположения. Все существующее и будущее оборудование, которое подпадает под область действия данной политики, должно быть сконфигурировано в соответствии с этим документом. Данная политика неприменима к лабораториям, размещающимся внутри корпоративного межсетевого экрана. Стандарты для такого оборудования описаны в политике безопасности внутренней лаборатории.

Суть политики *Владение и ответственность:*

• все новые лаборатории демилитаризованной зоны должны иметь письменное обоснование их создания за подписью вице-президента. Обоснования хранятся в отделе информационной безопасности;

• компании, организующие лаборатории, должны определить ответственных менеджеров, основных и резервных контактных лиц для каждой лаборатории. Владельцы лабораторий должны поддерживать список этой информации в актуальном состоянии. Список хранится в отделе информационной безопасности (и в системе управления компанией, если такая существует). Менеджеры лабораторий или резервные контактные лица должны быть доступны круглосуточно;

• должно быть получено разрешение от отдела поддержки сети и отдела информационной безопасности для внесения изменений в схемы подключений и/или задачи существующих лабораторий, а также для создания новых лабораторий;

• все подключения к поставщикам интернет-услуг должны поддерживаться отделом поддержки сети;

• отдел поддержки сети отвечает за поддержку функционирования межсетевого экрана между демилитаризованной зоной и Интернетом;

• отдел поддержки сети и отдел информационной безопасности имеют право заблокировать любые соединения к/от оборудованию лабораторий, если это несет угрозу безопасности сети компании;

• сотрудники лаборатории демилитаризованной зоны поддерживают функционирование всех устройств, расположенных в демилитаризованной зоне до границы зоны ответственности отдела поддержки сети;

• отдел поддержки сети должен иметь список всех IP-адресов и ответственных за оборудование лиц лаборатории демилитаризованной зоны (такой же список хранится в системе управления компанией, если такая существует);

• менеджеры демилитаризованной лаборатории несут полную ответственность за нее в соответствии с этой политикой;

• в соответствии с политикой аудита уязвимостей отделу поддержки сети и отделу

информационной безопасности должен при необходимости предоставляться немедленный доступ к оборудованию и журналам оборудования демилитаризованной зоны;

• тестовые учетные записи должны быть удалены в течение трех дней после того, как доступ станет ненужным. Пароли на групповые учетные записи должны быть изменены в течение трех дней после изменения состава членов группы;

• отдел информационной безопасности будет разбирать каждый случай отказа в доступе.

Основные требования к конфигурации: • производственная сеть компании не должна зависеть от сетей лаборатории демилитаризованной зоны;

• лаборатории демилитаризованной зоны не должны иметь соединений с внутренней сетью компании напрямую или через беспроводную сеть

• оборудование лабораторий демилитаризованной зоны должно быть размещено в серверных, физически отделенных от оборудования внутренних сетей компании. Если это невозможно, то данное оборудование должно размещаться в запираемой на ключ серверной стойке. Менеджер лаборатории должен иметь у себя список, в котором указаны лица, имеющие доступ к оборудованию;

• менеджер лаборатории отвечает за выполнение следующих политик:

– политики использования паролей,

– политики беспроводного доступа в сеть компании,

– политики лаборатории антивирусной защиты;

• отдел поддержки сети, поддерживающий функционирование межсетевых экранов, должен сконфигурировать их в соответствии с принципами наименьшего доступа и обеспечения функционирования лаборатории демилитаризованной зоны. Все списки доступа утверждаются отделом информационной безопасности;

• межсетевой экран должен быть единственной точкой доступа между лабораторией и внутренней сетью компании и/или Интернетом. Все другие способы подключения запрещены;

• начальная конфигурация и любые последующие изменения межсетевых экранов должны быть исследованы и одобрены отделом информационной безопасности. Отдел информационной безопасности может затребовать дополнительные настройки безопасности на межсетевых экранах;

• трафик из лаборатории демилитаризованной зоны во внутреннюю сеть компании, включая доступ посредством частной виртуальной сети, попадает под действие политики удаленного доступа;

• все маршрутизаторы и коммутаторы, не используемые для тестирования и/или обучения, должны быть настроены в соответствии со стандартами для маршрутизатора демилитаризованной зоны и коммутатора демилитаризованной зоны;

• операционные системы всех компьютеров внутри лаборатории демилитаризованной зоны, на которых выполняются интернет-сервисы (HTTP, FTP, SMTP и т. д.), должны быть сконфигурированы в соответствии со стандартом компьютеров демилитаризованной зоны (добавьте здесь ссылку на внутренний сайт, где находятся стандарты конфигураций);

• должны быть установлены все текущие сервисные пакеты и обновления, рекомендованные производителем для всех приложений и операционных систем. Администраторы должны иметь возможность устанавливать появляющиеся обновления быстро и эффективно;

• сервисы и приложения, не используемые для работы, должны быть отключены/деинсталлированы;

• в соответствии с политикой классификации информации запрещается размещать и хранить конфиденциальную информацию на оборудовании лаборатории демилитаризованной зоны, к которому имеют физический доступ сотрудники сторонних организаций;

• удаленное администрирование должно осуществляться по защищенным протоколам

(SSH, IPSEC) или через консольный доступ.

Ответственность Любой сотрудник, нарушивший эту политику, может быть подвергнут дисциплинарным мерам, вплоть до увольнения.

Термины и определения *Списки доступа (ACE)* – списки, хранимые на маршрутизаторах, коммутаторах, межсетевых экранах и регулирующие доступ к сервисам и приложениям.

Демилитаризованная зона – сеть, размещающаяся за пределами внутренней корпоративной сети, но находящаяся под управлением компании.

Отдел поддержки сети – любая утвержденная отделом информационной безопасности группа, управляющая внутренними сетями компании.

Принцип наименьшего доступа – доступ к сервисам, компьютерам, сетям запрещен, если только это не является необходимым для выполнения обязанностей.

Интернет-сервисы – сервисы, выполняющиеся на устройствах, доступных из-за пределов сети. К ним относятся FTP, DNS, HTTP и т. д.

Граница ответственности отдела поддержки сети – точка, в которой ответственность за поддержку сети переходит от отдела поддержки сети к сотрудникам лаборатории демилитаризованной зоны. Обычно это маршрутизатор или межсетевой экран.

Менеджер лаборатории – сотрудник, ответственный за всю лабораторию и ее персонал.

Лаборатория – сотрудники, оборудование и программное обеспечение, объединенные для разработки, тестирования, демонстрирования продуктов и услуг и обучения пользованию ими.

Межсетевой экран – устройство, контролирующее доступ между сетями, такое, как Cisco PIX, маршрутизатор со списками доступа, или подобное устройство, определенное отделом информационной безопасности.

Внутренняя лаборатория – лаборатория внутри корпоративного межсетевого экрана, подключенная к производственной сети компании.

16. Политика безопасности внутренней лаборатории ***Цель***

Эта политика устанавливает требования по информационной безопасности для всех лабораторий компании с целью обеспечения гарантий неразглашения конфиденциальной информации и технологий, а также для гарантии, что производственные сервисы и другие интересы компании защищены от действий, выполняемых в лабораториях.

Область действия Эта политика применима ко всем внутренним лабораториям, сотрудникам компании и сторонних организаций, имеющим доступ в лаборатории компании. Все существующее и будущее оборудование, которое подпадает под действие данной политики, должно быть сконфигурировано в соответствии с перечисленными ниже документами. Лаборатории демилитаризованной зоны и отдельные сети, не подключенные к сети компании, не подпадают под действие этой политики.

Суть политики *Владение и ответственность:*

• компании, организующие лаборатории, должны определить ответственных менеджеров, основных и резервных контактных лиц для каждой лаборатории. Владельцы лабораторий должны поддерживать список этой информации в актуальном состоянии. Список хранится в отделе информационной безопасности (и в системе управления компанией, если такая существует). Менеджеры лабораторий или резервные контактные лица должны быть доступны круглосуточно;

• менеджеры лабораторий несут ответственность за безопасность их лабораторий и воздействие деятельности лабораторий на производственную сеть компании. Если какая-либо политика или процедура недоступна, то менеджеры должны следовать принципам наибольшей защищенности сети компании;

• менеджеры лабораторий несут ответственность за соответствие лаборатории всем политикам безопасности компании. Следующие политики особенно важны: политика использования паролей, политика беспроводного доступа в сеть компании, политика

лаборатории антивирусной защиты и политика физической безопасности;

• менеджеры лабораторий несут ответственность за организацию доступа в лабораторию. Разрешение на доступ в лабораторию выдает только менеджер или лицо, которому делегирована эта обязанность. Доступ предоставляется только для выполнения служебных обязанностей. Сюда относится периодическая проверка списка доступа и немедленное удаление из него лиц, которым этот доступ стал не нужен;

• отдел поддержки сети отвечает за поддержку функционирования межсетевого экрана между производственной сетью и лабораторией;

• отдел поддержки сети и отдел информационной безопасности имеют право заблокировать любые соединения к/от оборудованию лаборатории, если это несет угрозу безопасности сети компании;

• отдел поддержки сети должен иметь список всех IP-адресов и ответственных за оборудование лиц внутренней лаборатории (такой же список хранится в системе управления компанией, если такая существует);

• любая лаборатория, которая захочет иметь доступ за свои границы, должна предоставить документацию в отдел информационной безопасности с аргументированным обоснованием такого доступа, списком оборудования, необходимого для этого, и информацию по IP-адресации. Отдел информационной безопасности исследует документы и разрешает/не разрешает такой доступ;

• все пользовательские пароли должны соответствовать политике использования паролей. Тестовые учетные записи должны быть удалены в течение трех дней после того, как доступ станет ненужным. Пароли на групповые учетные записи необходимо менять ежеквартально, кроме того, они должны быть изменены в течение трех дней после изменения состава членов группы;

• запрещается поддерживать производственные сервисы на оборудовании лаборатории;

• отдел информационной безопасности будет разбирать каждый случай отказа в доступе.

Основные требования к конфигурации: • весь трафик между производственной сетью и сетью лаборатории должен проходить через межсетевой экран, поддерживаемый отделом поддержки сети. Сетевые устройства лаборатории (включая беспроводные) не должны каким-либо другим способом соединяться с внутренней и производственной сетью компании;

• начальная конфигурация и любые последующие изменения межсетевых экранов должны быть исследованы и одобрены отделом информационной безопасности. Отдел информационной безопасности может затребовать дополнительные настройки безопасности на межсетевых экранах;

• в лаборатории запрещена деятельность, которая может негативно сказаться на производственной сети, типа сканирования портов, спуфинг IP-адресов, трафика и т. д. Такого рода деятельность должна быть ограничена рамками лаборатории;

• трафик между лабораторией и производственной сетью, так же как трафик между отдельными сетями лаборатории, используется только в деловых целях и не должен оказывать негативное влияние на другие сети. Лаборатории не должны иметь сетевые сервисы, которые могут скомпрометировать сервисы производственной сети или подвергнуть опасности конфиденциальную информацию, хранимую внутри лаборатории;

• отдел информационной безопасности имеет право проводить аудит всех данных внутри лаборатории, входящего и исходящего трафика, конфигурации всего оборудования;

• шлюзы лаборатории должны соответствовать стандартам безопасности компании и доступ к ним должен осуществляться через сервер аутентификации компании;

• пароли администрирования шлюзов не должны совпадать с какими-либо паролями на другое оборудование. Пароли должны соответствовать политике использования паролей. Пароли будут предоставляться только тем, кому разрешено администрировать сеть лаборатории;

• в лабораториях, где сотрудники сторонних организаций имеют физический доступ к оборудованию, прямое подключение к производственной сети компании запрещено. В соответствии с политикой классификации информации запрещается размещать и хранить конфиденциальную информацию на оборудовании внутренней лаборатории. Удаленное подключение разрешенного списка сотрудников лаборатории в производственную сеть компании должно быть аутентифицировано на корпоративном сервере аутентификации с использованием временных списков доступа (lock and key access control lists) и осуществляться по защищенным протоколам (SSH, IPSEC) или посредством виртуальной частной сети, как определено отделом информационной безопасности;

• инфраструктурные устройства, например IP-телефоны, которым необходим доступ в сеть компании, должны соответствовать политике открытых областей;

• все внешние соединения в лабораторию должны быть осуществлены после исследования и получения разрешения от отдела информационной безопасности. Аналоговые или ISDN-линии должны быть сконфигурированы на прием звонков только с определенных телефонных номеров. Для аутентификации необходимо использовать устойчивые к взлому пароли;

• все лаборатории, имеющие внешние соединения, не должны иметь доступа к производственной или внутренней сетям компании напрямую или через беспроводные сети.

Ответственность Любой сотрудник, нарушивший эту политику, может быть подвергнут дисциплинарным мерам, вплоть до увольнения.

Термины и определения *Демилитаризованная зона* – сеть, размещающаяся за пределами внутренней корпоративной сети, но находящаяся под управлением компании.

Отдел поддержки сети – любая утвержденная отделом информационной безопасности группа, управляющая внутренними сетями компании.

Принцип наименьшего доступа – доступ к сервисам, компьютерам, сетям запрещен, если только это не является необходимым для выполнения обязанностей.

Интернет-сервисы – сервисы, выполняющиеся на устройствах, доступных из-за пределов сети. К ним относятся FTP, DNS, HTTP и т. д.

Граница ответственности отдела поддержки сети – точка, в которой ответственность за поддержку сети переходит от отдела поддержки сети к сотрудникам внутренней лаборатории. Обычно это маршрутизатор или межсетевой экран.

Менеджер лаборатории – сотрудник, ответственный за всю лабораторию и ее персонал.

Лаборатория – сотрудники, оборудование и программное обеспечение, объединенные для разработки, тестирования, демонстрирования продуктов и услуг и обучения пользованию ими.

Межсетевой экран – устройство, контролирующее доступ между сетями, такое как Cisco PIX, маршрутизатор со списками доступа, или подобное устройство, определенное отделом информационной безопасности.

Внутренняя лаборатория – лаборатория внутри корпоративного межсетевого экрана, подключенная к производственной сети компании.

17. Политика экстранета ***Цель***

Документ описывает политику, которую должны выполнять сторонние организации, подключающиеся к сети компании для ведения совместного бизнеса.

Область действия Все соединения к внутренним ресурсам компании, независимо от того, осуществлены они через сети типа Frame Relay, ISDN или посредством виртуальной частной сети, подпадают под действие этой политики. Соединения с поставщиком услуг Интернета и с телефонными сетями общего доступа не подпадают под действие этой политики.

Суть политики *Предпосылки:*

оценка безопасности;

Все новые экстранет-подключения будут оцениваться на предмет обеспечения

безопасности отделом информационной безопасности. Эта оценка будет гарантировать, что подключения наилучшим образом соответствуют бизнес-по– требностям компании и принципам обеспечения наименьшего доступа.

соглашение о подключении со сторонними организациями;

Для выполнения запроса на новое подключение между сторонней организацией и компанией требуется подписание «Соглашения со сторонней организацией» между ней и уполномоченным представителем компании. Это соглашение подписывают вице-президент компании и уполномоченный представитель сторонней организации. Документы, относящиеся к подключениям к лабораториям компании, хранятся в отделе, отвечающем за безопасность данной лаборатории.

бизнес-потребность;

Все экстранет-подключения должны выполняться только для ведения бизнеса с письменным описанием необходимости такого подключения и с разрешением от менеджера проекта. Подключения к лаборатории должны быть разрешены сотрудником, отвечающим за безопасность лаборатории. Обычно порядок подключения описывается как часть «Соглашения со сторонней организацией».

контактные лица.

Сторонняя организация обязана определить сотрудника, ответственного за данное подключение. Это контактное лицо ответственно за выполнение своей части «Соглашения со сторонней организацией». При изменении контактного лица организацией компания должна быть незамедлительно проинформирована.

Установление подключения. Отдел внутри компании, у которого есть необходимость установить соединение со сторонней организацией, оформляет запрос в отдел экстранета, отвечающий за такие подключения. Этот отдел вместе с отделом информационной безопасности исследует все возможные проблемы безопасности, связанные с этим подключением. Если предполагается подключение в лабораторию компании, то в исследовании принимает участие и группа, отвечающая за безопасность данной лаборатории. Сторонняя организация должна предоставить полную информацию о предполагаемом подключении отделу экстранета и отделу информационной безопасности. Все устанавливаемые подключения должны отвечать принципу наименьшего доступа в соответствии с бизнес-требованиями и оценкой безопасности. Компания ни в коем случае не должна полагаться на стороннюю организацию при защите собственных сетей и ресурсов.

Изменение подключения и доступа. Все изменения в подключении и предоставлении доступа должны соответствовать бизнес-потребностям и являются объектом для оценки безопасности. Изменения осуществляются через корпоративную процедуру управления изменениями. Сторонняя организация должна немедленно уведомлять отдел экстранета и отдел информационной безопасности о любых изменениях в подключении или доступе.

Отключение. Сторонняя организация должна уведомить отдел экстранета компании, когда доступ становится не нужен, для прекращения подключения. Это может означать изменение существующих списков доступа или физический разрыв соединения. Отдел экстранета и группа, отвечающая за безопасность лабораторий, должны проводить ежегодный аудит для обеспечения гарантии, что все подключения все еще необходимы и уровень доступа не выше требуемого для выполнения задач. Подключения, не удовлетворяющие этим требованиям, должны быть немедленно разорваны. Отдел информационной безопасности и/или отдел экстранета должны уведомлять стороннюю организацию перед внесением изменений или прекращением подключения.

Ответственность К любому сотруднику, нарушившему эту политику, могут быть применены дисциплинарные меры, вплоть до увольнения.

18. Политика этики Целью компании при написании этой политики является установление культуры открытости, доверия и целостности в деловой деятельности. Эффективная этика – командное усилие, включающее участие и поддержку каждого сотрудника компании. Все служащие должны быть ознакомлены с руководящими

принципами этики.

Компания обязуется защищать сотрудников, партнеров, вендоров и собственный бизнес от злонамеренных умышленных и неумышленных действий. Если компания активно борется с проблемами и правильно использует законодательство, это помогает ей в борьбе с конкурентами.

Компания должна быстро использовать соответствующие меры и средства для решения проблемы при нарушении кодекса этики. Любые нарушения данного кодекса недопустимы.

Цель Цель публикации этого кодекса этики состоит в том, чтобы подчеркнуть ожидания сотрудников и потребителей в практике деловых отношений. Эта политика будет служить основой делового поведения, гарантируемого этическими нормами.

Область действия Данная политика применима ко всем сотрудникам, контрактникам, консультантам, временным сотрудникам и другим работающим в компании, включая весь персонал сторонних организаций-партнеров.

Суть политики *Обязанности руководства по следованию кодексу этики:*

• высшее руководство должно быть первым и главным примером в следовании кодексу этики. В любой деловой практике честность и целостность должны быть главным приоритетом для руководства;

• высшее руководство должно следовать политике открытых дверей и приветствовать предложения и замечания, исходящие от сотрудников. Это позволит сотрудникам комфортно обсуждать любые проблемы и будет напоминать руководству о необходимости заботиться о своей рабочей силе;

• руководство должно разрешать любой конфликт в соответствии с интересами сотрудников компании.

Обязанности сотрудников по следованию кодексу этики: • сотрудники компании будут рассматривать интересы каждого справедливо, соблюдая взаимное уважение, способствуя работе в команде и предупреждая намерения и проявления неэтичного поведения;

• каждый сотрудник должен прилагать интеллектуальные усилия для поддержания этических ценностей;

• сотрудники должны разрешать любые конфликты интересов в соответствии с их позицией в компании;

• сотрудники обязаны помогать компании в повышении степени удовлетворенности клиентов и поставщиков компании посредством своевременного и качественного обслуживания.

Осведомленность компании: • содействие этическому поведению в межличностных отношениях должно вознаграждаться;

• компания должна создавать атмосферу доверия и честности для укрепления этики в компании.

Поддержка этической практики: • компания обязана укреплять важность целостности сообщений, и тон в этом должно задавать руководство. Каждый сотрудник, менеджер и директор должны следовать принципам этического поведения;

• сотрудники компании должны поощрять принципы открытого диалога, получение честных ответов и рассматривать интересы каждого человека справедливо, честно и объективно;

• компании следует создать комитет лучших практик для получения уверенности в том, что кодекс этики доступен всем сотрудникам. Сотрудники могут обращаться в этот комитет по любым вопросам, связанным с кодексом этики.

Неэтичное поведение: • компания должна предупреждать намерения и проявления неэтичного поведения и действий;

• компания не должна принимать участие в преследовании и дискриминации;

• неавторизованное использование торговых и маркетинговых секретов компании, операционной, персональной, финансовой, технической информации и исходного кода компании, обеспечивающих ее конкурентное преимущество, недопустимо;

• компания всегда должна действовать этично, в соответствии с законодательством;

• сотрудникам компании запрещено использовать корпоративные активы и деловые отношения для собственных целей или выгоды.

Ответственность Любые нарушения этого кодекса этики недопустимы, и компания будет действовать быстро для исправления ситуации.

К любому сотруднику, нарушившему эту политику, могут быть применены дисциплинарные меры, вплоть до увольнения.

19. Политика лаборатории антивирусной защиты ***Цель***

Установление требований, которым должны отвечать все компьютеры, подключенные к сети лаборатории компании, для гарантии их защиты от заражения вирусами.

Область действия Эта политика обязательна для всех компьютеров лаборатории компании.

Суть политики Все компьютеры лаборатории должны иметь стандартное, рекомендованное к использованию в компании антивирусное программное обеспечение. Антивирусное программное обеспечение должно иметь самую свежую базу обновлений. Компьютеры, зараженные вирусом, необходимо немедленно удалять из сети до тех пор, пока они не будут вылечены. Менеджеры и администраторы лаборатории ответственны за создание процедур, гарантирующих, что антивирусное программное обеспечение выполняет периодическую проверку компьютеров и имеет самые свежие базы обновлений. Запрещена, в соответствии с политикой допустимого использования, любая деятельность по созданию/распространению вирусов, «червей», почтовых «бомб», программ типа «Троянский конь».

...

Примечание: политика охватывает только компьютеры с операционной системой Windows.

Ответственность

К любому сотруднику, нарушившему эту политику, могут быть применены дисциплинарные меры, вплоть до увольнения.

Приложение 5 ОЦЕНКА ЭКОНОМИЧЕСКОЙ ЭФФЕКТИВНОСТИ ЗАТРАТ НА ЗАЩИТУ ИНФОРМАЦИИ

1. Оценка затрат на защиту информации

Сегодня в отечественных компаниях и на предприятиях с повышенными требованиями в области информационной безопасности (банковские системы, биллинговые системы, ответственные производства и т. д.) затраты на обеспечение режима информационной безопасности составляют до 30 % всех затрат на информационную систему, и владельцы информационных ресурсов со всей серьезностью рассматривают экономические аспекты обеспечения их безопасности. Однако даже там, где уровень информационной безопасности явно недостаточен, у технических специалистов зачастую возникают проблемы обоснования для руководства необходимости затрат на повышение этого уровня. Как определить экономически оправданные затраты на защиту информации? Какие методы существуют и жизнеспособны на практике? Давайте рассмотрим эти вопросы.

Обзор существующих методов Первоначально определимся с целями, которые мы преследуем при выборе метода оценки целесообразности затрат на систему информационной безопасности. Во-первых, метод должен обеспечивать количественную оценку затрат на безопасность, используя качественные показатели оценки вероятностей событий и их последствий. Во-вторых, метод должен быть прозрачен с точки зрения пользователя и давать возможность вводить собственные эмпирические данные. В-третьих, метод должен быть

универсален, то есть одинаково применим к оценке затрат на приобретение аппаратных средств, специализированного и универсального программного обеспечения, затрат на услуги, затрат на перемещение персонала и обучение конечных пользователей и т. д. В-четвертых, выбранный метод должен позволять моделировать ситуацию, при которой существует несколько контрмер, направленных на предотвращение определенной угрозы, в разной степени влияющих на сокращение вероятности происшествия. Какие же методы оценки затрат и ценности инвестиций существуют и что можно использовать на практике?

Прикладной информационный анализ (Applied Information Economics, AIE). Методика AIE была разработана Дугласом Хаббардом, руководителем компании Hubbard Ross. Компания Hubbard Ross, основанная в марте 1999 года, стала первой организацией, которая использовала методику AIE для анализа ценности инвестиций в технологии безопасности с финансовой и экономической точки зрения.

Методика AIE позволяет повысить точность показателя действительной экономической стоимости вложений в технологии безопасности за счет определения доходности инвестиций (Return on Investment, ROI) до и после инвестирования. Применение AIE позволяет сократить неопределенность затрат, рисков и выгод, в том числе и неочевидных. Опираясь на знания экономики, статистики, теории информации и системного анализа, консультанты Hubbard Ross определяют важные финансовые показатели, используя дополнительные сведения для уменьшения их неопределенности, а также оценивают влияние рисков и помогают выбрать стратегию, которая уменьшала бы риск и оптимизировала инвестиционные вложения.

Отчет о проделанной работе включает в себя полученные сведения, рекомендации и комментарии консультантов, также в состав отчета входит сводная таблица (Microsoft Excel), отражающая взаимное влияние затрат, прибыли и рисков.

Потребительский индекс (Customer Index, CI). Метод предлагает оценивать степень влияния инвестиций в технологии безопасности на численность и состав потребителей. В процессе оценки предприятие или организация определяет экономические показатели своих потребителей за счет отслеживания доходов, затрат и прибылей по каждому заказчику в отдельности. Недостаток метода состоит в трудности формализации процесса установления прямой связи между инвестициями в технологии безопасности и сохранением или увеличением числа потребителей. Этот метод применяется в основном для оценки эффективности корпоративных систем защиты информации в компаниях, у которых число заказчиков непосредственно влияет на все аспекты бизнеса.

Добавленная экономическая стоимость (Economic Value Added, EVA). Консалтинговая компания Stern Stewart и Co., основанная в 1982 году, специализируется на оценке акционерного капитала новым инструментарием финансового анализа. Эта компания одна из первых разработала собственную методику вычисления добавленной стоимости, которая предлагает непротиворечивый подход к определению целей и измерению показателей, к оценке стратегий, размещению капитала и пр.

Методика EVA предлагает рассматривать службу информационной безопасности как «государство в государстве», то есть специалисты службы безопасности продают свои услуги внутри компании по расценкам, примерно эквивалентным расценкам на внешнем рынке, что позволяет компании отследить доходы и расходы, связанные с технологиями безопасности. Таким образом, служба безопасности превращается в центр прибыли и появляется возможность четко определить, как расходуются активы, связанные с технологиями безопасности, и увеличиваются доходы акционеров.

Исходная экономическая стоимость (Economic Value Sourced, EVS). Методика EVS была разработана компанией META Group Consulting, которая оказывает услуги средним и крупным компаниям, количественно измеряя возврат от инвестиций в технологии безопасности. Методика предполагает точный расчет всех возможных рисков и выгод для бизнеса, связанных с внедрением и функционированием корпоративной системы защиты информации. При этом расширяется использование таких инструментальных средств оценки ИТ, как добавленная экономическая стоимость (EVA), внутренняя норма рентабельности

(IRR) и возврат от инвестиций (ROI), за счет определения и вовлечения в оценочный процесс параметров времени и риска.

Управление портфелем активов (Portfolio Management, PM). Методика управления портфелем активов предполагает, что компании управляют технологиями безопасности так же, как управляли бы акционерным инвестиционным фондом с учетом объема, размера, срока, прибыльности и риска каждой инвестиции. Портфель активов технологий безопасности состоит из «статичных» и «динамичных» активов. К «статичным» активам относят: аппаратно-программные средства защиты информации, операционные системы и пакеты прикладных программных продуктов, сетевое оборудование и программное обеспечение, данные и информацию, оказываемые услуги, человеческие ресурсы и пр. В состав «динамичных» активов входят следующие компоненты: различные проекты по расширению и обновлению всего портфеля активов, знания и опыт, интеллектуальный капитал и т. д.

Таким образом, управление портфелем активов технологий безопасности представляет собой непрерывный анализ взаимодействия возникающих возможностей и имеющихся в наличии ресурсов. Непрерывность процесса управления связана с внешними изменениями (например, изменение ситуации на рынке, изменение позиций конкурента) и с внутренними изменениями (например, изменения в стратегии компании, в каналах сбыта, номенклатуре товаров и услуг и т. д.). А директор службы безопасности становится «фондовым менеджером», который управляет инвестициями в технологии безопасности, стремясь к максимизации прибыли.

Оценка действительных возможностей (Real Option Valuation, ROV). Основу методики составляет ключевая концепция построения модели «гибких возможностей компании» в будущем. Методика рассматривает технологии безопасности в качестве набора возможностей с большой степенью их детализации. Правильное решение принимается после тщательного анализа широкого спектра показателей и рассмотрения множества результатов или вариантов будущих сценариев, в терминах методики именующихся «динамическим планом выпуска/гибкости» управляющих решений, который поможет организациям лучше адаптировать или изменять свой курс в области информационной безопасности.

Метод жизненного цикла искусственных систем (System Life Cycle Analysis, SLCA). В основе российского метода SLCA лежит измерение «идеальности» корпоративной системы защиты информации – соотношение ее полезных факторов и суммы вредных факторов и факторов расплаты за выполнение полезных функций. Оценку предваряет совместная работа аналитика и ведущих специалистов обследуемой компании по выработке реестра полезных, негативных и затратных факторов бизнес-системы без использования системы безопасности и по присвоению им определенных весовых коэффициентов. Результатом работы является расчетная модель, описывающая состояние без системы безопасности. После этого в модель вводятся описанные факторы ожидаемых изменений и производится расчет уровня развития компании с корпоративной системой защиты информации. Таким образом, строятся традиционные модели «как есть» и «как будет» с учетом реестра полезных, негативных и затратных факторов бизнес-системы.

Метод SLCA применяется:

• на этапе предпроектной подготовки, для предварительной оценки эффекта от внедрения новой системы безопасности или от модернизации существующей;

• на этапе разработки технического задания на ИС в защищенном исполнении;

• на этапе проведения аудита информационной безопасности ИС предприятия, для проектной оценки ожидаемого эффекта;

• на этапе приемки ИС в защищенном исполнении в эксплуатацию или по окончании периода опытной эксплуатации для подтверждения расчетного эффекта, его уточнения и получения новой «точки отсчета» (нового уровня организационно-технологического развития компании) для последующих оценок эффекта от внедрения технологий безопасности.

Система сбалансированных показателей (Balanced Scorecard, BSC). Система сбалансированных показателей (ССП) – это методика, в рамках которой традиционные показатели финансовых отчетов объединяются с операционными параметрами, что создает достаточно общую схему, позволяющую оценить нематериальные активы: уровень корпоративных инноваций, степень удовлетворенности сотрудников, эффективность приложений и т. д. Концепция системы сбалансированных показателей впервые была представлена в 1990 году Дэвидом Нортоном, на сегодняшний день руководителем Balanced Scorecard Collaborative, и Робертом Капланом, профессором Harvard Business School. Традиционная концепция ССП предполагает формирование так называемых стратегических карт, группирующих цели и показатели по четырем категориям (перспективам):

- *финансы* – финансовые цели развития и результаты работы компании (прибыль, рентабельность и т. д.);
- *клиенты и рынки* – цели присутствия на рынке и показатели качества обслуживания клиентов (освоение рынков и территорий продаж, время выполнения заказа и т. д.);
- *процессы* – требования к эффективности процессов (стоимость, время, количество ошибок, риски и т. д.);
- *развитие* – цели поиска новых технологий и повышения квалификации персонала и т. д.

Между всеми показателями существуют причинно-следственные связи. Например, чем выше квалификация персонала и лучше технология ведения бизнеса, тем проще поддерживать бизнес-процессы, что, в свою очередь, способствует более качественному обслуживанию клиентов и реализации конкурентных преимуществ, а следовательно, помогает достичь запланированных финансовых показателей. Таким образом, для компании в целом финансовые показатели – это конечная цель функционирования, тогда как прочие перспективы определяют будущий потенциал компании. Подобным образом можно определить ключевые показатели функционирования службы информационной безопасности компании и задать перспективы развития корпоративных систем защиты информации. При этом следует помнить, что, поскольку технологии безопасности оказывают косвенное воздействие на финансовые показатели компании, их надо рассматривать с точки зрения вклада в развитие бизнеса. На уровне клиентской перспективы оценка технологий безопасности отражает эффективность взаимодействия соответствующего подразделения с основным бизнесом компании. Стратегия развития технологий безопасности на базе методов ССП формулируется в виде взаимосвязанного набора целей и показателей, сгруппированных по следующим перспективам:

- *миссия* – основное предназначение и пути развития ИТ в компании;
- *клиенты* – цели поддержки основной деятельности компании;
- *процессы* – показатели эффективности процедур разработки и внедрения;
- *технологии* – оценка обоснованности и эффективности используемых технологий;
- *организация* – показатели эффективности внутренних процедур ИТ-подразделения.

Эти перспективы могут быть ориентиром при разработке стратегических карт, но в соответствии с ситуацией и видением руководства состав перспектив может меняться. Обязательным условием вносимых изменений является сохранение логики взаимного влияния перспектив друг на друга. Как показывает практика, при освоении идеи ССП формирование стратегических карт не представляет особых затруднений. Но, несмотря на кажущуюся простоту, менеджеры часто допускают ошибки при использовании методологии. Первая типичная ошибка заключается в создании большого набора метрик, отражающих отдельные аспекты деятельности службы безопасности, но никак не связанных друг с другом или со стратегией развития компании в целом. Вторая ошибка – формирование стратегических карт, содержащих большое число причинно-следственных взаимосвязей между целями и показателями. Оба эти варианта приводят к невозможности расстановки приоритетов в развитии корпоративной системы защиты информации, хотя именно методология системы сбалансированных показателей позволяет обеспечить четкое

соответствие стратегии развития ИТ целям компании на формальном уровне. Пример соответствия стандартных перспектив ССП набору стратегических целей службы безопасности приведен в табл. П5.1. Таблица П5.1. Перспективы и цели при планировании технологий безопасности

Перспектива ССП	Стратегические цели в безопасности
Финансы	Понимание места расходов на технологии безопасности в общей структуре бизнеса Способность контролировать затраты на безопасность Сокращение затрат на защиту информации Обеспечение возврата инвестиций в безопасность Составление контрактов на внутренние сервисы безопасности
Клиенты	Обеспечение доступности сервисов безопасности Измерение производительности сервисов безопасности Установление стоимостных характеристик для определенного количества и качества сервисов безопасности Обеспечение надежности АС в защищенном исполнении Поддержка обращений пользователей
Внутренние процессы	Сервисно-ориентированная культура предоставления сервисов безопасности Квалифицированный персонал Эффективность предоставления сервисов безопасности Время предоставления сервисов безопасности Производительность инфраструктуры предоставления сервисов безопасности Возможность учета количества предоставленных сервисов безопасности
Обучение и развитие	Обеспечение гибкости системы безопасности Возможность контролировать изменения в системе безопасности Обеспечение адаптации системы безопасности к изменяющимся требованиям бизнеса формирование и передача основанных на опыте корпоративных знаний в области предоставления сервисов безопасности Способность использовать новые технологии безопасности

Как и любой инструмент стратегического планирования, система сбалансированных показателей имеет возможности и ограничения в практическом применении. Использование ССП позволяет: • устранить разрыв между разработкой стратегии безопасности и ее реализацией;

• оперативно реагировать на изменения окружающей среды;

• оценить существующую стратегию безопасности.

Однако применение методики ССП не предполагает создания стратегии развития предприятия и не требует отказа от традиционных инструментов планирования и контроля.

Совокупная стоимость владения (Total Cost of Ownership, TCO). Методика TCO первоначально разрабатывалась как средство расчета стоимости владения компьютером. Но в последнее время, благодаря усилиям компании Gartner Group, эта методика стала основным инструментом подсчета совокупной стоимости владения корпоративных систем защиты информации. Основной целью расчета TCO является выявление избыточных статей расходов и оценка возможности возврата инвестиций, вложенных в технологии безопасности. Таким образом, полученные данные по совокупной стоимости владения используются для выявления расходной части использования корпоративной системы защиты информации.

Главной проблемой при определении TCO является проблема выявления составляющих совокупной стоимости владения и их количественная оценка. Все составляющие TCO условное разделяются на «видимые» пользователю (первоначальные затраты) и «невидимые» (затраты эксплуатации и использования). При этом «видимая» часть TCO составляет 32 %, а по некоторым оценкам и 21 %, а «невидимая» – 68 % или, соответственно, 79 %.

К группе «видимых» затрат относятся следующие:

• стоимость лицензии,

• стоимость внедрения,

• стоимость обновления,

• стоимость сопровождения.

Все эти затраты, за исключением внедрения, имеют фиксированную стоимость и могут быть определены еще до принятия решения о внедрении корпоративной системы защиты информации. Следует отметить, что и в «видимом» секторе поставщиками систем безопасности иногда могут использоваться скрытые механизмы увеличения стоимости для

привлечения клиента. Дополнительные затраты («невидимые») появляются у каждого предприятия, завершившего у себя внедрение корпоративной системы защиты информации. «Невидимые» затраты также разделяются на группы:

- *затраты на оборудование* – сюда включаются затраты на приобретение или обновление средств защиты информации, на организацию бесперебойного питания и резервного копирования информации, на установку новых устройств безопасности и пр.;
- *дополнительное программное обеспечение* – системы управления безопасностью, VPN, межсетевые экраны, антивирусы и пр.;
- *персонал* – например, ошибки и трудности в работе со средствами защиты, неприятие или даже саботаж новых средств защиты и т. д.;
- *стоимость возможностей* – стоимость возможных альтернатив. Рассматриваются следующие варианты: приобретение или обновление корпоративной системы защиты информации, сделать ли это собственными силами или заказать сторонней организации;
- *другие* – в этом случае оценивается степень и стоимость риска «выхода из строя» системы.

Показатель TCO корпоративной системы информационной безопасности рассчитывается как сумма всех затрат, «видимых» и «невидимых». Затем этот показатель сравнивается с рекомендуемыми величинами для данного типа предприятия. Существует 17 типов предприятий, которые в свою очередь делятся на малые, средние и крупные. Если полученная совокупная стоимость владения системы безопасности значительно превышает рекомендованное значение и приближается к предельному, то необходимо принять меры по снижению TCO. Сокращения совокупной стоимости владения можно достичь следующими способами: максимальной централизацией управления безопасностью, уменьшением числа специализированных элементов, настройкой прикладного программного обеспечения безопасности и пр.

Функционально-стоимостной анализ (Activity Based Costing, ABC). ABC – это процесс распределения затрат с использованием первичных носителей стоимости, ориентированных на производственную и/или логистическую структуру предприятия с конечным распределением затрат по основным носителям (продуктам и услугам). Данный подход позволяет весьма точно и понятно установить связь между элементами себестоимости продукции и производственными процессами.

При оценке эффективности корпоративных систем защиты информации метод ABC используется для построения моделей бизнес-процессов предприятия «как есть» и «как будет». Модель «как будет» отражает изменение технологии реализации основных бизнес-процессов при использовании выбранной корпоративной системы информационной безопасности. На основе показателей стоимости, трудоемкости и производительности определяется наилучшая модель бизнес-процессов «как будет».

Таким образом, метод ABC является альтернативой традиционным финансовым подходам и позволяет:

- предоставить информацию в форме, понятной для персонала предприятия, непосредственно участвующего в бизнес-процессе;
- распределить накладные расходы в соответствии с детальным просчетом использования ресурсов, подробным представлением о процессах и функциях их составляющих, а также влиянием на себестоимость.

Следует отметить, что развитием метода ABC стал метод функционально-стоимостного управления – ФСУ (Activity Based Management, ABM). Совместно методы ABC и ABM используются для реорганизации бизнес-процессов с целью повышения производительности, снижения стоимости и улучшения качества.

Основные положения методики Total Cost of Ownership Анализ методов оценки эффективности инвестиций в корпоративные системы информационной безопасности показывает, что только метод совокупной стоимости владения (TCO) позволяет рассчитать расходную часть на систему безопасности. Поэтому давайте рассмотрим методику TCO

более подробно.

Информационная безопасность обеспечивается комплексом мер на всех этапах жизненного цикла информационной системы, совокупная стоимость владения (показатель TCO) для системы информационной безопасности в общем случае складывается из стоимости:

• проектных работ;

• закупки и настройки программно-технических средств защиты, включающих следующие основные группы: межсетевые экраны, средства криптографии, антивирусы и средства аутентификации, авторизации и администрирования (AAA);

• затрат на обеспечение физической безопасности;

• обучения персонала;

• управления и поддержки системы (администрирование безопасности);

• аудита информационной безопасности;

• периодической модернизации системы информационной безопасности.

Таким образом, методика совокупной стоимости владения компании Gartner Group позволяет:

• получить адекватную информацию об уровне защищенности распределенной вычислительной среды и совокупной стоимости владения корпоративной системы защиты информации;

• сравнить подразделения службы информационной безопасности компании как между собой, так и с аналогичными подразделениями других предприятий в данной отрасли;

• оптимизировать инвестиции в информационную безопасность компании с учетом реального значения показателя TCO.

Здесь под показателем TCO понимается сумма прямых и косвенных затрат на организацию (реорганизацию), эксплуатацию и сопровождение корпоративной системы защиты информации в течение года. TCO может рассматриваться как ключевой количественный показатель эффективности организации информационной безопасности в компании, так как позволяет не только оценить совокупные затраты на нее, но и управлять этими затратами для достижения требуемого уровня защищенности КИС. При этом прямые затраты включают как капитальные компоненты затрат (ассоциируемые с фиксированными активами или «собственностью»), так и трудозатраты, которые учитываются в категориях операций и административного управления. Сюда же относят затраты на услуги удаленных пользователей, аутсорсинг и др., связанные с поддержкой деятельности организации.

В свою очередь косвенные затраты отражают влияние КИС и подсистемы защиты информации на деятельность сотрудников компании посредством таких измеримых показателей, как простои и «зависания» корпоративной системы защиты информации и КИС в целом, затраты на операции и поддержку (не относящиеся к прямым затратам). Очень часто косвенные затраты играют значительную роль, так как они обычно изначально не отражаются в бюджете на информационную безопасность, а выявляются при анализе затрат впоследствии, что в конечном счете приводит к росту «скрытых» затрат компании на систему информационной безопасности.

Существенно, что TCO не только отражает «стоимость владения» отдельных элементов корпоративной системы защиты информации и их взаимодействия в течение всего жизненного цикла системы: «овладение методикой» TCO помогает службе информационной безопасности лучше измерять, управлять и снижать затраты и/или улучшать уровни сервиса защиты информации с целью адекватности мер защиты бизнесу компании.

Подход к оценке TCO базируется на результатах аудита структуры и поведения корпоративной системы защиты информации и КИС в целом, включая действия сотрудников служб автоматизации, информационной безопасности и просто пользователей КИС. Сбор и анализ статистики по структуре прямых (HW/SW, операции, административное управление) и косвенных затрат (на конечных пользователей и простои) проводится, как правило, в течение 12 месяцев. Полученные данные оцениваются по ряду критериев с учетом сравнения

с данными по аналогичным компаниям в отрасли.

Методика TCO позволяет оценить и сравнить состояние защищенности КИС компании с типовым профилем защиты, в том числе показать узкие места в организации защиты, на которые следует обратить внимание. Иными словами, на основе полученных данных можно сформировать понятную с экономической точки зрения стратегию и тактику развития корпоративной системы защиты информации, а именно: «сейчас мы тратим на информационную безопасность столько-то, если будем тратить столько-то по конкретным направлениям информационной безопасности, то получим такой-то эффект».

Известно, что в методике TCO в качестве базы для сравнения используются данные и показатели TCO для западных компаний. Однако данная методика способна учитывать специфику российских компаний с помощью так называемых поправочных коэффициентов, например:

• по стоимости основных компонентов корпоративной системы защиты информации и КИС, информационных активов компании (Cost Profiles) с учетом данных по количеству и типам серверов, персональных компьютеров, периферии и сетевого оборудования;

• по заработной плате сотрудников (Salary and Asset Scalars) с учетом дохода компании, географического положения, типа производства и размещения организации в крупном городе или нет;

• по конечным пользователям ИТ (End User Scalars) с учетом типов пользователей и их размещения (для каждого типа пользователей требуется различная организация службы поддержки и вычислительной инфраструктуры);

• по использованию методов так называемой лучшей практики в области управления информационной безопасностью (best practices) с учетом реального состояния дел по управлению изменениями, операциями, активами, сервисному обслуживанию, обучению, планированию и управлению процессами;

• по уровню сложности организации (Complexity Level) с учетом состояния организации конечных пользователей (процент влияния – 40 %), технологии SW (40 %), технологии HW (20 %).

Определение затрат компании на информационную безопасность подразумевает решение следующих трех задач:

• оценка текущего уровня TCO корпоративной системы защиты информации и КИС в целом;

• аудит информационной безопасности компании на основе сравнения уровня защищенности компании и рекомендуемого (лучшая мировая практика) уровня TCO;

• формирование целевой модели TCO.

Рассмотрим каждую из перечисленных задач. *Оценка текущего уровня TCO.* В ходе работ по оценке TCO проводится сбор информации и расчет показателей TCO организации по следующим направлениям:

• существующие компоненты ИС (включая систему защиты информации) и информационные активы компании (серверы, клиентские компьютеры, периферийные устройства, сетевые устройства);

• существующие расходы на аппаратные и программные средства защиты информации (расходные материалы, амортизация);

• существующие расходы на организацию информационной безопасности в компании (обслуживание СЗИ и СКЗИ, а также штатных средств защиты периферийных устройств, серверов, сетевых устройств, планирование и управление процессами защиты информации, разработку концепции и политики безопасности и пр.);

• существующие расходы на организационные меры защиты информации;

• существующие косвенные расходы на организацию информационной безопасности в компании, и в частности обеспечение непрерывности или устойчивости бизнеса компании.

Аудит информационной безопасности компании. По результатам собеседования с TOP-менеджерами компании и проведения инструментальных проверок уровня

защищенности организации проводится анализ следующих основных аспектов: • политики безопасности,

• организации защиты,
• классификации и управления информационными ресурсами,
• управления персоналом,
• физической безопасности,
• администрирования компьютерных систем и сетей,
• управления доступом к системам,
• разработки и сопровождения систем,
• планирования бесперебойной работы организации,
• проверки системы на соответствие требованиям информационной безопасности.

На основе проведенного анализа выбирается модель ТСО, сравнимая со средними и оптимальными значениями для репрезентативной группы аналогичных организаций, имеющих схожие с рассматриваемой организацией показатели по объему бизнеса. Такая группа выбирается из банка данных по эффективности затрат на информационную безопасность и эффективности соответствующих профилей защиты аналогичных компаний. Сравнение текущего показателя ТСО проверяемой компании с модельным значением показателя ТСО позволяет провести анализ эффективности организации информационной безопасности компании, в результате выявить «узкие» места в организации и причины их появления и выработать дальнейшие шаги по реорганизации корпоративной системы защиты информации и обеспечению требуемого уровня защищенности КИС.

Формирование целевой модели ТСО. По результатам проведенного аудита моделируется целевая (желаемая) модель, учитывающая перспективы развития бизнеса и корпоративной системы защиты информации (активы, сложность, методы лучшей практики, типы СЗИ и СКЗИ, квалификация сотрудников компании и т. п.).

Кроме того, рассматриваются капитальные расходы и трудозатраты, необходимые для проведения преобразований текущей среды в целевую среду. В трудозатраты на внедрение включаются затраты на планирование, развертывание, обучение и разработку. Сюда же входят возможные временные увеличения затрат на управление и поддержку.

Для обоснования эффекта от внедрения новой корпоративной системы защиты информации (ROSI) могут быть использованы модельные характеристики снижения совокупных затрат (ТСО), отражающие возможные изменения в корпоративной системе защиты информации.

Виды затрат на систему информационной безопасности Затраты на информационную безопасность подразделяются на следующие категории:

1. Затраты на формирование и поддержание звена управления системой защиты информации (организационные затраты):

• затраты на приобретение и ввод в эксплуатацию программно-технических средств: серверов, компьютеров конечных пользователей (настольных и мобильных), периферийных устройств и сетевых компонентов;
• затраты на приобретение и настройку средств защиты информации;
• затраты на содержание персонала, стоимость работ и аутсорсинг;
• затраты на формирование политики безопасности предприятия.

2. Затраты на контроль (определение и подтверждение достигнутого уровня защищенности ресурсов предприятия): • затраты на контроль:

– плановые проверки и испытания;
– затраты на проверки и испытания программно-технических средств защиты информации;
– затраты на проверку навыков эксплуатации средств защиты персоналом предприятия;
– затраты на обеспечение работы лиц, ответственных за реализацию конкретных процедур безопасности по подразделениям;
– оплата работ по контролю правильности ввода данных в прикладные системы;

– оплата инспекторов по контролю требований, предъявляемых к защитным средствам при разработке любых систем (контроль выполняется на стадии проектирования и спецификации требований);

• внеплановые проверки и испытания:

– оплата работы испытательного персонала специализированных организаций;

– обеспечение испытательного персонала (внутреннего и внешнего) материально-техническими средствами;

• контроль за соблюдением политики информационной безопасности:

– затраты на контроль реализации функций, обеспечивающих управление защитой коммерческой тайны;

– затраты на организацию временного взаимодействия и координации между подразделениями для решения конкретных повседневных задач;

– затраты на проведение аудита безопасности по каждой автоматизированной информационной системе, выделенной в информационной среде предприятия;

– материально-техническое обеспечение системы контроля доступа к объектам и ресурсам предприятия;

• затраты на внешний аудит:

– затраты на контрольно-проверочные мероприятия, связанные с лицензионно-разрешительной деятельностью в сфере защиты информации.

3. Внутренние затраты на ликвидацию последствий нарушений политики информационной безопасности (затраты, понесенные организацией в результате того, что требуемый уровень защищенности не был достигнут): • пересмотр политики информационной безопасности предприятия (проводится периодически):

– затраты на идентификацию угроз безопасности;

– затраты на поиск уязвимостей системы защиты информации;

– оплата работы специалистов, выполняющих работы по определению возможного ущерба и переоценке степени риска;

• затраты на ликвидацию последствий нарушения режима информационной безопасности:

– восстановление системы безопасности до соответствия требованиям политики безопасности;

– установка патчей или приобретение последних версий программных средств защиты информации;

– приобретение технических средств взамен пришедших в негодность;

– проведение дополнительных испытаний и проверок технологических информационных систем;

– затраты на утилизацию скомпрометированных ресурсов;

• восстановление информационных ресурсов предприятия:

– затраты на восстановление баз данных и прочих информационных массивов;

– затраты на проведение мероприятий по контролю достоверности данных, подвергшихся атаке на целостность;

• затраты на выявление причин нарушения политики безопасности:

– затраты на проведение расследований нарушений политики безопасности (сбор данных о способах совершения, механизме и способах сокрытия неправомерного деяния, поиск следов, орудий, предметов посягательства, выявление мотивов неправомерных действий и т. д.);

– затраты на обновление планов обеспечения непрерывности деятельности службы безопасности;

• затраты на переделки:

– затраты на внедрение дополнительных средств защиты, требующих существенной перестройки системы безопасности;

– затраты на повторные проверки и испытания системы защиты информации.

4. Внешние затраты на ликвидацию последствий нарушения политики информационной безопасности: • внешние затраты на ликвидацию последствий нарушения политики безопасности:

– обязательства перед государством и партнерами;

– затраты на юридические споры и выплаты компенсаций;

– потери в результате разрыва деловых отношений с партнерами;

• потеря новаторства:

– затраты на проведение дополнительных исследований и разработки новой рыночной стратегии;

– отказ от организационных, научно-технических или коммерческих решений, ставших неэффективными в результате утечки сведений, и затраты на разработку новых средств ведения конкурентной борьбы;

– потери от снижения приоритета в научных исследованиях и невозможности патентования и продажи лицензий на научно-технические достижения;

• прочие затраты:

– заработная плата секретарей и служащих, организационные и прочие расходы, которые непосредственно связаны с предупредительными мероприятиями;

– другие виды возможного ущерба предприятию, в том числе связанные с невозможностью выполнения функциональных задач, определенных его уставом.

5. Затраты на техническое обслуживание системы защиты информации и мероприятия по предотвращению нарушений политики безопасности предприятия (предупредительные мероприятия): • затраты на управление системой защиты информации:

– затраты на планирование системы защиты информации предприятия;

– затраты на изучение возможностей информационной инфраструктуры предприятия по обеспечению безопасности информации ограниченного распространения;

– затраты на осуществление технической поддержки производственного персонала при внедрении средств защиты и процедур, а также планов по защите информации;

– проверка сотрудников на лояльность, выявление угроз безопасности;

– организация системы допуска исполнителей и сотрудников конфиденциального делопроизводства с соответствующими штатами и оргтехникой;

• регламентное обслуживание средств защиты информации:

– затраты, связанные с обслуживанием и настройкой программно-технических средств защиты, операционных систем и используемого сетевого оборудования;

– затраты, связанные с организацией сетевого взаимодействия и безопасного использования информационных систем;

– затраты на поддержание системы резервного копирования и ведения архива данных;

– проведение инженерно-технических работ по установлению сигнализации, оборудованию хранилищ конфиденциальных документов, защите телефонных линий связи, вычислительной техники и т. п.;

• аудит системы безопасности:

– затраты на контроль изменений состояния информационной среды предприятия;

– затраты на систему контроля за действиями исполнителей;

• обеспечение должного качества информационных технологий:

– затраты на обеспечение соответствия требованиям качества информационных технологий, в том числе анализ возможных негативных аспектов информационных технологий, которые влияют на целостность и доступность информации;

– затраты на доставку (обмен) конфиденциальной информации;

– удовлетворение субъективных требований пользователей: стиль, удобство интерфейса и др.;

• обеспечение требований стандартов:

– затраты на обеспечение соответствия принятым стандартам и требованиям,

достоверности информации, действенности средств защиты;

• обучение персонала:

– повышение квалификации сотрудников предприятия в вопросах использования имеющихся средств защиты, выявления и предотвращения угроз безопасности;

– развитие нормативной базы службы безопасности.

Пример использования методики Total Cost of Ownership Допустим, что объектом исследования является страховая компания ЗАО «Страхование». Название компании вымышленное, возможные совпадения случайны и носят непреднамеренный характер.

Для определения затрат на систему информационной безопасности по методике совокупной стоимости владения воспользуемся программным продуктом TCO Manager компании Gartner Group. Технология работы с ПП TCO Manager заключается в следующем: пользователь вводит первоначальные данные об объекте (профайл компании, данные о конечных пользователях, об информационных активах предприятия), исходя из них определяется текущий показатель TCO и вычисляются ежегодные затраты на поддержание существующего уровня безопасности. Также TCO Manager позволяет оптимизировать показатель TCO, сравнив текущий показатель TCO компании с «лучшим» в отрасли и смоделировав целевой показатель TCO для данного предприятия.

Теперь обратимся к исходным данным по ЗАО «Страхование» и вычислим текущий показатель TCO.

Название компании – ЗАО «Страхование».

Период анализа – январь-декабрь 2004 года.

Основной вид деятельности – страхование.

Общий годовой доход – 450 млн. руб.

Количество рабочих часов в год – 1880 час/год.

Средняя годовая зарплата конечных пользователей – 38 тыс. руб.

Средний процент, отчисляемый на налоги, медицинское страхование, страхование от несчастных случаев и т. д. персонала службы безопасности (ЕСН) – 37 %.

Средний процент, отчисляемый на налоги, медицинское страхование, страхование от несчастных случаев и т. д. конечных пользователей (ЕСН) – 37 %.

Количество конечных пользователей – 2 869 чел.

Классификация конечных пользователей представлена в табл. П5.2-П5.3.

Таблица П5.2. Классификация конечных пользователей по типам

Тип конечных пользователей	Доля, %	Количество, чел.
Руководящий персонал	1	29
Научные работники	20	574
Исполнительный персонал	75	2 152
Операторы	4	115
Общее количество	100	2869

Таблица П5.3. Классификация конечных пользователей по местоположению

Тип местоположения	Доля, %	Количество, чел.
Desktop	85	2 439
Mobile	10	287
Telecommuters	5	143
Общее количество	100	2 869

Таблица П5.4. Сравнение текущего и целевого уровней системы защиты

Критерии	Текущий уровень	Целевой уровень
Усовершенствование технологии управления активами		
Автоматизированное управление активами	Базовый	Высокий
Учет программного обеспечения	Базовый	Высокий
Учет аппаратных средств	Базовый	Высокий
Усовершенствование технологии управления системы		
Системы обнаружения вирусов и защиты	Базовый	Высокий
Системное управление	Базовый	Средний
Стандартизация процессов модернизации		
Стандартизация процессов модернизации		
Стандартизация поставщиков	Базовый	Средний
Стандартизация платформы	Средний	Высокий
Совершенствование управления персоналом		
Обучение пользователей	Базовый	Высокий
Обучение ИТ-специалистов	Базовый	Средний
Мотивация ИТ-персонала	Базовый	Средний
Организация устойчивой ИТ-службы	Базовый	Средний

Форма ввода данных «Интервью» в TCO Manager содержит сведения об информационных активах предприятия (аппаратные средства и программное обеспечение), информацию о конечных пользователях, и на основании этих данных мы получаем следующие отчеты (см. табл. П5.5-П5.7). Также TCO Manager, используя практический подход к определению совокупной стоимости владения, позволяет сравнивать текущие затраты с эталонными («лучшими в группе») и строить целевые показатели затрат (см. табл. П5.5-П5.15). В частности, в табл. П5.6-П5.15. приведена детализация и расшифровка укрупненных прямых и косвенных затрат, которые отображены в табл. П5.5.

Таблица П5.5. Анализ затрат по показателям TCO

Категории затрат	Текущие, руб.	Эталонные, руб.	Целевые, руб.	Разница между эталонными и текущими, руб.	Разница в %	Разница между целевыми и эталонными, руб.	Разница в %	Разница между целевыми и текущими, руб.	Разница в %
Прямые затраты									
Затраты на программное обеспечение и оборудование	5 601 557	4 931 610	5 400 695	-669 947	-12 %	469 085	10 %	200 862	-4 %
Операционные затраты (управление)	4 831 911	4 711 401	2 695 527	-120 511	-2 %	-2 015 873	-43 %	-2 136 384	-44 %

Окончание табл. П5.5

Категории затрат	Текущие, руб.	Эталонные, руб.	Целевые, руб.	Разница между эталонными и текущими, руб.	Разница в %	Разница между целевыми и эталонными, руб.	Разница в %	Разница между целевыми и текущими, руб.	Разница в %
Административные затраты (поддержка)	1 477 957	994 636	1 272 225	-483 321	-33 %	277589	28 %	-205732	-14 %
Общие прямые	***11 911 426***	***10 637 647***	***9 368 447***	***-1 273 779***	***-11 %***	***-1 269 199***	***-12 %***	***-2 542 978***	***-21 %***
Косвенные затраты									
Поддержка конечных пользователей	11 853 266	20 458 366	9 005 139	8 605 100	73 %	-1 1453 227	-56 %	-2 848 127	-24 %
Простой	2 619 053	636 117	149 1347	-1 982 936	-76 %	855 230	134 %	-1 127 705	-43 %
Общие косвенные	***14 472 318***	***21 094 483***	***10 496 486***	***6 622 165***	***46 %***	***-10 597 997***	***-50 %***	***-3 975 832***	***-27 %***
Ежегодный TCO	26 383 744	31 732 130	19 864 933	5 348 386	20 %	-11 867 196	-37 %	-6 518 811	-25 %
Процент TCO от дохода	59	71	44	12	203 %	-26	-374 %	-14	-247 %
Процент прямых затрат от дохода	26	24	21	-03	-107 %	-03	-119 %	-06	-213 %

Таблица П5.6. Детализация затрат на программное обеспечение и оборудование по

Категории затрат на программное обеспечение и оборудование	Текущие, руб.	Эталонные, руб.	Целевые, руб.	Разница между эталонными и текущими, руб.	Разница в %	Разница между целевыми и эталонными, руб.	Разница в %	Разница между целевыми и текущими, руб.	Разница в %
Оборудование	2 451 546	2 617 140	2 836 522	165 594	7 %	219 382	8 %	384 976	16 %
Программное обеспечение	2 873 154	2 040 780	2 262 723	-832 374	-29 %	221 943	11 %	-610 431	-21 %
Оборудование ИС	79 617	78 690	89 665	-927	-1 %	10 975	14 %	10 048	13 %
Программное обеспечение ИС	197 240	195 000	211 786	-2 240	-1 %	16 786	9 %	14 546	7 %
Общие затраты	**5 601 557**	**4 931 610**	**5 400 695**	**-669 947**	**-12 %**	**469 085**	**10 %**	**-200 862**	**-4 %**

категориям

Таблица П5.7. Расшифровка затрат на аппаратные средства

Категории затрат на аппаратные средства	Текущие, руб.	Эталонные, руб.	Целевые, руб.	Разница между эталонными и текущими, руб.	Разница в %	Разница между целевыми и эталонными, руб.	Разница в %	Разница между целевыми и текущими, руб.	Разница в %
Покупка оборудования	1 909 668	1 894 950	2 109 357	-14 718	-1 %	214 407	11 %	199 689	10 %
Лизинговые платежи	307 521	260 480	395 994	-47 041	-15 %	135 514	52 %	88 473	29 %
Модернизация	67 972	258 340	57 254	190 368	280 %	-201 086	-78 %	-10 717	-16 %
Комплектующие	81 855	36 640	165 148	-45 215	-55 %	128 508	351 %	83 292	102 %
Лицензии	84 530	166 730	108 769	82 200	97 %	-57 961	-35 %	24 238	29 %
Общие затраты	**2 451 546**	**2 617 140**	**2 836 522**	**165 594**	**7 %**	**219 382**	**8 %**	**384 976**	**16 %**

Таблица П5.8. Расшифровка затрат на программное обеспечение

Категории затрат на программное обеспечение	Текущие, руб.	Эталонные, руб.	Целевые, руб.	Разница между эталонными и текущими, руб.	Разница в %	Разница между целевыми и эталонными, руб.	Разница в %	Разница между целевыми и текущими, руб.	Разница в %
Затраты на собственную разработку программных продуктов и баз данных	502 767	352 500	427 128	-150 267	-30 %	74 628	21 %	-75 639	-15 %
Затраты на бизнес приложения и инженерное программное обеспечение	1 179 383	1 393 000	1 002 000	213 617	18 %	-391 000	-28 %	-177 382	-15 %
Затраты на средства и инструменты разработки	410 817	57 480	357 167	-353 337	-89 %	299 687	521 %	-53 650	-13 %
Затраты на формирование системы внутренних коммуникаций	163 804	49 400	142 425	-114 404	-70 %	93 025	188 %	-21 379	-13 %
Другие	616 384	188 400	334 003	-427 984	-69 %	145 603	77 %	-282 381	-46 %
Общие затраты	**2 873 154**	**2 040 780**	**2 262 723**	**-832 374**	**-29 %**	**221 943**	**11 %**	**-610 431**	**-21 %**

Таблица П5.9. Детализация операционных затрат

Операционные затраты	Текущие, руб.	Эталонные, руб.	Целевые, руб.	Разница между эталонными и текущими, руб.	Разница в %	Разница между целевыми и эталонными, руб.	Разница в %	Разница между целевыми и текущими, руб.	Разница в %
Обслуживание клиентских мест и периферийных устройств	1 563 387	2 473 600	836 474	910 213	58 %	-1 637 126	-66 %	-726 913	-46 %
Обслуживание серверов	559 468	427 961	336 049	-131 507	-24 %	-91 912	-21 %	-223 419	-40 %
Обслуживание сети	223 624	253 680	171 567	30 056	13 %	-82 113	-32 %	-52 056	-23 %
Планирование и управление процессами	460 701	0	329 119	-460 701	-100 %	329 119	Undefined	-131 582	-29 %
Обслуживание и администрирование баз данных	241 331	0	230 757	-241 331	-100 %	230 757	Undefined	-10 574	-4 %
Затраты на сервисную поддержку	1 783 400	1 556 160	791 561	-227 240	-13 %	-764 599	-49 %	-991 839	-56 %
Общие ежегодные затраты	**4 831 911**	**4 711 401**	**2 695 527**	**-120 511**	**-2 %**	**-2 015 873**	**-43 %**	**-2 136 384**	**-44 %**

Таблица П5.10. Расшифровка затрат на обслуживание клиентских мест и периферийных устройств

Затраты на обслуживание клиентских мест и периферийных устройств	Текущие, руб.	Эталонные, руб.	Целевые, руб.	Разница между эталонными и текущими, руб.	Разница в %	Разница между целевыми и эталонными, руб.	Разница в %	Разница между целевыми и текущими, руб.	Разница в %
Решение проблем 2-го уровня	247 995	494 720	121 749	246 725	99 %	-372 971	-75 %	-126 246	-51 %
Решение проблем 3-го уровня	86 580	296 832	32 519	210 252	243 %	-264 313	-89 %	-54 061	-62 %
Планирование и управление трафиком	32 449	123 680	30 753	91 231	281 %	-92 927	-75 %	-1 696	-5 %
Точная настройка	24 337	74 208	22 871	49 871	205 %	-51 337	-69 %	-1 466	-6 %
Администрирование конечных пользователей	62 903	296 832	33 507	233 929	372 %	-263 325	-89 %	-29 396	-47 %
Поддержка операционной системы	50 821	74 208	23 106	23 387	46 %	-51 102	-69 %	-27 715	-55 %
Обслуживание рабочей силы	105 663	123 680	72 396	18 017	17 %	-51 284	-41 %	-33 267	-31 %
Установка программного обеспечения	387 563	321 568	268 821	-65 995	-17 %	-52 747	-16 %	-118 742	-31 %
Управление приложениями	225 460	74 208	74 208	-151 252	-67 %	18 037	24 %	-133 215	-59 %
Конфигурация аппаратных средств	49 525	197 888	24 539	148 363	300 %	-173 349	-88 %	-24 985	-50 %
Установка аппаратных средств	120 721	123 680	41 130	2 959	2 %	-82 550	-67 %	-79 591	-66 %
Управление дисками и файлами	29 736	74 208	14 963	44 472	150 %	-59 245	-80 %	-14 773	-50 %
Планирование емкостью архива	8 980	49 472	7 252	40 492	451 %	-42 220	-85 %	-1 729	-19%
Резервное копирование и архивирование	130 654	123 680	50 622	-6 974	-5 %	-73 058	-59 %	-80 032	-61 %
Управление архивами	0	24 736	0	24 736	Undefined	-24 736	-100 %	0	-
Общие ежегодные затраты	**1 563 387**	**2 473 600**	**836 474**	**910 213**	**58 %**	**-1 637 126**	**-66 %**	**-726 913**	**-46 %**

Таблица П5.11. Расшифровка затрат на обслуживание серверов

Затраты на обслуживание серверов	Текущие, руб.	Эталонные, руб.	Целевые, руб.	Разница между эталонными и текущими, руб.	Разница в %	Разница между целевыми и эталонными, руб.	Разница в %	Разница между целевыми и текущими, руб.	Разница в %
Решение проблем 2-го уровня	73 882	85 592	29 237	11 711	16 %	-56 356	-66 %	-44 645	-60 %
Решение проблем 3-го уровня	43 166	51 355	23 722	8 189	19 %	-27 633	-54 %	-19 444	-45 %
Планирование и управление трафиком	18 721	21 398	9 812	2 677	14 %	-11 586	-54 %	-8 908	-48 %
Точная настройка	18 721	12 839	9 730	-5 882	-31 %	-3 109	-24 %	-8 991	-48 %
Администрирование конечных пользователей	22 642	51 355	14 304	28 714	127 %	-37 051	-72 %	-8 337	-37 %
Поддержка операционной системы	21 481	12 839	13 687	-8 642	-40 %	848	7 %	-7 794	-36 %
Обслуживание рабочей силы	17 026	21 398	10 481	4 372	26 %	-10 917	-51 %	-6 544	-38 %
Установка программного обеспечения	46 023	55 635	24 230	9 612	21 %	-31 404	-56 %	-21 792	-47 %
Управление приложениями	28 751	12 839	12 434	-15 912	-55 %	-405	-3 %	-16 317	-57 %
Конфигурация аппаратных средств	143 021	34 237	94 451	-108 784	-76 %	60 215	176 %	-48 569	-34 %
Установка аппаратных средств	44 956	21 398	31 956	-23 558	-52 %	10 558	49 %	-13 000	-29 %
Управление дисками и файлами	27 732	12 839	16 619	-14 894	-54 %	3 780	29 %	-11 114	-40 %
Планирование вместимостью архива	5 783	8 559	4 175	2 777	48 %	-4 384	-51 %	-1 607	-28 %
Резервное копирование и архивирование	24 229	21 398	20 786	-2 831	-12 %	-612	-3 %	-3 444	-14 %
Управление архивами	23 335	4 280	20 423	-19 056	-82 %	16 143	377 %	-2 913	-12 %
Общие ежегодные затраты	**559 468**	**427 961**	**336 049**	**-131 507**	**-24 %**	**-91 912**	**-21 %**	**-223 419**	**-40 %**

Таблица П5.12. Расшифровка затрат на планирование и управление процессами

Затраты на планирование и управление процессами	Текущие, руб.	Эталонные, руб.	Целевые, руб.	Разница между эталонными и текущими, руб.	Разница в %	Разница между целевыми и эталонными, руб.	Разница в %	Разница между целевыми и текущими, руб.	Разница в %
Управление стоимостью	69 097	0	67 866	-69 097	-100 %	67 866	Undefined	-1 232	-2 %
Управление системными исследованиями, планированием и продуктами	117 328	0	69 918	-117 328	-100 %	69 918	Undefined	-47 410	-40 %
Оценка закупок	86 071	0	76 853	-86 071	-100 %	76 853	Undefined	-9 218	-11 %
Безопасность и защита от вирусов	169 951	0	103 863	-169 951	-100 %	103 863	Undefined	-66 088	-39 %
Затраты на восстановление бизнеса	18 254	0	10 620	-18 254	-100 %	10 620	Undefined	-7 634	-42 %
Общие ежегодные затраты	**460 701**	**0**	**329 119**	**-460 701**	**-100 %**	**329 119**	**Undefined**	**-131 582**	**-29 %**

Таблица П5.13. Детализация административных затрат

Административные затраты	Текущие, руб.	Эталонные, руб.	Целевые, руб.	Разница между эталонными и текущими, руб.	Разница в %	Разница между целевыми и эталонными, руб.	Разница в %	Разница между целевыми и текущими, руб.	Разница в %
Финансовые и административные затраты	795 837	665 036	575 326	-130 801	-16 %	-89 710	-13 %	-220 511	-28 %
Затраты на обучение ИТ-специалистов	188 798	114 240	188 339	-74 558	-39 %	74 099	65 %	-459	0 %
Обучение конечных пользователей	493 322	215 360	508 560	-277 962	-56 %	293 200	136 %	15 237	3 %
Общие ежегодные затраты	**1 477 957**	**994 636**	**1 272 225**	**-483 321**	**-33 %**	**277 589**	**28 %**	**-205 732**	**-14 %**

Таблица П5.14. Расшифровка финансовых и административных затрат

Финансовые и административные затраты	Текущие, руб.	Эталонные, руб.	Целевые, руб.	Разница между эталонными и текущими, руб.	Разница в %	Разница между целевыми и эталонными, руб.	Разница в %	Разница между целевыми и текущими, руб.	Разница в %
Затраты на контроль	388 410	199 511	317 198	-188 899	-49 %	117 688	59 %	-71 211	-18 %
Административная помощь сотрудникам ИТ-отдела	39 656	133 007	36 556	93 351	235 %	-96 451	-73 %	-3 101	-8 %
Управление активами	70 323	66 504	17 374	-3 819	-5 %	-49 129	-74 %	-52 949	-75 %
Бюджетирование	36 128	66 504	32 001	30 375	84 %	-34 502	-52 %	-4 127	-11 %
Аудит	18 032	33 252	10 023	15 220	84 %	-23 229	-70 %	-8 009	-44 %
Управление приобретением и контрактованием	84 239	133 007	54 290	48 768	58 %	-78 717	-59 %	-29 949	-36 %
Управление вендорами	159 048	33 252	107 883	-125 797	-79 %	74 632	224 %	-51 165	-32 %
Общие ежегодные затраты	**795 837**	**665 036**	**575 326**	**-130 801**	**-16 %**	**-89 710**	**-13 %**	**-220 511**	**-28 %**

Таблица П5.15. Расшифровка затрат на поддержку конечных пользователей

Затраты на поддержку конечных пользователей	Текущие, руб.	Эталонные, руб.	Целевые, руб.	Разница между эталонными и текущими, руб.	Разница в %	Разница между целевыми и эталонными, руб.	Разница в %	Разница между целевыми и текущими, руб.	Разница в %
Затраты на поддержку	542 1467	6 507 639	3 799 406	1 086 172	20 %	-2 708 233	-42 %	-1 622 061	-30 %
Затраты на самостоятельное изучение и поддержку	4 265 978	4 743 988	3 149 395	478 010	11 %	-1 594 593	-34 %	-1 116 583	-26 %
Формальное обучение	1 171 363	960 321	1 086 988	-211 041	-18 %	126 667	13 %	-84 375	-7 %
Управление данными	535 383	1 258 021	508 870	722 639	135 %	-749 151	-60 %	-26 512	-5 %
Разработка приложений	459 075	691 431	460 479	232 357	51 %	-230 953	-33 %	1 404	0 %
Форсмажор	0	6 296 965	0	6 296 965	Undefined	-6 296 965	-100 %	0	-
Общие ежегодные затраты	**11 853 266**	**20 458 366**	**9 005 139**	**8 605 100**	**73 %**	**-11 453 227**	**-56 %**	**-2848127**	**-24 %**

Целевые показатели моделируются на основании проекта модернизации корпоративной системы антивирусной защиты и системы управления доступом на объекте информатизации (физическая защита). Условно определяют три возможных состояния системы защиты КИС от вирусов и вредоносного программного обеспечения, а именно: базовое, среднее и высокое. Рассмотрим характеристики этих состояний:

- *базовое* – стационарные и мобильные рабочие станции обладают локальной защитой от вирусов. Антивирусное программное обеспечение и базы сигнатур регулярно обновляются для успешного распознавания и парирования новых вирусов. Установлена

программа автоматического уничтожения наиболее опасных вирусов. Основная цель уровня – организация минимальной защиты от вирусов и враждебного программного обеспечения при небольших затратах;

• *среднее* – установлена сетевая программа обнаружения вирусов. Управление программными обновлениями на сервере автоматизировано. Системный контроль над событиями оповещает о случаях появления вирусов и предоставляет информацию по предотвращению дальнейшего распространения вирусов. Превентивная защита от вирусов предполагает выработку и следование определенной политике защиты информации, передаваемой по открытым каналам связи Интернета. Дополнительно к техническим мерам активно предлагаются и используются организационные меры защиты информации;

• *высокое* – антивирусная защита воспринимается как один из основных компонентов корпоративной системы защиты. Система антивирусной защиты тесно интегрирована в комплексную систему централизованного управления информационной безопасностью компании и обладает максимальной степенью автоматизации. При этом организационные меры по защите информации преобладают над техническими мерами. Стратегия защиты информации определяется исключительно стратегией развития бизнеса компании.

Согласно практическому подходу в TCO Manager формируется отчет (табл. П5.4.) для ЗАО «Страхование», в котором отражаются требования к состоянию корпоративной системы защиты на основании данных о типе предприятия и текущего показателя TCO.

Таким образом, можно сделать вывод о том, что ЗАО «Страхование» необходимо повышать уровень защиты информационной системы от вирусов, совершенствовать технологию управления активами и проводить обучение конечных пользователей и специалистов отдела информационных технологий.

Теперь обратимся к отчетам по совокупной стоимости владения, приведенным в таблицах, и проанализируем полученные показатели TCO.

Сопоставляя табл. П5.4 и данные отчетов (табл. П5.5-П5.15), можно сделать следующие выводы: при построении целевой модели TCO наибольшему снижению подверглись административные затраты на управление (на 44 %) и затраты при простое (на 43 %). Сокращение административных расходов связано в основном с внедрением автоматизированной системы управления активами, а значительное снижение затрат от простоев – с пересмотром уровня знаний конечных пользователей и ИТ-персонала и увеличением затрат на обучение.

Небольшое повышение затрат на аппаратные средства (на 16 %) вызвано закупкой оборудования, необходимого для внедрения корпоративной системы защиты.

Таким образом, целевой показатель TCO значительно меньше текущего, но вместе с тем поддержание соответствующего уровня защиты требует существенных расходов (5–7% от ежегодного дохода), и для обоснования этих расходов необходимо применять методы оценки эффективности инвестиций в корпоративную систему информационной безопасности.

2. Обоснование инвестиций в информационную безопасность Впервые термин Return on Investment for Security (ROSI) был введен в употребление специалистами в области IT Security после публикации в начале 2002 года статьи в журнале CIO Magazine «Finally, a Real Return on Security Spending». Примерно в это же время вышло несколько статьей, посвященных количественным методам оценки затрат на безопасность. Сегодня тема возврата инвестиций (Return on Investment, ROI) в информационные технологии стала темой повышенного интереса для TOP-менеджмента многих российских компаний. При этом особое внимание уделяется методам расчета возврата инвестиций в безопасность (Return on Investment for Security, ROSI).

Традиционно обоснования расходов на безопасность были в большинстве своем качественными или «стратегическими», доказывающими, что без инвестирования в корпоративную систему защиты информации компания упускает более «осязаемые» выгоды. Обоснование расходов на информационную безопасность включало в себя следующие

утверждения:

• расходы на безопасность являются составляющей стоимости ведения бизнеса;

• расходы на безопасность родственны расходам на страхование;

• компания не может заниматься электронной коммерцией без обеспечения определенного уровня защиты электронных денежных потоков;

• безопасность является одним из аспектов управления рисками;

• заказчик имеет право подать на компанию в суд, если она отказывается соблюдать минимальные стандарты безопасности (например, защищать конфиденциальную информацию о клиенте);

• нежелание вкладывать денежные средства в безопасность означает нежелание следовать общим тенденциям развития информационных технологий.

После приведения подобных доводов ни у кого не вызывает сомнений необходимость расходов на требуемый уровень информационной безопасности компании, но вместе с этим появляется потребность количественного расчета для финансового обоснования инвестиций в корпоративную систему защиты информации. Давайте посмотрим, какие способы обоснования инвестиций в корпоративные системы защиты информации существуют и подтверждены практикой.

Метод ожидаемых потерь Этот подход базируется на том, что вычисляются потери от нарушений политики безопасности, с которыми может столкнуться компания, и эти потери сравниваются с инвестициями в безопасность, направленными на предотвращение нарушений. Метод ожидаемых потерь основан на эмпирическом опыте организаций и сведениях о вторжениях, о потерях от вирусов, об отражении сервисных нападений и т. д. Например, нарушения безопасности коммерческих организаций приводят к следующим финансовым потерям:

• при ведении электронной коммерции – потери, связанные с простоем и выходом из строя сетевого оборудования;

• нанесение ущерба имиджу и репутации компании;

• оплата сверхурочной работы ИТ-персонала и/или оплата работ подрядчиков, которые занимались восстановлением корпоративной информационной системы;

• оплата консультаций внешних специалистов, которые осуществляли восстановление данных, выполняли ремонт и оказывали юридическую помощь;

• оплата ремонта физических повреждений от виртуальных атак;

• судебные издержки при подаче искового заявления о виртуальных преступлениях и нарушениях политики безопасности.

Чтобы «смягчить» ожидаемые потери, компания должна инвестировать средства в безопасность (сетевые экраны, системы обнаружения вторжений, чтобы предотвратить атаку, антивирусы для обнаружения различных форм вирусов). Если компания решает установить систему информационной безопасности, то ее стоимость обобщенно будет складываться из:
единовременных затрат:

– покупка лицензий антивирусного программного обеспечения, средств Firewall, средств AAA;

– приобретение аппаратных средств;

– возможно, оплата консультаций внешнего эксперта в области информационной безопасности;

периодических затрат:

– затраты на техническую поддержку и сопровождение;

– заработная плата ИТ-персонала;

– затраты на наем необходимых специалистов;

– затраты на исследование угроз нарушений политики безопасности.

Следует отметить, что нет совершенной системы информационной безопасности. Чтобы определить эффект от внедрения системы информационной безопасности, мы должны вычислить показатель ожидаемых потерь (Annualized Loss Expectancy, ALE). По оценкам

экспертов, правильно установленная и настроенная система защиты дает 85 % эффективности в предупреждении или уменьшении потерь от нарушений политики безопасности. Следовательно, финансовая выгода обеспечивается ежегодной экономией средств компании, достигаемой при внедрении системы информационной безопасности:

$AS = ALE \times E - AC$, где:

AS – ежегодные сбережения (Annual Saving), ALE – показатель ожидаемых потерь (Annualized Loss Expectancy),

E – эффективность системы защиты (около 85 %),

AC – ежегодные затраты на безопасность (Annual Cost).

Метод оценки свойств системы безопасности Метод оценки свойств системы безопасности (Security Attribute Evaluation Method, SAEM) был разработан в Carnegie Melon University, он основан на сравнении различных архитектур систем информационной безопасности для получения стоимостных результатов оценки выгод от внедрения системы информационной безопасности. Методология SAEM заключается в том, чтобы, объединив вероятность события и ранжировав воздействие окружающей среды, предложить различные проекты по информационной безопасности с многовариантным влиянием окружающей среды на относительные затраты.

Недостатком метода является то, что чаще всего безопасность находится вне понимания менеджеров, занимающихся оценкой эффективности, а специалисты по информационной безопасности редко имеют точные данные относительно выгод, приносимых технологией, поэтому приходится полагаться на опыт и интуицию и на их основе принимать решения. Однако этот метод может быть использован для предоставления комплекса разнообразных мер по информационной безопасности и для поддержки принятия решения при выборе тех или иных мероприятий.

Анализ «дерева ошибок» Нетрадиционным инструментом оценки выгод является метод анализа «дерева ошибок» (Fault Tree Analysis). Цель применения данного метода – показать, в чем заключаются причины нарушений политики безопасности, и какие сглаживающие контрмеры могут быть применены. «Дерево ошибок» – это графическое средство, которое позволяет свести всю систему возможных нарушений к логическим отношениям «и – или» компонентов этой системы. Если доступны данные по нормам отказа критических компонентов системы, то «дерево ошибок» позволяет определить ожидаемую вероятность отказа всей системы.

Применяя этот метод к системам информационной безопасности, мы можем построить «дерево» с причинно-следственными отношениями между атаками на систему и нарушениями системы. Использование контрмер по предотвращению нарушений позволяет уменьшить ответвления «дерева» и, таким образом, может быть определен эффект от внедрения системы информационной безопасности на сравнении «двух деревьев» с использованием контрмер и без.

Важно заметить, что этот метод базируется на двух связанных предположениях: во-первых, что компоненты системы разрушаются случайным образом согласно хорошо известной статистике, во-вторых, на самом нижнем уровне «дерева» составляющие отказа независимы друг от друга. Все-таки отказы программного обеспечения системы информационной безопасности неслучайны и, скорее всего, возникают из-за системных ошибок, что в большинстве случаев влияет на работу других частей системы. Об этом не следует забывать при применении данного метода к системе информационной безопасности.

В настоящее время метод еще недостаточно адаптирован к области информационной безопасности и требует дальнейшего изучения.

Выбор подходящего метода Принципиальный недостаток приведенных выше методов в том, что они не дают количественной оценки стоимости и выгод от контрмер безопасности, кроме метода ожидаемых потерь, объединяющего выгоду от каждой контрмеры в единый количественный показатель «эффективности». А с точки зрения системы безопасности этот показатель интерпретируется как показатель пригодности всей

системы защиты, который обычно указан в договоре с поставщиком системы защиты.

Поэтому на практике можно воспользоваться методом оценки целесообразности затрат на систему информационной безопасности. Такой выбор был обусловлен несколькими соображениями – это финансовая ориентированность метода и достаточно полная оценка стоимости различных мер по безопасности и выгод от внедрения. Для того чтобы привести пример оценки мер по обеспечению безопасности, воспользуемся упрощенным вариантом «дерева ошибок», так называемой таблицей оценки угроз и рисков (Threat and Risk Assessment – TRA). Использование TRA позволит показать, как на практике получить количественную оценку вероятности событий и возникновения последствий и в дальнейшем использовать эти данные для определения ожидаемых потерь без применения контрмер безопасности.

Методика Return on Investment for Security Ранее мы определились с методами оценки экономической целесообразности затрат на систему информационной безопасности: расходную часть мы рассчитали с помощью программного продукта TCO Manager и получили текущий и целевой показатели совокупной стоимости владения. Сейчас мы оценим доходную часть, объединяя метод ожидаемых потерь с таблицей оценки угроз и риска.

Первым шагом является построение таблицы TRA. Но прежде дадим краткое описание контрмер по обеспечению информационной безопасности.

Контрмеры по обеспечению безопасности направлены на достижение следующих эффектов: уменьшение вероятности происхождения инцидента и/или уменьшение последствий, если инцидент все равно случается. Меры, снижающие вероятность, называются профилактическими, а меры, снижающие последствия, называются лечебными. Примеры контрмер обоих типов представлены в табл. П5.16.

Таблица П5.16. Типы контрмер безопасности

Тип контрмеры	Пример
Профилактические	Стандарты, процедуры, должностные инструкции Аудит системы безопасности Сетевые экраны Системы обнаружения вторжений Антивирусы Средства шифрования Формирование архивов
Лечебные	Резервные режимы работы
Принадлежат обоим типам	Планирование непрерывности бизнеса / планирование восстановления бизнеса Обучение

Пусть вероятность происшествия описана семью уровнями – от «незначительного» до «экстремального». Определим эти уровни в следующей таблице (табл. П5.17). Таблица П5.17. Преобразованные вероятности угроз к ежегодной частоте

Уровень вероятности	Описание	Частота
Незначительный	Вряд ли произойдет	0,05
Очень низкий	Событие происходит два-три раза в пять лет	0,6
Низкий	Событие происходит реже одного раза в год или раз в год	1,0
Средний	Событие происходит реже одного раза в полгода или раз в полгода	2,0
Высокий	Событие происходит реже одного раза в месяц или раз в месяц	12,0
Очень высокий	Событие происходит несколько раз в месяц	36,0
Экстремальный	Событие происходит несколько раз в день	365,0

Последствия от нарушения политики безопасности также описаны шестью уровнями – от «несущественного» к «критическому», и каждому уровню соответствуют потери в случае ликвидации нарушений, которые определены экспертами Gartner Group (см. табл. П5.18).

Таблица П5.18. Последствия, преобразованные в стоимость ликвидации нарушений

Степень тяжести нарушения	Описание	Потери, тыс. руб.
Несущественная	При осознанной угрозе нарушение не будет иметь последствий	0
Низкая	Нарушение не ведет к финансовым потерям, но выяснение характера происшествия потребует незначительных затрат	15
Существенная	Происшествие принесет некоторый материальный и моральный вред	150
Угрожающая	Потеря репутации, конфиденциальной информации Затраты на восстановление данных, проведение расследований	1 500
Серьезная	Потеря клиентов, деловой репутации Восстановление практически всех данных на электронных и бумажных носителях	3 000
Критическая	Потеря системы или перевод в другую безопасную среду	7 500

Теперь рассчитаем показатель ALE для ЗАО «Страхование», используя форму таблицы TRA (см. табл. П5.19), в которой сопоставляются вероятности угроз, степень тяжести нарушения и частота событий. Следует отметить, что показатель ALE мы вычисляем согласно формуле:

$ALE = f \times L$, где:

f – частота возникновения потенциальной угрозы, уровень которой определяется на основании вероятности (см. табл. П5.17). L – величина потерь в рублях, которая определяется на основании степени тяжести нарушения (см. табл. П5.18).

Таблица П5.19. Расчет показателя ожидаемых потерь для ЗАО «Страхование»

Актив	Потенциальная угроза	Уровень вероятности	Степень тяжести нарушения	Частота в год	Потери, тыс. руб.	ALE, тыс. руб.
Интернет-каналы	Разрушение ключевой инфраструктуры	Незначительный	Серьезная	0,05	3 000	150
	Отказ системы охлаждения	Средний	Существенная	2	150	300
	Нарушение конфиденциальности информации	Низкий	Серьезная	1	3 000	3 000
	Повреждение аппаратных средств инфраструктуры	Очень низкий	Угрожающая	0,6	1 500	900
	Неправильное построение инфраструктуры	Низкий	Существенная	1	150	150
	Атака на сетевую инфраструктуру провайдера	Очень низкий	Существенная	0,6	150	90
	Отказ DNS	Незначительный	Угрожающая	0,05	1 500	75
Система электронной почты	Атака на систему электронной почты	Очень высокий	Существенная	36	150	5 400
Бизнес-приложения	Проблема вывода документов	Высокий на печать	Несущественная	12	0	0
	Проблемы чтения/сохранения файлов данных	Высокий	Несущественная	12	0	0
	Нарушения надежной работы бизнес-приложений	Низкий	Угрожающая	1	1 500	1 500
	Выход из строя корпоративной системы документооборота	Высокий	Угрожающая	12	1 500	18 000
					ИТОГО	**29 565**

...

Примечание: потенциальные угрозы, указанные в табл. для ЗАО «Страхование», определены согласно рекомендациям эксперта в области информационной безопасности.

Следующим шагом обоснования инвестиций в систему информационной безопасности является проведение анализа возврата инвестиций (см. табл. П5.21). Для этого сначала определим затраты на внедрение системы информационной безопасности.

Чтобы обеспечить должный уровень безопасности, в ЗАО «Страхование» необходимо внедрить следующие элементы системы информационной безопасности: систему защиты

шлюзов Интернета, систему антивирусной защиты файловых серверов и рабочих станций и систему защиты корпоративной электронной почты. Руководством в качестве поставщика решений была выбрана компания Trend Micro, которая предоставляет широкий спектр решений в области информационной безопасности для предприятий различного масштаба.

Затраты на внедрение комплекса решений Trend Micro приведены в табл. П5.20.

Таблица П5.20. Инвестиции в систему корпоративной защиты для ЗАО «Страхование»

Статьи затрат	Стоимость, руб.
Затраты на покупку лицензий	2 358 048
Затраты на проектные работы	369 785
Техническая поддержка (30% от стоимости лицензий ежегодно)	707 414

Период окупаемости инвестиционных проектов, связанных с внедрением информационных технологий, не должен превышать трех лет, поэтому период оценки эффективности данного проекта внедрения равен трем годам. Обозначим показатели оценки:

Свн – затраты на внедрение; Сл – затраты на покупку лицензий;

С пр – затраты на проектные работы;

Ci – затраты на техническую поддержку;

ТСОт – текущий показатель ТСО (из отчетов TCO Manager);

ТСОц – целевой показатель ТСО (из отчетов TCO Manager);

ТСОф – фактический показатель ТСО;

AS – ежегодные сбережения;

B – выгоды при оптимизации показателя ТСО;

CF – денежный поток;

r – ставка дисконтирования;

NPV3 – чистая приведенная стоимость затрат на проект внедрения; NPVfl – чистая приведенная стоимость доходов от проекта внедрения.

Затраты на внедрение системы защиты информации рассчитываются по следующей формуле:

$$C_{вн} = C_{л} + C_{пр} + \sum_{i} C_i.$$

Выгоды от оптимизации текущего показателя ТСО вычисляются по формуле:

$$B = TCO_{т} + TCO_{ф}.$$

Чистая приведенная стоимость затрат на проект внедрения и доходов от проекта внедрения рассчитываются по следующим формулам:

$$NPV = \sum_{i=0} \frac{CF}{(1+r)^i}.$$

В первом случае роль денежного потока играют затраты на внедрение, а во втором – это выгоды от оптимизации показателя ТСО и внедрения корпоративной системы защиты.

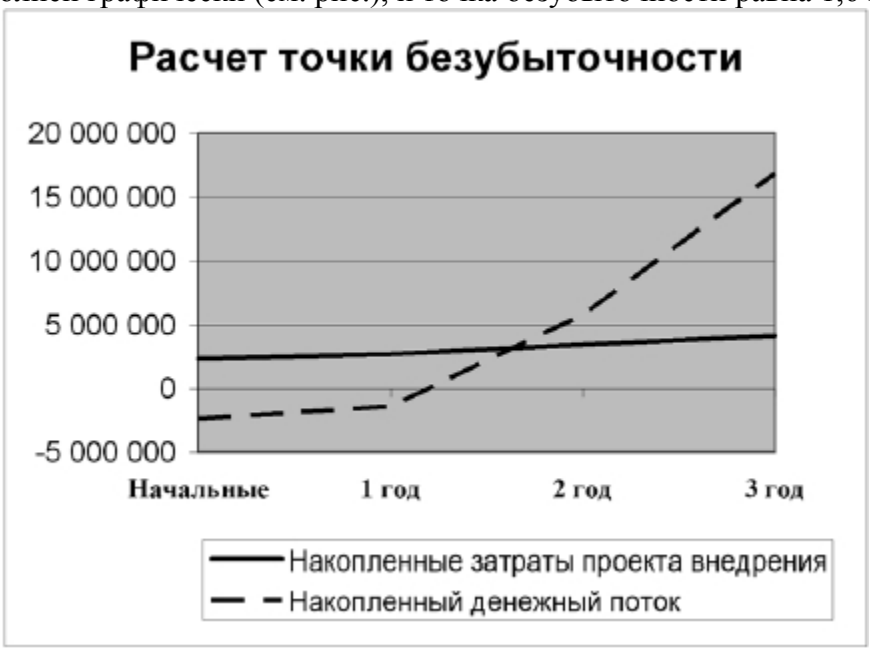
Таблица П5.21. Расчет показателей возврата инвестиций в систему информационной безопасности для ЗАО «Страхование»

Показатели	Начальные затраты, руб.	1 год, руб.	2 года, руб.	3 года, руб.	Итого, руб.
Затраты на внедрение	2 358 048	369 785	707 414	707 414	4 142 661
Накопленные затраты проекта внедрения	2 358 048	2 727 833	3 435 247	4 142 661	
Чистая приведенная стоимость (NPV) затрат на проект внедрения	3 645 614				
Текущий показатель TCO	n/a	26 383 744	26 383 744	26 383 744	79 151 232
Целевой показатель TCO	n/a	19 864 933	19 864 933	19 864 933	59 594 799
Фактический показатель TCO	n/a	25 079 982	21 820 576	19 864 933	
Выгоды при оптимизации показателя TCO	0	1 303 762	4 563 167	6 518 811	12 385 740
Показатель ожидаемых потерь (ALE)	0	29 565 000	29 565 000	29 565 000	88 695 000
Эффективность системы корпоративной защиты		85%	85%	85%	
Ежегодные сбережения (AS)	0	50 268	3 309 674	5 265 317	
Показатель выгод при оптимизации показателя TCO и ежегодные сбережения	0	1 354 030	7 872 841	11 784 128	21 010 999
Накопленный показатель выгод при оптимизации показателя TCO и ежегодные сбережения	0	1 354 030	9 226 871	21 010 999	
Денежный поток	-2 358 048	984 245	7 165 427	11 076 714	16 868 338
Накопленный денежный поток	-2 358 048	-1 373 803	5 791 624	16 868 338	
Чистая приведенная стоимость (NPV) доходов от проекта внедрения	10 577 426				
Внутренняя норма рентабельности (IRR)	145%				

...

Примечание: ставка дисконтирования равна ставке рефинансирования Центрального банка РФ (14 %).

Внутренняя норма рентабельности рассчитывается при NPV, равном нулю. Расчет точки безубыточности проекта внедрения корпоративной системы информационной безопасности выполнен графически (см. рис.), и точка безубыточности равна 1,6 года.



...

Рис. Расчет точки безубыточности проекта внедрения системы информационной безопасности

Таким образом, проект внедрения корпоративной системы информационной безопасности можно считать экономически выгодным, так как чистая приведенная стоимость доходов от проекта внедрения положительна и больше чистой приведенной стоимости затрат на проект внедрения в 2,9 раза.

Приложение 6 ПРИМЕРЫ МЕТОДИЧЕСКИХ МАТЕРИАЛОВ ПО ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

Инструкция для администратора безопасности сети

Администратор безопасности сети компании X назначается из числа наиболее подготовленных системных администраторов, владеющих сетевыми технологиями на основе TCP/IP-протокола.

Он отвечает за корректное функционирование брандмауэров, настройку и поддержание в работоспособном состоянии серверов и клиентов, а также за реализацию политики безопасности сети.

Администратор безопасности сети подчиняется начальнику ИТ-службы и его заместителю, а при организации группы интернет-технологий – руководителю группы.

Администратор безопасности сети обязан:

• администрировать брандмауэр преимущественно с локального терминала;

• использовать усиленную аутентификацию и сквозное шифрование трафика в случае удаленного соединения с брандмауэром;

• не использовать брандмауэр как сервер общего назначения;

• создавать ежедневные, еженедельные и ежемесячные архивные копии системных программ брандмауэра;

• при наличии «зеркального «брандмауэра поддерживать его в «холодном» резерве;

• контролировать все разрешенные соединения с внешними сетями;

• периодически проверять и удалять неиспользуемые логины пользователей;

• вести системный журнал соединений с внешними сетями;

• по указанию руководителя группы удалять все параметры ненужного соединения;

• использовать механизм шифрования при работе с частными виртуальными сетями, VPN;

• контролировать все утвержденные VPN-соединения;

• поддерживать механизмы распределения и администрирования ключей шифрования при эксплуатации VPN-соединений;

• администрировать все основные, вторичные или кэшируемые DNS-серверы;

• ежедневно, еженедельно и ежемесячно обновлять и хранить в установленном месте данные для проверки целостности брандмауэра; документировать параметры конфигурации брандмауэра в рабочих журналах;

• создавать ежедневные, еженедельные и ежемесячные отчеты для анализа сетевой активности;

• каждую неделю анализировать таблицы состояния брандмауэра для выявления следов атак;

• в случае атаки немедленно прибыть к локальному терминалу брандмауэра и предпринять необходимые контрмеры;

• обнаруживать попытки сканирования или зондирования брандмауэра сети; блокировать работу всех типов программ, представляющих угрозу безопасности сети;

• при выявлении факта проникновения поставить в известность руководителя группы и

с его разрешения отключить брандмауэр сети от Интернета. Переконфигурировать брандмауэр и подключиться к Интернету; придерживаться рекомендаций производителя брандмауэра в отношении мощности процессора и объема оперативной памяти; производить оценку возможностей каждой новой версии брандмауэра на предмет необходимости установления доработок;

• оперативно модифицировать исполняемый код брандмауэра по рекомендациям его производителя;

• получать модули доработки брандмауэра только у его производителя; подписаться на список рассылки производителя брандмауэра или другим доступным способом получать информацию обо всех требуемых доработках; выявлять недокументированные возможности брандмауэра и уметь их парировать при его эксплуатации;

• запретить использование Интернета в личных целях; запретить доступ в Интернет с использованием нештатных модемов; определить порядок доступа в Интернет через шлюзы сети; регулярно пересматривать политику сетевой безопасности (не реже одного раза в три месяца);

• следить за тем, чтобы структура и параметры сети были скрыты внешним брандмауэром;

• выявлять и наказывать всех нарушителей системной политики безопасности сети;

• тестировать брандмауэр перед началом работы и проверять правильность его конфигурации;

• сконфигурировать брандмауэр так, чтобы он был прозрачен для входящих соединений;

• контролировать трафик на открытый интернет-сервер и закрытый интранет-сервер;

• в случае аварии или сбоя брандмауэра блокировать доступ к любым сетевым службам;

• запретить маршрутизацию источника на всех брандмауэрах и внешних маршрутизаторах;

• блокировать трафик из внешних интерфейсов, выдающих себя за внутренние интерфейсы сети;

• вести журнал нештатных ситуаций брандмауэра;

• вести рабочий журнал работы брандмауэра, в котором отражать: схему сети с IP-адресами всех сетевых устройств, IP-адреса провайдера (внешние серверы новостей, маршрутизаторы, DNS-серверы и др.), параметры конфигурации брандмауэра, правила фильтрации пакетов и т. п.;

• использовать для хранения журналов и системных носителей специальное место хранения с ограниченным доступом;

• по умолчанию запретить все сервисы, которые явно не разрешены;

• проводить регулярный аудит брандмауэра на предмет выявления попыток проникновения или неверного использования Интернета;

• немедленно устранять все ситуации, приводящие к сбою или аварийному завершению брандмауэра;

• обслуживать брандмауэр на выделенном сервере. При этом все системные и прикладные программы, не относящиеся к брандмауэру, удалить или заблокировать;

• протоколировать весь доступ к Интернету;

• выявлять всех нарушителей использования Интернета.

Администратор безопасности сети обязан следить за исправным функционированием сети, выполнять все распоряжения и указания руководителя группы, оказывать ему помощь в поддержании Интернет/интранет-технологий в работоспособном состоянии; оставаясь за старшего группы, выполнять его обязанности.

Инструкция для администратора Web-сереера сети

Администратор Web-сереера сети компании X назначается из числа наиболее подготовленных системных администраторов, владеющих сетевыми технологиями на основе

TCP/IP-протокола.

Он отвечает за корректное функционирование Web-сереера, настройку и поддержание в работоспособном состоянии внутренних Web-серверов и клиентов, а также за реализацию политики безопасности при работе с технологией WWW.

Администратор Web-сереера сети подчиняется начальнику ИТ-службы и его заместителю, а при организации группы интернет-технологий – руководителю группы.

Администратор Web-сереера сети обязан:

• поддерживать локальные архивы программ Web-серверов и опубликованной ранее информации;

• запретить пользователям устанавливать и запускать Web-серверы;

• не размещать информацию на Web-сереере без получения письменного разрешения руководства;

• установить порядок размещения утвержденных документов на Web-сереере;

• разрешить пользователям – участникам проекта иметь собственные Web-страницы;

• размещать утвержденные, публично доступные данные на открытом Интернет-сервере;

• размещать утвержденную служебную информацию на внутреннем интранет-сервере в защищенном сегменте сети;

• конфигурировать Web-серверы так, чтобы пользователи не могли устанавливать CGI-скрипты;

• отключить все неутвержденные сетевые приложения за исключением HHTP;

• с помощью IP-адресов разрешить доступ к Web-серверам только авторизованным системам;

• по умолчанию всегда менять пароли пользователей;

• контролировать сетевой трафик на предмет выявления неавторизованных Web-серверов;

• выявлять и наказывать нарушителей системной политики безопасности сети;

• тестировать все доступные Web-сайты на предмет корректности ссылок;

• запретить использование средств удаленного управления Web-серверами;

• запретить вход в систему с удаленного терминала с правами суперпользователя;

• проводить все исправления программ Web-серверов и ОС, рекомендованные производителями ПО;

• сканировать входящий трафик HTTP на предмет появления неавторизованных Web-серверов;

• осуществлять аудит всех Web-сайтов;

• протоколировать деятельность всех пользователей, некорректно использующих Интернет;

• контролировать разработку и использование CGI-скриптов.

Администратор Web-сереера сети обязан следить за исправным функционированием Web-серверов, выполнять все распоряжения и указания руководителя группы, оказывать ему помощь в поддержании интернет/интранет-технологий в работоспособном состоянии; оставаясь за старшего группы, выполнять его обязанности. *Инструкция для пользователя интернет/интранет-технологий сети* Пользователь интернет/интранет-технологий сети компании X назначается приказом по подразделению.

Он отвечает за корректное использование интернет/интранет-технологий сети в служебных целях, поддержание в работоспособном состоянии программного обеспечения серверов и клиентов, а также за выполнение принятой политики безопасности сети.

Пользователь интернет/интранет-технологий сети подчиняется начальнику подразделения и его заместителю, а в порядке работы в сети – сотрудникам-администраторам группы интернет-технологий.

Пользователь интернет/интранет-технологий сети обязан:

• использовать интернет только в служебных целях;

• осуществлять выход в Интернет через шлюзы сети, используя рекомендованное ПО;

• не пытаться обойти брандмауэр с помощью модемов или программ сетевого туннелирования;

• при разрешенном удаленном доступе к сети использовать усиленную аутентификацию (одноразовые пароли, информационные подписи, асимметричные ключи);

• не пытаться подключиться к объявленным сайтам, запрещенным для доступа;

• использовать программы поиска WWW, FTP и другие только в служебных целях;

• работать на Web-браузерах, разрешенных администратором безопасности сети;

• проверять все загружаемые файлы WWW на наличие вирусов;

• не обрабатывать на своих Web-браузерах программы Java, JavaScript и ActiveX, не утвержденные начальником ИТ-службы;

• проверять каждый загружаемый файл на наличие вирусов и закладок;

• предоставлять информацию для опубликования на Web-сереере только в служебных целях;

• не устанавливать и не запускать Web-серверы;

• соблюдать порядок и правила утверждения официальных документов, установленные в сети;

• при участии в проектах использовать только специальные Web-страницы;

• не использовать электронную почту в личных целях, в ущерб деятельности и политики безопасности сети компании;

• помнить, что все электронные письма, создаваемые и хранимые на компьютерах, являются собственностью компании и не считаются персональными;

• получить личный адрес и пароль у администратора электронной почты сети;

• для отправления электронной почты регистрироваться путем ввода своего имени и пароля на своем браузере по адресу: http://*******;

• не использовать адреса в письмах-«пирамидах»;

• использовать только утвержденные почтовые службы;

• не использовать анонимные адреса;

• не разрешать никому от своего имени посылать письма;

• при отправлении утвержденной конфиденциальной информации использовать доступные механизмы шифрования, аутентификации и сертификации.

Пользователь интернет/интранет-технологий сети обязан помнить, что в соответствии с приказом директора компании X, лица участвующие в передаче по Интернету информации, составляющей коммерческую тайну, несут персональную ответственность.

Рекомендуемая политика безопасности компьютерной сети компании X Таблица П6.1. Регламент доступа компьютерной сети предприятия к Интернету

Сервис	Протоколы	Что делать	Почему
E-mail		Пользователи должны иметь только один адрес электронной почты	Чтобы не раскрывать коммерческой информации
	SMPT	Сервис электронной почты для организации должен осуществляться с помощью одного центрального сервера	Централизованный сервис легче администрировать В SMTP-серверах трудно конфигурировать безопасную работу
	POP3	POP-пользователи должны использовать APOP-аутентификацию Рекомендовать переход на IMAP	Чтобы предотвратить перехват паролей
	IMAP4		Лучше подходит для удаленных пользователей, имеет средства шифрования данных
WWW	HTTP	Направлять на ******	Централизованный WWW легче администрировать WWW-серверы тяжело конфигурировать
Новости USENET	NTTP	Блокировать на брандмауэре.	Сервис не нужен для деятельности

Таблица П6.2. Рекомендуемая политика безопасности сети

Сервис	Состояние (в Интернете)	Аутентификация	Состояние (в интранете)	Аутентификация	Политика
FTP	Да	Нет	Да	Да	Доступ разрешен в Интернет Использовать усиленную аутентификацию для доступа в интранет
Telnet	Да	Нет	Да	Да	Доступ должен быть разрешен в Интернет Использовать усиленную аутентификацию для доступа в интранет
Rlogin	Да	Нет	Да	Да	Усиленная аутентификация и наличие письменного разрешения администратора по безопасности
HTTP	Да	Нет	Нет	Нет	Открытый WWW-сервер размещается за брандмауэром Входящий HTTP через брандмауэр должен быть запрещен

Окончание табл. П6.2

Сервис	Состояние (в Интернете)	Аутентификация	Состояние (в интранете)	Аутентификация	Политика
SSL	Да	Нет	Да	Да	Использовать сертификаты клиентов для прохождения через брандмауэр
POP3	Нет	Нет	Да	Нет	POP-сервер размещается за брандмауэром Брандмауэр пропускает POP-трафик только к POP-серверу Требуется использовать APOP
NNTP	Да	Нет	Нет	Нет	Внешний доступ запретить
Real Audio	Нет	Нет	Нет	Нет	Запретить вход
Lp	Да	Нет	Нет	Нет	Запретить вход
Finger	Да	Нет	Нет	Нет	Запретить вход
Gopher	Да	Нет	Нет	Нет	Запретить вход
Whois	Да	Нет	Нет	Нет	Запретить вход
SQL	Да	Нет	Нет	Нет	Соединения утверждаются начальником ИТ-службы Используются утвержденные proxy-серверы
Rsh	Да	Нет	Нет	Нет	Запретить вход
Другие	Нет	Нет	Нет	Нет	Запретить

Приложение 7 ПЕРЕЧЕНЬ ЗАКОНОДАТЕЛЬНЫХ АКТОВ ПО ЗАЩИТЕ ИНФОРМАЦИИ

Нормативно-правовые акты

• Конституция Российской Федерации, 1993 г. • Гражданский кодекс Российской Федерации, часть I, 1994 г.

• Гражданский кодекс Российской Федерации, часть II, 1995 г.

• Уголовный кодекс Российской Федерации, 1996 г.

• Постановление Пленума Верховного Суда РФ и Высшего Арбитражного Суда РФ «О некоторых вопросах, связанных с применением части I ГК РФ», № 6/8, 1996 г.

• Концепция национальной безопасности Российской Федерации, утверждена Президентом РФ № Пр-1300, 1997 г.

• Доктрина информационной безопасности Российской Федерации, утверждена Президентом РФ № Пр-1895, 2000 г.

• Уголовно-Процессуальный кодекс Российской Федерации, 2001 г.

• Кодекс Российской Федерации об административных правонарушениях, 2001 г.

Федеральные законы

• Федеральный закон «О средствах массовой информации», № 2224-1,1991 г • Закон «О безопасности», № 2446-1, 1992 г.

• Закон «О государственной тайне», № 5485-1, 1993 г.

• Федеральный закон «О статусе депутата СФ и статусе депутата ГД ФС РФ», № 3-ФЗ, 1994 г.

• Федеральный закон «О связи», № 126-ФЗ, 2003 г.

• Федеральный закон «Об основах государственной службы», № 20-ФЗ, 1995 г.

• Федеральный закон «Об информации, информатизации и защите информации», № 24-ФЗ, 1995 г.

• Федеральный закон «Об органах федеральной службы безопасности РФ», № 40-ФЗ, 1995 г.

• Федеральный закон «Об участии в международном информационном обмене», № 85-ФЗ, 1995 г.

• Федеральный закон «Об оперативно-розыскной деятельности», № 144-ФЗ, 1995 г.

• Федеральный закон «О прокуратуре Российской Федерации», № 168-ФЗ, 1995 г.

• Федеральный закон «О лицензировании отдельных видов деятельности» (с изменениями от 13.03.2002 г.), № 128-ФЗ, 2001 г.

• Федеральный закон «Об электронной цифровой подписи», № 1-ФЗ, 2002 г.

• Федеральный закон «О техническом регулировании», № 184-ФЗ, 2002 г.

• Федеральный закон «О коммерческой тайне», № 98-ФЗ, 2004 г.

Указы Президента РФ

• Указ Президента РФ «Об основах государственной политики в сфере информатизации», № 170, 1994 г. • Указ Президента РФ «О мерах по соблюдению законности в области разработки, производства, реализации и эксплуатации шифровальных средств, а также предоставления услуг в области шифрования информации», № 334, 1995 г.

• Указ Президента РФ «Об утверждении перечня сведений, отнесенных к государственной тайне», № 1203, 1995 г.

• Указ Президента РФ «Вопросы межведомственной комиссии по защите государственной тайны», № 71, 1996 г.

• Указ Президента РФ «Об утверждении перечня сведений конфиденциального характера», № 188, 1997 г.

• Указ Президента РФ «Об утверждении концепции национальной безопасности РФ», № 1300, 1997 г.

• Указ Президента РФ «Вопросы государственной технической комиссии при Президенте РФ», № 212, 1999 г.

• Указ Президента РФ «О составе межведомственной комиссии по защите государственной тайны по должностям», № 1467, 1999 г.

• Распоряжение Президента РФ «Об утверждении Перечня лиц органов государственной власти Российской Федерации, наделенных полномочиями по отнесению сведений к государственной тайне», № 6, 2000 г.

Постановления Правительства РФ

• Постановление Правительства РСФСФ «О перечне сведений, которые не могут составлять коммерческую тайну», № 35, 1991 г. • Постановление Совета Министров – Правительства РФ «Об утверждении Положения о государственной системе защиты информации в Российской Федерации от иностранных технических разведок и от ее утечки по техническим каналам», № 912-51, 1993 г.

• Постановление Правительства РФ «Об утверждении Положения о порядке обращения со служебной информацией ограниченного распространения в федеральных органах исполнительной власти», № 1233, 1994 г.

• Постановление Правительства РФ «Об утверждении Положения о сертификации средств защиты информации», № 608, 1995 г.

• Постановление Правительства РФ «О лицензировании деятельности предприятий, учреждений и организаций по проведению работ, связанных с использованием сведений, составляющих государственную тайну, созданием средств защиты информации, а также с осуществлением мероприятий и (или) оказанием услуг по защите государственной тайны»,

№ 333, 1995 г. (с изменениями от 29 июля 1998 г.).

• Постановление Правительства РФ «О лицензировании деятельности по международному техническому обмену», № 564, 1998 г.

• Постановление Правительства РФ «О лицензировании отдельных видов деятельности», № 135, 2002 г.

• Постановление Правительства РФ «О лицензировании деятельности по технической защите конфиденциальной информации», № 290, 2002 г.

• Постановление Правительства РФ «Об утверждении Положения о лицензировании деятельности по разработке и (или) производству средств защиты конфиденциальной информации», № 348, 2002 г.

• Постановление Правительства РФ «Об утверждении Положений о лицензировании отдельных видов деятельности, связанных с шифровальными (криптографическими) средствами», № 691, 2002 г.

ГОСТ и Руководящие документы Гостехкомиссии (ФСТЭК)

• ГОСТ ВД 21552-84. «СВТ. ОТТ, правила приемки, методы испытаний, маркировка, упаковка, транспортирование и хранение». • ГОСТ ВД 16325-88. «Машины вычислительные электронные цифровые общего назначения. ОТТ».

• ГОСТ 34.201-89. «ИТ. Комплекс стандартов на АС. Виды, комплектность и обозначение документов при создании АС».

• ГОСТ 34.602-89. «ИТ. Комплекс стандартов на АС. Техническое задание на создание АС».

• ГОСТ 34.003-90. «ИТ. Комплекс стандартов на АС. Термины и определения».

• ГОСТ 29339-92. «ИТ. Защита информации от утечки за счет ПЭМИН при ее обработке СВТ. Общие технические требования».

• Положение по аттестации объектов информатизации по требованиям безопасности информации, Гостехкомиссия России, 1994 г.

• ГОСТ Р 50739-95. «СВТ. Защита от несанкционированного доступа к информации. Общие технические требования».

• ГОСТ Р 50752-95. «ИТ. Защита информации от утечки за счет ПЭМИН при ее обработке СВТ. Методы испытаний».

• ГОСТ Р 50922-96. «ЗИ. Основные термины и определения».!!!!!!

• ОСТ 4.0029-97. «Защита информации от технических разведок. Волоконно-оптические системы передачи. Технические требования по защите используемых компонентов от побочных излучений».

• ОСТ 4.0030-97. «Защита информации от технических разведок. Волоконно-оптические системы передачи. Технические требования по защите от побочного излучения».

• Решение Гостехкомиссии России и ФАПСИ «Положение о государственном лицензировании деятельности в области защиты информации» (с дополнением), № 10, 1997 г.

• ГОСТ Р 51188-98. «ЗИ. Испытания программных средств на наличие компьютерных вирусов. Типовое руководство».

• Руководящий документ. «АС. Защита от НСД к информации. Классификация АС и требования по защите информации», Гостехкомиссия России, 1998 г.

• Руководящий документ. «Концепция защиты СВТ и АС от НСД к информации», Гостехкомиссия России, 1998 г.

• Руководящий документ. «СВТ. Защита от НСД к информации. Показатели защищенности от НСД к информации», Гостехкомиссия России, 1998 г.

Руководящий документ. «СВТ. МЭ. Защита от НСД к информации. Показатели защищенности от НСД к информации», Гостехкомиссия России, 1998 г.

• Руководящий документ. «Средства защиты информации. Защита информации в контрольно-кассовых машинах и автоматизированных кассовых системах. Классификация

контрольно-кассовых машин, автоматизированных кассовых систем и требования по защите информации. Сборник руководящих документов по защите информации от несанкционированного доступа», Гостехкомиссия России, 1998 г.

• Руководящий документ. «Защита от НСД к информации. Часть 1. Программное обеспечение СЗИ. Классификация по уровню контроля отсутствия недекларированных возможностей», Гостехкомиссия России, 1999 г.

• ГОСТ Р 51275-99. «ЗИ. Объект информатизации. Факторы, воздействующие на информацию. Общие положения».

• ГОСТ Р 51318.22–99 (СИСПР 2297). «Совместимость технических средств электромагнитная. Радиопомехи индустриальные от оборудования информационных технологий. Нормы и методы испытаний».

• ГОСТ Р ИСО 7498-1-99 «ИТ. Взаимосвязь открытых систем. Базовая эталонная модель. Часть 1. Базовая модель».

• ГОСТ Р ИСО 7498-2-99 «ИТ. Взаимосвязь открытых систем. Базовая эталонная модель. Часть 2. Архитектура защиты информации».

• ГОСТ Р 51583-00. ЗИ. «Порядок создания автоматизированных систем в защищенном исполнении. Общие положения».

• ГОСТ Р 51624-00. «ЗИ. Автоматизированные системы в защищенном исполнении. Общие требования».

• ГОСТ Р ИСО/МЭК 15408-1-2002. «ИТ. Методы и средства обеспечения безопасности. Критерии оценки безопасности информационных технологий. Часть 1. Введение и общая модель».

• ГОСТ Р ИСО/МЭК 15408-2-2002. «ИТ. Методы и средства обеспечения безопасности. Критерии оценки безопасности информационных технологий. Часть 2. Функциональные требования безопасности».

• ГОСТ Р ИСО/МЭК 15408-3-2002. «ИТ. Методы и средства обеспечения безопасности. Критерии оценки безопасности информационных технологий. Часть 3. Требования доверия к безопасности».

• Специальные требования и рекомендации по технической защите конфиденциальной информации (СТР-К), Гостехкомиссия России, 2002 г. Руководящий документ. «Безопасность информационных технологий. Положение по разработке профилей защиты и заданий по безопасности». Гостехкомиссия России, 2003 г.

• Руководящий документ. «Безопасность информационных технологий. Руководство по регистрации профилей защиты». Гостехкомиссия России, 2003 г.

• Руководящий документ. «Безопасность информационных технологий. Руководство по формированию семейств профилей защиты». Гостехкомиссия России, 2003 г.

• Руководящий документ. «Руководство по разработке профилей защиты и заданий по безопасности». Гостехкомиссия России, 2003 г.

Примечания

1

ГОСТ 51583-2000 «Защита информации. Порядок создания автоматизированных систем в защищенном исполнении. Общие положения»; ГОСТ Р 51624-2000 «Защита информации. Автоматизированные системы в защищенном исполнении. Общие требования».

2

Федеральный закон «Об информации, информатизации и защите информации», № 24-ФЗ, 1995 г., ст. 2; Конституция Российской Федерации, ст. 23; Гражданский кодекс Российской Федерации, часть I, ст. 139, 128.

3

Международные стандарты безопасности ISO разработаны the International Organization for Stan– dartization (ISO) и the International Electrotechnical Commission (IEC). В России

стандарты ISO пока не являются общепринятыми, за исключением ISO 15408, адаптированная версия которого была принята Госстандартом и Гостехкомиссией летом 2002 года. ISO не вступают в противоречие с действующими в РФ стандартами и рекомендациями Гостехкомиссии при Президенте РФ, ФАПСИ и рекомендуются к применению ведущими специалистами в области информационной безопасности. Тексты ISO можно найти по адресу: www.iso.org.

4

УК РФ, 1996 г., ст. 183, 272–274.

5

Румянцев О.Г., Додонов В.Н. Юридический энциклопедический словарь. М.: ИНФРА-М, 1997.

6

Указ Президента Российской Федерации от 6 марта 1997 г. № 188 «Об утверждении перечня сведений конфиденциального характера»; Постановление Правительства РСФСР от 5 декабря 1991 г. № 35 «О перечне сведений, которые не могут составлять коммерческую тайну».

7

См. сноски 1, 2.

8

Федеральный закон «Об информации, информатизации и защите информации», № 24-ФЗ, 1995, ст. 2.

9

Федеральный закон «Об информации, информатизации и защите информации», № 24-ФЗ, 1995, ст. 2; Конституция Российской Федерации, ст. 23.

10

Федеральный закон «Об информации, информатизации и защите информации», № 24-ФЗ, 1995, ст. 2; Конституция Российской Федерации, ст. 23., Гражданский кодекс РФ, часть I, ст. 139, 128.

11

Остальные шаблоны политик безопасности SANS см. в Приложении 4.

12

Полный текст нового стандарта см.: «Вестник Банка России». 2004. № 68 (792).