## ТЕМА: «ПОЛИТИКА БЕЗОПАСНОСТИ»

Политика безопасности определяет стратегию управления в области ин формационной безопасности, а также меру внимания и количество ресурсов которые считает целесообразным выделить руководство. Политика безопасно сти строится на основе анализа рисков, которые признаются реальными дл ИС организации. Когда проведен анализ рисков и определена стратегия защи ты, составляется программа, реализация которой должна обеспечить информа ционную безопасность. Под эту программу выделяются ресурсы, назначаются ответственные, определяется порядок контроля выполнения программы и т. п. Политика безопасности организации должна иметь структуру краткого, легк понимаемого документа высокоуровневой политики, поддерживаемого кон кретными документами специализированных политик и процедур безопасно сти.

Высокоуровневая политика безопасности должна периодически пере сматриваться, гарантируя тем самым учет текущих потребностей организации Документ политики составляют таким образом, чтобы политика была относи тельно независимой от конкретных технологий, в этом случае документ не по требуется изменять слишком часто. Для того чтобы познакомиться с основны ми понятиями политики безопасности рассмотрим в качестве конкретног примера гипотетическую локальную сеть, принадлежащую некоторой органи зации, и ассоциированную с ней политику безопасности. Политика безопасно сти обычно оформляется в виде документа, включающего такие разделы, ка описание проблемы, область применения, позиция организации, распределе ние ролей и обязанностей, санкции и др.

Описание проблемы. Информация, циркулирующая в рамках локально сети, является критически важной. Локальная сеть позволяет пользователя совместно использовать программы и данные, что увеличивает угрозу безо пасности. Поэтому каждый из компьютеров, входящих в сеть, нуждается в бо лее сильной защите. Эти повышенные меры безопасности и являются темо данного документа, который призван продемонстрировать сотрудникам орга низации важность защиты сетевой среды, описать их роль в обеспечении безо пасности, а также распределить конкретные обязанности по защите информа ции, циркулирующей в сети.

Область применения. В сферу действия данной политики попадают вс аппаратные, программные и информационные ресурсы, входящие в локальну сеть предприятия. Политика ориентирована также на людей, работающих с се тью, в том числе на пользователей, субподрядчиков и поставщиков.

Позиция организации. Основные цели — обеспечение целостности, дос тупности и конфиденциальности данных, а также их полноты и актуальности К частным целям относятся: • обеспечение уровня безопасности, соответст вующего нормативным документам;• следование экономической целесообраз ности в выборе защитных мер (расходы на защиту не должны превосходит предполагаемый ущерб от нарушения информационной безопасности); • обес печение безопасности в каждой функциональной области локальной сети;

обеспечение подотчетности всех действий пользователей с информацией и ре сурсами; • обеспечение анализа регистрационной информации; • предоставле ние пользователям достаточной информации для сознательного поддержани режима безопасности; • выработка планов восстановления после аварий иных критических ситуаций для всех функциональных областей с целью обес печения непрерывности работы сети; • обеспечение соответствия с имеющи мися законами и общеорганизационной политикой безопасности.

Распределение ролей и обязанностей. За реализацию сформулированны выше целей отвечают соответствующие должностные лица и пользователи се ти. Руководители подразделений отвечают за доведение положений политик безопасности до пользователей и за контакты с ними. Администраторы ло кальной сети обеспечивают непрерывное функционирование сети и отвечаю за реализацию технических мер, необходимых для проведения в жизнь поли тики безопасности. Они обязаны: • обеспечивать защиту оборудования ло кальной сети, в том числе интерфейсов с другими сетями; • оперативно и эф фективно реагировать на события, таящие угрозу, информировать администт раторов сервисов о попытках нарушения защиты; • использовать проверенны средства аудита и обнаружения подозрительных ситуаций, ежедневно анали зировать регистрационную информацию, относящуюся к сети в целом и файловым серверам в особенности; • не злоупотреблять своими полномочия ми, так как пользователи имеют право на тайну; • разрабатывать процедуры подготавливать инструкции для защиты локальной сети от вредоносного про граммного обеспечения, оказывать помощь в обнаружении и ликвидации вре доносного кода; • регулярно выполнять резервное копирование информации хранящейся на файловых серверах; • выполнять все изменения сетевой аппа ратно-программной конфигурации; • гарантировать обязательность процедур идентификации и аутентификации для доступа к сетевым ресурсам, выделят пользователям входные имена и начальные пароли только после заполнени регистрационных форм; • периодически производить проверку надежност защиты локальной сети, не допускать получения привилегий неавторизован ными пользователями.

Администраторы сервисов отвечают за конкретные сервисы, и в частно сти за построение защиты в соответствии с общей политикой безопасности Они обязаны: • управлять правами доступа пользователей к обслуживаемы объектам; • оперативно и эффективно реагировать на события, таящие угрозу оказывать помощь в отражении угрозы, выявлении нарушителей и предостав лении информации для их наказания; • регулярно выполнять резервное копи рование информации, обрабатываемой сервисом; • выделять пользователя входные имена и начальные пароли только после заполнения регистрационны форм; • ежедневно анализировать регистрационную информацию, относящую ся к сервису, регулярно контролировать сервис на предмет вредоносного про граммного обеспечения; • периодически производить проверку надежност защиты сервиса, не допускать получения привилегий неавторизованным пользователями.

Пользователи работают с локальной сетью в соответствии с политико безопасности, подчиняются распоряжениям лиц, отвечающих за отдельные ас пекты безопасности, ставят в известность руководство обо всех подозрительн ных ситуациях. Они обязаны: • знать и соблюдать законы, правила, принятые данной организации, политику безопасности, процедуры безопасности, ис пользовать доступные защитные механизмы для обеспечения конфиденциальн ности и целостности своей информации; • использовать механизм защит файлов и должным образом задавать права доступа; • выбирать качественны пароли, регулярно менять их, не записывать пароли на бумаге, не сообщать и другим лицам; • информировать администраторов или руководство о наруше ниях безопасности и иных подозрительных ситуациях;• не использовать сла бости в защите сервисов и локальной сети в целом, не совершать неавторизо ванной работы с данными, не создавать помех другим пользователям; • всегд сообщать корректную идентификационную и аутен-тификационную информа цию, не пытаться работать от имени других пользователей; • обеспечивать ре зервное копирование информации с жесткого диска своего компьютера; знать принципы работы вредоносного программного обеспечения, пути ег проникновения и распространения, знать и соблюдать процедуры для преду преждения проникновения вредоносного кода, его обнаружения и уничтоже ния; • знать и соблюдать правила поведения в экстренных ситуациях, последо вательность действий при ликвидации последствий аварий.

Санкции. Нарушение политики безопасности может подвергнуть ло кальную сеть и циркулирующую в ней информацию недопустимому риску Случаи нарушения безопасности со стороны персонала должны оперативн рассматриваться руководством для принятия дисциплинарных мер вплоть д увольнения.

Дополнительная информация. Конкретным группам исполнителей могу потребоваться для ознакомления дополнительные документы, в частности, до кументы специализированных политик и процедур безопасности, а также дру гие руководящие указания. Необходимость в дополнительных документах по литик безопасности в значительной степени зависит от размеров и сложност организации. Для достаточно большой организации могут потребоваться в до полнение к базовой политике специализированные политики безопасности Организации меньшего размера нуждаются только в некотором подмножеств специализированных политик. Многие из этих документов поддержки могу быть краткими — объемом в одну-две страницы.

Управленческие меры обеспечения информационной безопасности

Главной целью мер, предпринимаемых на управленческом уровне, явля ется формирование программы работ в области информационной безопасно сти и обеспечение ее выполнения путем выделения необходимых ресурсов осуществления регулярного контроля состояния дел. Основой этой программ является многоуровневая политика безопасности, отражающая комплексны подход организации к защите своих ресурсов и информационных активов.

С практической точки зрения политики безопасности можно разделит на три уровня: верхний, средний и нижний.

Верхний уровень политики безопасности определяет решения, затраги
вающие организацию в целом. Эти решения носят весьма общий характер
исходят, как правило, от руководства организации. Такие решения могу
включать в себя следующие элементы: • формулировку целей, которые пре
следует организация в области информационной безопасности, определени
общих направлений в достижении этих целей; • формирование или пересмот
комплексной программы обеспечения информационной безопасности, опреде
ление ответственных лиц за продвижение программы; • обеспечение матери
альной базы для соблюдения законов и правил; • формулировку управленче
ских решений по вопросам реализации программы безопасности, которы
должны рассматриваться на уровне организации в целом.

Политика безопасности верхнего уровня формулирует цели организаци
в области информационной безопасности в терминах целостности, доступно
сти и конфиденциальности. Если организация отвечает за поддержание крити
чески важных баз данных, на первом плане должна стоять целостность дан
ных. Для организации, занимающейся продажами, важна актуальность инфор
мации о предоставляемых услугах и ценах, а также ее доступность максимальн
ному числу потенциальных покупателей. Режимная организация в первую
очередь будет заботиться о конфиденциальности информации, т. е. о ее защит
от НСД. На верхний уровень выносится управление ресурсами безопасности
координация использования этих ресурсов, выделение специального персона
ла для защиты критически важных систем, поддержание контактов с другим
организациями, обеспечивающими или контролирующими режим безопасно
сти. Политика верхнего уровня должна четко определять сферу своего влия
ния. В нее могут быть включены не только все компьютерные системы орга
низации, но и домашние компьютеры сотрудников, если политика регламен
тирует некоторые аспекты их использования. Возможна и такая ситуация, ко
гда в сферу влияния включаются лишь наиболее важные системы. В политик
должны быть определены обязанности должностных лиц по выработке про
граммы безопасности и по проведению ее в жизнь, т. е. политика может слу
жить основой подотчетности персонала. Политика верхнего уровня имеет дел
с тремя аспектами законопослушности и исполнительской дисциплины. Во
первых, организация должна соблюдать существующие законы. Во-вторых
следует контролировать действия лиц, ответственных за выработку программ
безопасности. В-третьих, необходимо обеспечить исполнительскую дисципли
ну персонала с помощью системы поощрений и наказаний.

Средний уровень политики безопасности определяет решение вопросов
касающихся отдельных аспектов информационной безопасности, но важны
для различных систем, эксплуатируемых организацией. Примеры таких вопро
сов — отношение к доступу в Internet (проблема сочетания свободы получени
информации с защитой от внешних угроз), использование домашних компью
теров и т. д. Политика безопасности среднего уровня должна определять дл
каждого аспекта информационной безопасности следующие моменты:

• описание аспекта — позиция организации может быть сформулирован
в достаточно общем виде, а именно как набор целей, которые преследует орга

низация в данном аспекте; • область применения — следует специфицировать где, когда, как, по отношению к кому и чему применяется данная политик безопасности; • роли и обязанности — документ должен содержать информа цию о должностных лицах, отвечающих за проведение политики безопасност в жизнь; • санкции — политика должна содержать общее описание запрещен ных действий и наказаний за них; • точки контакта — должно быть известно куда следует обращаться за разъяснениями, помощью и дополнительной ин формацией. Обычно «точкой контакта» служит должностное лицо.

Нижний уровень политики безопасности относится к конкретным серви сам. Она включает два аспекта — цели и правила их достижения, поэтому е порой трудно отделить от вопросов реализации. В отличие от двух верхни уровней, рассматриваемая политика должна быть более детальной, т. е. пр следовании политике безопасности нижнего уровня необходимо дать ответ например, на такие вопросы: • кто имеет право доступа к объектам, поддержи ваемым сервисом; • при каких условиях можно читать и модифицировать дан ные; • как организован удаленный доступ к сервису. Политика безопасност нижнего уровня может исходить из соображений целостности, доступности конфиденциальности, но она не должна на них останавливаться. В общем слу чае цели должны связывать между собой объекты сервиса и осмысленные дей ствия с ними. Из целей выводятся правила безопасности, описывающие, кто что и при каких условиях может делать. Чем детальнее правила, чем боле четко и формально они изложены, тем проще поддерживать их выполнени программно-техническими мерами. Обычно наиболее формально задаютс права доступа к объектам.