Лучшие практики создания нормативных документов по кибербезопасности в компании

С. А. Петренко, В. А. Курбатов

В настоящее время сформировалась так называемая лучшая практика, «Best Practices», разработки нормативных документов по защите конфиденциальной информации в организациях и компаниях. 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 нормативных документов по безопасности в отечественных компаниях? Давайте посмотрим вместе.

Подход компании IBM

По мнению IBM, разработка корпоративных руководящих документов в области безопасности должна начинаться с создания политики информационной безопасности компании. При этом рекомендуется использовать международный стандарт ISO 17799:2002 и рассматривать политику безопасности компании как составную часть процесса управления информационными рисками (см. рис. 1). Считается, что разработка политики безопасности относится к стратегическим задачам TOP-менеджмента компании, который способен адекватно оценить стоимость информационных активов компании и принять обоснованные решения по защите информации с учетом целей и задач бизнеса.

Компания IBM выделяет следующие основные этапы разработки политики безопасности:

1. Определение информационных рисков компании, способных нанести максимальный ущерб для определения в дальнейшем процедур и мер по предупреждению их возникновения.
2. Разработка политики безопасности, которая описывает меры защиты информационных активов, адекватных целям и задачам бизнеса.

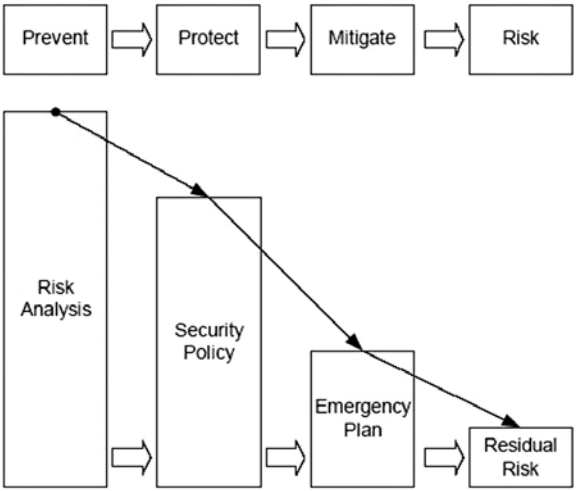

Рис. 1. Процесс разработки политики безопасности компании

3. Выработка планов действий в чрезвычайных ситуациях для уменьшения ущерба в случаях, когда выбранные меры защиты не смогли предотвратить инциденты в области безопасности.
4. Оценка остаточных информационных рисков и принятие решения о дополнительных инвестициях в средства и меры безопасности. Решение принимает руководство на основе анализа остаточных рисков.

Структура документов безопасности

По мнению IBM, политика безопасности компании 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 содержит минимум технических деталей, являясь 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, которые включают:

1) соответствие требованиям законодательства и контрактных обязательств;
2) обучение вопросам информационной безопасности;
3) предупреждение и обнаружение вирусных атак;
4) планирование непрерывности бизнеса;
5) определение ролей и обязанностей по различным аспектам общей программы информационной безопасности;
6) описание требований и процесса отчетности по инцидентам связанным с информационной безопасностью;
7) описание процесса поддержки политики безопасности.

Компания IBM выделяет следующие основные этапы разработки политики безопасности компании:

- анализ бизнес-стратегии компании и связанные с этим требования по информационной безопасности;
- анализ ИТ-стратегии, текущие проблемы информационной безопасности и требования по информационной безопасности, которые появятся в будущем;
- создание политики безопасности, взаимно увязанной с бизнес- и IT-стратегиями.

Рекомендуемая структура руководящих документов по обеспечению информационной безопасности компании может быть представлена следующим образом (см. рис. 2).

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 быть часто изменяющимися документами, так как на них оказывают влияние текущие угрозы и уязвимости информационных технологий.

В представлении IBM, политики и стандарты безопасности создаются для:

- создания 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.

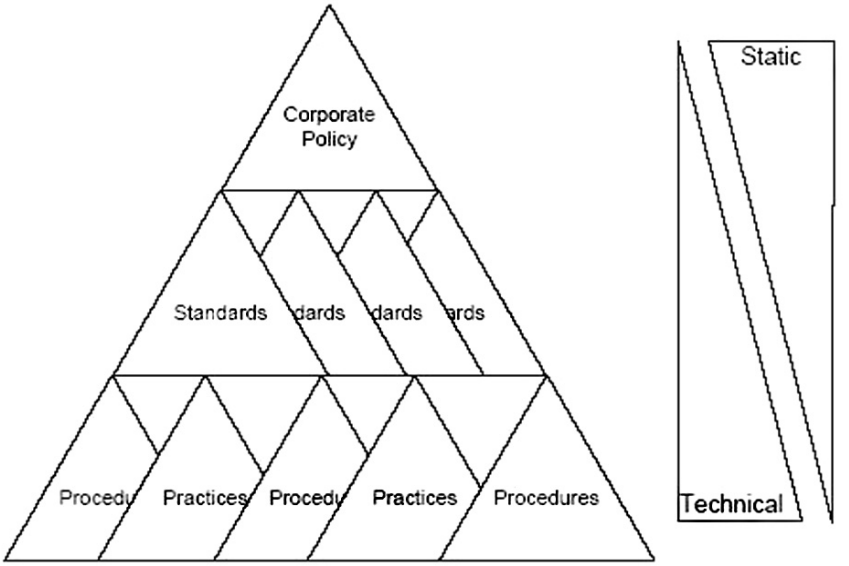

Рис. 2. Структура руководящих документов безопасности

Стандарты реализуются с помощью практик и/или процедур. Практики являются практической 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.

Давайте рассмотрим особенности предлагаемого подхода IBM на следующем примере:

1. Проблемная ситуация — сотрудники загружают программное обеспечение из сети Интернет, что приводит к заражению вирусами, а в конечном счете к уменьшению производительности работы сотрудников компании.
2. В политику безопасности добавляется строка — «информационные ресурсы компании могут быть использованы только для выполнения служебных обязанностей». Политика безопасности доступна для ознакомления всем сотрудникам компании.
3. Создается стандарт безопасности, в котором описывается, какие сервисы и программное обеспечение разрешены для использования сотрудниками.

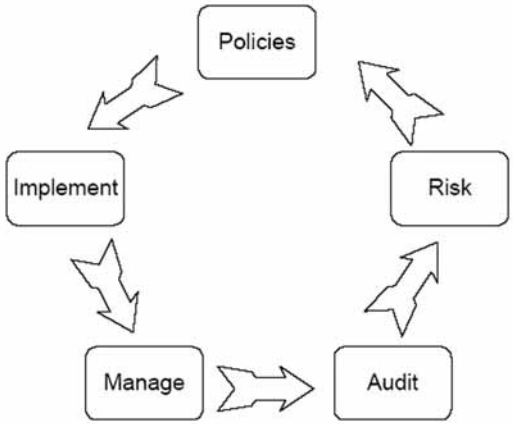

Рис. 3. Подход IBM к разработке документов безопасности

4. Практика безопасности описывает как настроить операционную систему в соответствии с требованиями стандарта безопасности.
5. Процедура безопасности описывает процесс запроса и получения разрешения на использование дополнительных сервисов или установку дополнительного программного обеспечения сотрудниками.
6. Устанавливаются дополнительные сервисы для контроля выполнения требований политики безопасности.

Общий подход к этому процессу представлен на рис. 3.

Пример стандарта безопасности

1. *Цель и область действия стандарта*

Этот документ определяет требования по защите и управлению компьютеров, работающих под управлением ОС семейства UNIX.

Аудитория: персонал служб информационных технологий и информационной безопасности.

Полномочия: Департамент управления информационными рисками 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: действует с 1 января до 31 декабря 2005.

Исключения: все отклонения от выполнения данного стандарта должны получить подтверждение в Департаменте управления информационными рисками.

Поддержка: по всем вопросам, связанным с этим стандартом, обращаться в Департамент управления информационными рисками.

Пересмотр стандарта: стандарт пересматривается ежегодно.

2. *Стандарт безопасности ОС семейства UNIX*

2.1. Учетные записи пользователей и групп

2.1.1. *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.

2.1.2. *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.

2.1.3. *Профили пользователей*

Все глобальные профили должны иметь значение umask, равное 0 2 3, т. е. 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.

2.1.4. *Политика использования паролей*

Пароли должны удовлетворять требованиям, описанным в Инструкции по использованию паролей.

2.1.5. *Домашние директории*

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

2.1.6. *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.

2.1.7. *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.

2.1.8. *Привилегированные учетные записи*

Эти учетные записи имеют право повышать свои привилегии до уровня root. Совместное использование таких учетных записей строго запрещается. Использование таких учетных записей должно журналироваться, и эти учетные записи могут быть выданы только системным администраторам и администраторам приложений.

2.1.9. *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.

3. *Сетевой доступ*

3.1. Удаленный доступ

3.1.1. *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.

3.1.2. *Устройства удаленного доступа*

Установка и использование любых устройств удаленного доступа запрещено за исключением систем, специально предназначенных для этих целей. Для указанных систем все действия регистрируются.

3.1.3. *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.

3.1.4. *Удаленный доступ для привилегированных пользователей и администраторов*

Все сетевые протоколы, передающие пароли в незашифрованном виде, запрещены для подключения. Такие протоколы могут быть использованы только в случае использования криптозащищенного туннеля.

3.1.5. *Цепочка доверия*

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

3.1.6. *Сервис TFTP*

Сервис TFTP не должен разрешать выгрузку файлов.

3.1.7. *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 Интернет, то для выгрузки файлов необходимо использовать отдельную файловую систему.

3.1.8. *Сервис HTTP*

Перед установкой веб-сервера обязательным является получение разрешения у владельца системы. Веб-приложения не должны нуждаться в административных привилегиях ни для администрирования, ни для функционирования.

3.1.9. *Приветственное приглашение*

При попытке пользователей войти в систему должно появляться приветственное приглашение. Приглашение должно отображать сообщение в формате, описанном в пункте 2.1.9. Там, где возможно, приглашение должно скрывать название операционной системы и ее версию.

3.2. Приложения

3.2.1. *Учетные записи*

Должны быть созданы 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.

3.2.2. *Владение процессом сетевого сервиса*

Процессы, которые обеспечивают удаленный доступ к некоторым приложениям, не должны выполняться под привилегированными учетными записями и не должны иметь возможность повышать привилегии учетной записи. Приложения, которые используют привилегированные порты, должны убрать такие привилегии до инициализации сетевого уровня.

3.2.3. *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. Должны быть использованы настройки, предупреждающие неавторизованное удаление и кражу файлов. Должны быть использованы списки контроля доступа, если система предлагает расширенные механизмы безопасности из POSIX.

3.3. Целостность системы

3.3.1. *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.

3.3.2. *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.

3.3.3. *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 предоставлено всем, должны быть смонтированы с опциями эквивалентными nosuid, nodev и noexec.

3.3.4. *Файлы управления заданиями*

Доступ к механизмам управления заданиями, таким как at или cron, должен быть разрешен только системным администраторам или администраторам приложений.

3.3.5. *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, которые могут иметь возможность повышения привилегий до уровня root, должны повышать привилегии только с использованием упаковщиков shell, таких как sudo, calife, super. Эти упаковщики должны быть установлены так, чтобы только администраторы могли выполнять набор команд, который им разрешен для выполнения. Должен быть организован тщательный анализ аргументов командной строки.

3.3.6. *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.

3.3.7. *Синхронизация времени*

Синхронизация времени должна происходить из доверенного источника.

4. *Критичные системы и системы доступные из Интернет*

4.1. Учетные записи групп и пользователей

4.1.1. *Глобальные профили пользователей*

Все глобальные профили пользователей должны использовать минимальную umask 0 2 7, т. е. полный доступ для владельца, read и execute для владельца группы, нет доступа для всех остальных пользователей.

4.1.2. *Учетные записи конечных пользователей*

Учетные записи конечных пользователей запрещены. Должны быть доступны только учетные записи системных администраторов.

4.1.3. *Обновление паролей*

Все пароли должны обновляться в соответствии с Политикой использования паролей.

4.1.4. *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.

4.2. Удаленный доступ

4.2.1. *Использование r-команд BSD*

Использование этих команд строго запрещено.

4.2.2. *Удаленный доступ для привилегированных пользователей и администраторов*

Для организации такого доступа необходимо использовать механизмы шифрования. Все другие протоколы, передающие пароли открытым текстом, запрещены.

4.3. *Приложения*

4.3.1. *Сетевые приложения*

Сетевые приложения должны быть интегрированы и сконфигурированы таким образом, чтобы взлом приложения не привел к взлому самого сервера.

4.3.2. *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.

4.3.3. *Уязвимости программного обеспечения*

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

4.3.4. *Инструменты разработки*

Установка любых средств разработки и отладки, включая, но не ограничиваясь компиляторами и отладчиками, запрещена.

4.4. Целостность системы

4.4.1. *Уменьшение поверхности атак*

Все неиспользуемые сервисы должны быть отключены.

4.4.2. *Файлы управления заданиями*

Все внешние команды, используемые в заданиях, должны использовать абсолютные пути, а не относительные.

4.4.3. *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 проведено расследование.
- Поиск, журналирование и отчеты о новых файлах и директориях, не представленных в базе данных, должны быть автоматизированы и анализироваться администраторами.
- Появление выполняемых или специальных файлов во временных директориях должно быть немедленно обнаружено и проведено расследование.

4.4.4. *Журналирование*

Журналы активности приложений и системы должны храниться минимум один месяц на локальных носителях информации. Журналы должны храниться минимум шесть месяцев на внешних носителях информации.

Журналы для систем типа серверов аутентификации удаленных пользователей должны храниться на внешних носителях информации в течение одного года.

4.4.5. *Синхронизация времени*

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

4.4.6. *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.

4.4.7. *Сервисы каталогов*

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

4.4.8. *Уязвимости программного обеспечения*

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

Подход компании Sun Microsystems

По мнению 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», т. е. 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 следующих подразделений компании:

- 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.

Структура политики безопасности

Рекомендуется следующая структура политики безопасности:

- описание основных целей и задач защиты информации;
- определение отношения руководства компании к политике безопасности;
- обоснование путей реализации политики безопасности;
- определение роли 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 с помощью которых достигается выполнение этих требований безопасности. Для этого в политике безопасности должны быть определены показатели и критерии защищенности активов компании в соответствии с которыми будут приобретаться и настраиваться соответствующие 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 быть реализована в соответствующих процедурах, руководствах и стандартах безопасности. Эти стандарты, процедуры и руководства обеспечивают детальную интерпретацию положений поли-

тики 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 требований политики безопасности.

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, определение 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 необходимо воспользоваться концепцией управления информационными рисками. В теории управления финансами категория риска определяется следующим образом:

$$R = H \times P.$$

Здесь H — денежная оценка ущерба в результате инцидента, а P — вероятность инцидента.

Представим, например, защиту источника питания хранилища данных некоторого коммерческого банка. Источник питания стоит $10 000 000. 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 $3 000, то риск составит 30 центов. То есть риск взлома банковского счета может в 30 раз быть выше риска потери источника питания стоимостью 10 млн долларов.

В основном, конечно, задача управления рисками не заключается в определении риска исключительно количественно с высокой точностью и достоверностью. Здесь достаточно просто понимание природы риска и определение такой метрики риска, которая позволяет *измерять, сравнивать, наблюдать и оптимизировать* остаточные риски компании, и тем

самым определять 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, т. е. все системы контроля доступа, межсетевые экраны, криптосистемы, управления ключами и другие средства защиты информации должны работать как единое целое.

Обоснованное доверие

Доверие — основа всех утверждений 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

Определение принципов обеспечения информационной безопасности является первым важным шагом при разработке политики безопасности так как они определяют сущность организации режима информационной безопасности компании. К названным принципам безопасности относятся:

- **Принцип ответственности —** ответственность за обеспечение безопасности информационных систем компании должна быть явно определена.
- **Принцип ознакомления —** собственники информации, пользователи информационных систем, а также клиенты и партнеры по бизнесу должны быть проинформированы о правилах утвержденной политики безопасности компании, а также степени ответственности при работе с конфиденциальной информацией компании.
- **Принцип этики —** обеспечение информационной безопасности компании должно осуществляться в соответствии со стандартами этики, применимыми к деятельности компании.
- **Принцип комплексности —** политики, стандарты, практики и процедуры безопасности должны охватывать все уровни обеспечения безопасности: нормативно-методический, экономический, технологический, технический и организационно-управленческий.
- **Принцип экономической оправданности —** обеспечение безопасности компании должно быть экономически оправданным.

- **Принцип интеграции** — политики, стандарты, практики и процедуры безопасности должны быть скоординированы и интегрированы между собой.
- **Принцип своевременности** — обеспечение безопасности компании должно позволять своевременно реагировать и парировать угрозы безопасности.
- **Принцип пересмотра** — регулирующие документы в области безопасности компании должны периодически пересматриваться и дополняться.
- **Принцип демократичности** — обеспечение безопасности информационных активов компании должно осуществляться в соответствии с принятыми нормами демократии.
- **Принцип сертификации и аккредитации** — информационные системы компании и компания в целом должны быть сертифицированы на соответствующие требования безопасности. Сотрудники компании, ответственные за организацию режима информационной безопасности должны быть сертифицированы и внутренними приказами руководства компании допущены к исполнению своих должностных обязанностей.
- **Принцип парирования злоумышленника** — стратегии и тактики обеспечения безопасности, а также соответствующие технические решения должны быть адекватны уровню нападения различного рода злоумышленников.
- **Принцип наименьших привилегий** — сотрудникам компании должны быть предоставлены привилегии, необходимые для выполнения служебных обязанностей, и более того.
- **Принцип разделения привилегий** — привилегии сотрудников компании должны быть распределены таким образом, чтобы предупредить возможность нанесения ими умышленного или непреднамеренного ущерба критически важным информационным системам компании.
- **Принцип непрерывности** — должна быть обеспечена требуемая непрерывность бизнеса компании в случае чрезвычайных ситуаций.
- **Принцип 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 про-

граммных и аппаратных решений. В добавлении 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, подтверждающей сам факт ознакомления с политикой безопасности, а также означающей, что все требования политики безопасности понятны и их обязуются выполнить.

Пересмотр политики безопасности

Необходимо организовать процесс периодического пересмотра политики безопасности для того, чтобы ее положения не устаревали. Этот процесс должен включать некоторую форму механизма внесения изменений, чтобы при изменении операционного окружения в компании они могли быть быстро отражены в политике безопасности. 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 внесение изменений при необходимости.

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 потребовать установки дополнительных криптопровайдеров сторонних производителей, в то время как другие требования политики безопасности могут быть реализованы встроенной в JAVA библиотекой Security API. Необходимо 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 17799:2002. При этом рекомендуются следующие этапы разработки политики безопасности.

1. Определение основных целей и задач развития бизнеса компании.

Определение основных целей и задач развития бизнеса компании важно для определения области применения политики безопасности. Очень важно получить 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, должна включать представителей отдела защиты информации, юридического отдела, отдела кадров, отдела внутреннего аудита и качества, отдела системных операций и отдела программных разработок.

2. Описание основных принципов безопасности.

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

3. 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 необходимости степени защищенности этих ресурсов.

4. Анализ информационных потоков.

Цель анализа информационных потоков — определить все критичные точки обработки данных компании. Например, в системе обработки транзакций, данные могут перемещаться через веб-браузеры, сервера 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.

5. 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 их последствия, а также стоимость восстановления.

6. Определение сервисов безопасности.

Следующим этапом является определение сервисов безопасности компании, например, журналирование, авторизация, идентификация, ау-

тентификация и пр. Определение сервисов безопасности позволяет правильно выработать политику безопасности.

7. Создание шаблона политики безопасности.

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

8. 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:

1) Категорирования информационных ресурсов.
2) Доступа к информационным ресурсам.
3) Использования паролей.
4) Использования шифрования и управления ключами.
5) Сетевой безопасности.
6) Физической безопасности.
7) Работы с электронной почтой.
8) Реагирования на инциденты в области безопасности.
9) Мониторинга и аудита безопасности.
10) Межсетевого экранирования.
11) Антивирусной защиты.
12) Управления системами и сетями.
13) Контроля действий сотрудников.
14) Резервного копирования.
15) Допуска сторонних организаций.
16) Разработки и внедрения приложений.
17) Управления конфигурациями.
18) Обнаружения вторжений и пр.

Пример шаблона политики безопасности

Разделы политики безопасности

Делается краткий обзор основных разделов политики безопасности.

Заявление о назначении

Почему нужна политика.

Область действия

Какова область действия политики безопасности?

Заявление политики

Каковы специфические особенности политики?

Обязанности

Кто и что должен делать?

Аудитория

На кого ориентирована политика безопасности?

Внедрение

Кто отвечает за внедрение политики?
Кто отвечает за нарушения политики безопасности?

Исключения

Описание возможных исключений.

Другие соглашения

Описание дополнительных соглашений.

Доведение политики до сотрудников

Кто за это отвечает?
Каков процесс доведения?

Процесс пересмотра и обновления политики

Кто за это отвечает?
Что представляет собой процесс пересмотра?
По каким причинам это происходит?
Периодичность пересмотра политики безопасности (например, ежегодно или при возникновении проблемы)

Осуществление политики

Кто за это отвечает?
Как это выполняется?

Мониторинг соответствия

Как выполняется мониторинг соответствия политики безопасности требованиям бизнеса?

Наилучший способ проиллюстрировать подход Sun — провести анализ примера политики безопасности. Давайте рассмотрим и прокомментируем следующий пример политики безопасности.

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 к 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 этой секции 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, невозможности предоставлять услуги, поддерживать целостность, конфиденциальность и доступность данных и пр.

Преднамеренные действия сотрудников компании, которые привели к нарушению настоящей политики безопасности приведут к дисциплинарным наказаниям. 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 компании, 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

Описывает подход к хранению информации.

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

Уничтожение носителей информации

Описывает подход к уничтожению носителей информации.

Уничтожение носителей информации осуществляется в соотвествии с процедурой Отдела безопасности компании.

Утверждения политики безопасности

Эта секция содержит детальное описание основных положений политики информационной безопасности компании.

Цели

Цели описывают административные задачи политики и почему она необходима.

Цель 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

Содержит описание состава и структуры информационной системы компании.

Обязанности по защите информации

Определение обязанностей компании по защите информации является важной задачей.

К названным обязанностям относятся:

- 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/или групп сотрудников.

К другим обязанностям относятся:

- Все партнеры компании, вендоры, провайдеры и сторонние организации которые участвуют в процессе обработки конфиденциальной информации компании, должны руководствоваться четко документированной политики безопасности для сторонних организаций.
- Все партнеры компании, вендоры, провайдеры и сторонние организации, которые имеют доступ к конфиденциальной информации компании, должны подписать соглашение о 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 для управления пользовательскими идентификаторами на рабочих станциях списками контроля доступа на рабочих местах компании, для сбора и анализа 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 актуальности политики безопасности.

Обязанность по периодическому пересмотру политики безопасности возлагается на службу безопасности. В связи с быстро изменяющимися информационными технологиями, политика безопасности должна пересматриваться не реже одного раза в год. Как минимум, высшее руководство компании, сотрудники службы безопасности, отдела системного администт-

рирования и юридического отдела должны входить в группу по пересмотру политики безопасности компании.

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 классифицируется на:

Информацию открытого доступа или публичную информацию — информацию, 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 ценную информацию или собственность компании — информацию, не подлежащую разглашению за пределами компании. Эта информация защищается компанией по требованиям контрактов или законодательных актов. Если такая информация будет разглашена, то она потеряет свою экономическую ценность. Большинство информации в компании должно попадать в эту категорию. Копирование и передача такой информации может быть разрешена только определенному списку сотрудников внутри компании. Разглашение такой информации за пределы компании должно осуществляться только с письменного разрешения лица, ответственного за надлежащее обращение с названной информацией (пример: политики компании, планы продаж, исходный код программы).

Конфиденциальную информацию компании — информацию, 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).

Конфиденциальную информацию клиентов и партнеров компании — информацию 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. Такой тип информации может храниться в системах обработки информации компании, но не иметь владельца (пример: банковские реквизиты клиента, ключи шифрования).

Публичную информацию клиентов и партнеров компании — информацию 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.

Подход компании Cisco Systems

По мнению 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.

Создание политик использования

Компания Cisco рекомендует создать политики использования, которые описывают роли и обязанности сотрудников компании для надлежащей защиты конфиденциальной информации компании. 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 использовании для партнеров, чтобы проинформировать партнеров компании о том, какая информация им доступна. При этом следует четко описать любые действия которые будут восприниматься как враждебные, а также описать возможные способы реагирования при обнаружении таких действий.

В заключении необходимо создать политику допустимого использования для администраторов, для того чтобы описать процедуры администрирования учетных записей сотрудников, внедрение политики и проверки привилегий. При этом, если компания имеет определенную политику относительно использования паролей или категорирования информации, то нужно упомянуть здесь эти политики. 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 риска**. 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 риска**. 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 риска**. 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 каждому из перечисленных устройств: сетевые устройства, устройства мониторинга сети, сервера аутентификации (TACACS+ и RADIUS), почтовые сервера, файловые сервера, сервера сетевых приложений(DNS и DHCP), сервера баз данных (Oracle, MS SQL Server), персональные компьютеры и другие устройства.

При этом считается, что сетевое оборудование, такое как коммутаторы, маршрутизаторы, DNS и DHCP сервера в случае компрометации могут быть использованы для дальнейшего проникновения в сеть и, поэтому, должны относиться к группе среднего или высокого рисков. Возможное повреждение этих устройств может привести к прекращению работы всей сети. Такие инциденты могут нанести серьезный ущерб компании.

После определения уровней риска необходимо определить роли пользователей 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 рисков и типов доступа требуемых для каждой сети позволяет сформировать некоторую матрицу безопасности (см. табл. 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 1

Матрица безопасности Cisco

Система	Описание	Уровень риска	Типы пользователей
ATM коммутаторы	Основные сетевые устройства	Высокий	Администраторы для конфигурирования (только персонал поддержки); все другие для использования в качестве транспорта
Сетевые маршрутизаторы	Сетевые устройства распределения	Высокий	Администраторы для конфигурирования (только персонал поддержки); все другие для использования в качестве транспорта
Коммутаторы доступа	Сетевые устройства доступа	Средний	Администраторы для конфигурирования (только персонал поддержки); все другие для использования в качестве транспорта
ISDN или dial up сервера	Сетевые устройства доступа	Средний	Администраторы для конфигурирования (только персонал поддержки); партнеры и привилегированные пользователи для специального доступа
Межсетевые экраны	Сетевые устройства доступа	Высокий	Администраторы для конфигурирования (только персонал поддержки); все другие для использования в качестве транспорта
Сервера DNS и DHCP	Сетевые приложения	Средний	Администраторы для конфигурирования; пользователи для повседневного использования
Внешние почтовые сервера	Сетевое приложение	Низкий	Администраторы для конфигурирования; Все другие как транспорт для передачи почты между Интернетом и внутренним почтовым сервером
Внутренний почтовый сервер	Сетевое приложение	Средний	Администраторы для конфигурирования; Все другие для повседневного использования
Сервер базы данных Oracle	Сетевое приложение	Средний или высокий	Администраторы для конфигурирования; привилегированные пользователи для обновления информации; сотрудники компании для доступа к информации; все остальные имеют частичный доступ к информации

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. Как минимум, необходим 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, и 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 предупреждению 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 могут иметь потенциальное

воздействие на состояние безопасности сети. Политика безопасности компании должна определять специфические требования конфигурации безопасности описанные не техническими терминами. Другими словами, вместо определения требования, например как «не разрешены внешние ftp соединения во внутреннюю сеть» нужно определить это требование как «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 о 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 не соответствия, 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 следующие изменения:

- любые изменения в конфигурации межсетевых экранов;
- любые изменения в списках контроля доступа;
- любые изменения в конфигурации SNMP;
- любые изменения или обновления программного обеспечения, версия которого отличается от разрешенного списка 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 нарушения безопасности. Анализ угроз и информационных рисков позволяет определить требуемый уровень полноты мониторинга безопасности сети компании. В дальнейшем при проведении процесса утверждения изменений безопасности каждый раз проверяется значимость выявленных угроз сети. Оценивания эти угрозы определяется объект мониторинга 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 отслеживать все изменения в настройках конфигурации межсетевого экрана. Это означает, что 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.

Следуя этому примеру, 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 необходимости получения разрешения от руководства.

Отметим, что существует две основных причины для сбора и хранения информации об атаках: для определения последствий реализации атаки и для расследования и преследования злоумышленников. Тип информации и способ ее сбора зависит от этих целей.

Для определения последствий нарушения безопасности рекомендуется проделать 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.

- Хранить и просматривать файлы журналов устройств безопасности и сетевого мониторинга, так как они часто являются ключом в определении метода атаки.

Если необходимо провести юридические действия, необходимо уведомить руководство компании 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, то необходимо 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. Здесь необходимо регулярно обращаться на веб-сайты различных независимых аналитических центров, например CERT или SANS, за полезными советами и рекомендации 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 требования 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.

Рассмотрим возможности подхода компании Cisco на следующем примере.

Политика 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 — политики) 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 IT 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 целями и задачами бизнеса.
- Юристов компании и аудиторов, которые обеспокоены сохранением репутации компании и ответственностью компании перед клиентами и партнерами.

Область действия

Политика является частью программы компании по обеспечению безопасности информационных активов компании. 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 операций информационных систем.
- 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 должен проводить аудит сети на регулярной основе и документировать 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 должен быть проведен аудит после установки и подключения к сети нового сетевого оборудования и компьютеров.

Обучение сотрудников

Ознакомление с политикой должно осуществляться 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 должны 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 входит в их служебные обязанности.

Требования по соответствию

Сотрудники обязаны выполнять все требования этой политики и любых последующих версий этой политики. 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 любому 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 и должны иметь длину, как минимум, восемь символов;
- изменять пароли ежеквартально;
- не записывать пароли;
- не сообщать пароли кому бы то ни было.

Руководство по аутентификации

Компания будет 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, в то же время понимая, что такие подключения подвергают компанию серьезному риску.

Политика доступа в Интернет определяет руководства 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, как минимум, состоящий из пограничного маршрутизатора и защищенного компьютера, должен быть использован для защиты от несанкционированного доступа к внутренней сети компании из Интернет. Должны быть разработаны 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 основываясь на уровне доверия определяемым руководителем сотрудника. Компания старается балансировать между прозрачным доступом сотрудника к ресурсам и безопасностью сети. Компания устанавливает 5 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.

Удаленный доступ является расширением внутренней сети компании, обеспечивающий потенциальный доступ к конфиденциальной информации компании. Поэтому сотрудники, получающие такой вид доступа, несут повышенный уровень ответственности за то, что только они имеют доступ к ресурсам компании. Любой компьютер, получающий 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, кому необходим удаленный доступ в сеть компании с мобильных компьютеров, получают такой доступ через сервера 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. Такой доступ обязательно должен использовать 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 компанию 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, должны подписать 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 должны совместно разработать детальную процедуру описания всех инцидентов связанных с безопасностью и содержащую планы по обеспечению непрерывности бизнеса. Процедура описания инцидентов должна быть написана в виде книги 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 в этой политике.

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 иметь следующие возможности:

- Системы обнаружения вторжений должны иметь возможность и соответствующую производительность для мониторинга демилитаризованной зоны.
- Системы обнаружения вторжений должны быть реализованы в виде многоуровневой архитектуры для быстрого и беспроблемного внедрения в растущую сеть.
- Центральная станция управления должна иметь возможность удаленного администрирования системы обнаружения вторжений через интуитивно-понятный графический интерфейс, интегрированный в систему управления сетью. Это гарантирует целостность внедрения политики безопасности на уровне компании.
- Станция управления должна иметь возможность сохранять события в базе данных. Должна быть возможность сохранения информации об источнике атаки, типе атаки, цели атаки и времени атаки для последующего детального исследования.

Процедура реагирования на инциденты

Начальник отдела информационных систем должен создать детальную процедуру реагирования на инциденты, и этот документ должен пересматриваться и обновляться по мере необходимости 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 этот документ. Процедура реагирования на инциденты должна определять реакцию компании при возникновении инцидента так, что в случае возникновения инцидента, выделенные ресурсы приступили к нейтрализации и уменьшении проблем, а не решали бы как с ней бороться. В процедуре реагирования на инциденты должны быть описаны следующие моменты:

1. Подготовка и планирование — персонал отдела информационных систем должен минимум 16 часов ежегодно обучаться обнаружению и нейтрализации инцидентов. Процедура должна определять тип и длительность тренингов.
2. Определение инцидентов — системные администраторы должны мониторить системы обнаружения вторжений несколько раз в день. Системные журналы должны просматриваться 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 как предлагается в RFC 2196, «Site Security Handbook».
3. Обработка инцидента — процедура реагирования на инциденты должна определять, 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.
4. Документирование — должен быть создан отчет об инциденте под руководством директора службы информационных технологий, который должен затрагивать следующие вопросы:

- инвентаризация ценности затронутых атакой систем;
- описание атаки;
- пересмотр Политики сетевой безопасности, при необходимости;
- поиск и наказание злоумышленников.

Контактные лица

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 операций информационных систем	• 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 к 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

Подход компании Microsoft

Компания Microsoft обладает сложной корпоративной инфраструктурой, которая состоит из 5 000 серверов Windows Server 2003 (из них 800 серверов приложений). В штате компании работает более 55 000 сотрудников. Сотрудники очень хорошо готовы технически и 95 % из них имеют администраторские права на своих компьютерах. Более чем 300 000 компьютеров компании расположены в 400 представительствах по всему миру, используется более 1 600 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 30 000 партнеров.

Уникальная инфраструктура по разработке продуктов, тестированию и поддержке, исходный код продуктов требуют особой защиты. Ежемесячно на сеть компании осуществляется свыше 100 000 попыток вторжения. В почтовую систему ежемесячно поступает свыше 125 000 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;
- тактическая приоритезация деятельности по уменьшению рисков.

Фундаментом для дизайна, разработки и работе защищенных систем являются принципы безопасности, разделенные на несколько категорий:

Категория	Принцип безопасности
Организационная: направлена на получение поддержки руководства по управлению рисками и ознакомлению 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

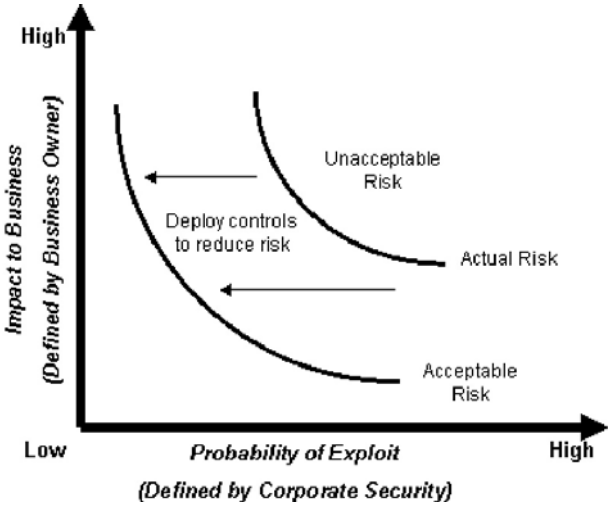

Рис. 4. Модель управления рисками Corporate Security Group

Для обеспечения информационной безопасности Corporate Security Group использует подход по управлению информационными рисками. 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 (рис. 4) представляет собой комбинацию различных подходов, таких как количественный анализ рисков, анализ возврата инвестиций в безопасность, качественный анализ рисков, а также подходы лучших практик.

Для реализации этого подхода Corporate Security Group разработала структуру, которая основана на традиционной модели управления информационными рисками.

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

1. **Оценка информационных рисков**. В соответствии с методологией.
2. **Разработка политики безопасности**. Разработка политики безопасности по уменьшению, уклонению и предупреждению рисков.

Рис. 5. Этапы управления информационными рисками

3. **Внедрение средств защиты**. Объединение сотрудников, процессов и технологий для уменьшения рисков, основанных на анализе соотношения цена/качество.
4. **Аудит безопасности и измерение текущей защищенности**. Мониторинг, аудит безопасности и измерение защищенности информационных систем компании.

Как видно из рис. 5, разработка политики является одним из этапов по управлению информационными рисками.

Методология, используемая при разработке политики, базируется на стандарте ISO 17799:2002 (BS 7799).

Рекомендуемая компанией Microsoft политика безопасности включает в себя:

- определение целей безопасности;
- важность обеспечения безопасности;
- 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 требуемого 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 вопросам безопасности;
- консультирование персонала по вопросам безопасности;
- определение бюджета и требуемых ресурсов по обеспечению безопасности.

Подход компании Symantec

По мнению Symantec, руководящие документы в области безопасности (политики, стандарты, процедуры и метрики безопасности) являются основой любой успешной программы обеспечения информационной безопасности компании (см. рис. 6).

При этом различия политик, процедур, стандартов и руководств безопасности проявляются в следующем (см. рис. 7).

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.

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.

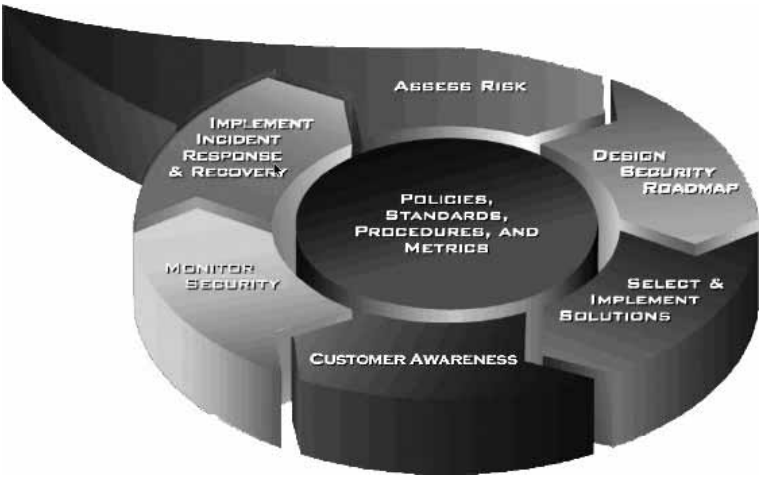

Рис. 6. Компоненты программного обеспечения информационной безопасности компании

- **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 угрозы 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, потери 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.

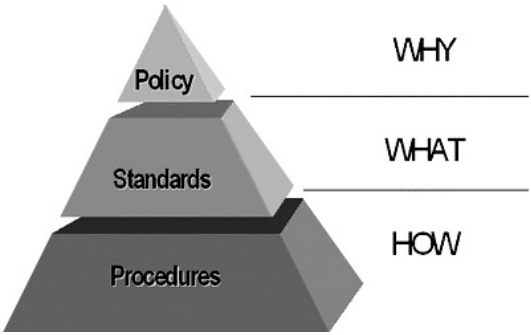

Рис. 7. Различия политики, стандартов и процедур безопасности

- **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, ответственных за информационные системы и защиту информации. Компания может потребовать от сотрудников подписи о том, что они с ознакомлены с политикой безопасности и обязуются соблюдать ее требования. Ответственность реализуется с помощью определения:
  1. Процедуры соответствия — для определения ответственности за выполнение требований политики безопасности.
  2. Состава и структуры подразделения офицеров безопасности — определяет сотрудников которые несут ответственность за обеспечение режима информационной безопасности. Здесь необходимо предусмотреть проблемы связанные с конфликтом интересов.
  3. 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:

- 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 размер политики информационной безопасности не должен превышать 2 страниц.

Реализация политики достигается использованиям 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 тоже 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 17799:2002.

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 соответствие 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:

1. Цель процедуры:
   - для соответствия какому стандарту она разработана;
   - для чего нужна процедура.
2. 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.

3. Определение процесса:
   - введение в процесс (описание);
   - детальное описание процесса (как, когда, что, критерии успеха, виды отчетов, взаимодействие с другими процессами).
4. Контрольный список процесса.
5. Проблемы процесса (действия при возникновении проблем).

Подход SANS (www.sans.org)

Организация SANS выработала свой подход в понимании понятия 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:

1. Утверждение руководства о поддержке политики информационной безопасности.
2. Основные политики компании.
3. Функциональные политики.
4. Обязательные стандарты (базовые).
5. Рекомендуемые руководства.
6. Детализированные процедуры.

Стандарты детализируют различие 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:

1. Направленные на решение конкретной проблемы. Примерами таких политик могут служить политика по найму персонала, политика использования паролей, политика использования Internet.
2. 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.
3. Применяемые к конкретной среде. Например, каждая операционная система требует отдельного стандарта по ее настройке.

Рекомендуемые компоненты политики безопасности:

1. Цель.
2. Область действия.
3. Утверждение политики.
4. История документа.
5. Необходимость политики.
6. Какие политики отменяет.
7. Действия по выполнению политики.
8. Ответственность.
9. Исключения.
10. 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 антивирусной защиты лаборатории.

Рассмотрим возможности подхода SANS на следующем примере.

Пример политики аудита безопасности

1.0. *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.

2.0. *Область действия*

Политика охватывает все компоненты информационных систем компании. Аудиторы не будут проводить атаки класса «Отказ в обслуживании».

3.0. *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.) которая создается, передается и хранится в системе;

- доступ в помещения (лаборатории, офисы, серверные и т. д.);
- доступ к сетевому трафику.

3.1. *Управление сетью*

Если в компании доступ из корпоративной сети в Internet 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.

3.2. *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.

3.3. *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.

3.4. *Период сканирования*

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

4.0. *Процесс оценки рисков*

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

5.0. *Ответственность*

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

Литература

1. *Петренко С. А., Петренко А. А.* Аудит безопасности Intranet. М.: ДМК Пресс, 2002. 416 с.
2. *Петренко С. А., Симонов С. В.* Управление информационными рисками. Экономически оправданная безопасность. М.: ДМК Пресс, 2004. 400 с.
3. *Петренко С. А., Курбатов В. А.* Политики информационной безопасности. М.: ДМК Пресс, 2006. 400 с.