21. Понятие о политике безопасности: анализ риска; угрозы/вид имость; уязвимость/последствия; учет информационных ценностей

Под политикой безопасности организации понимают совокупность документированных управленческих решений, направленных на защиту информации и ассоциированных с ней ресурсов. Политика безопасности является тем средством, с помощью которой реализуется деятельность в компьютерной информационной системе организации. Вообще политики безопасности определяются используемой компьютерной средой и отражают специфические потребности организации.

Обычно корпоративная информационная система представляет собой сложный комплекс разнородного, иногда плохо согласующегося между собой аппаратного и программного обеспечения: компьютеров, операционных систем, сетевых средств, СУБД, разнообразных приложений. Все эти компоненты обычно обладают собственными средствами защиты, которые нужно согласовать между собой.

Поэтому очень важна эффективная политика безопасности в качестве согласованной платформы по обеспечению безопасности корпоративной системы. По мере роста компьютерной системы и интеграции ее в глобальную сеть необходимо обеспечить отсутствие в системе слабых мест, поскольку все усилия по защите информации могут быть обесценены лишь одной оплошностью.

Можно построить такую политику безопасности, которая будет устанавливать, кто имеет доступ к конкретным активам и приложениям, какие роли и обязанности будут иметь конкретные лица, а также предусмотреть процедуры безопасности, которые четко предписывают, как должны выполняться конкретные задачи безопасности. Индивидуальные особенности работы сотрудника могут потребовать доступа к информации, которая не должна быть доступна другим работникам.

Например, менеджер по персоналу может иметь доступ к частной информации любого сотрудника, в то время как специалист по отчетности может иметь доступ только к финансовым данным этих сотрудников. А рядовой сотрудник будет иметь доступ только к своей собственной персональной информации.

Политика безопасности определяет позицию организации по рациональному использованию компьютеров и сети, а также процедуры по предотвращению и реагированию на инциденты безопасности. В большой корпоративной системе может применяться широкий диапазон разных политик от бизнес-политик до специфичных правил доступа к наборам данных. Эти политики полностью определяются конкретными потребностями организации.

- обеспечение сохранности, целостности информационных ресурсов и предоставление доступа к ним в строгом соответствии с установленными приоритетами и правилами разграничения доступа;
- обеспечение защиты подсистем, задач и технологических процессов от угроз информационной безопасности;
- обеспечение защиты управляющей информации от угроз информационной безопасности;
- обеспечение защиты каналов связи.
- Политика безопасности *определяет стратегию управления в области информационной безопасности*, а также ту меру внимания и количество ресурсов, которые считает целесообразным выделить руководство.
- Политика безопасности строится на основе *анализа рисков*, которые признаются реальными для информационной системы организации. Когда проведен анализ рисков и определена стратегия защиты, составляется программа, реализация которой должна обеспечить информационную безопасность. Под эту программу выделяются ресурсы, назначаются ответственные, определяется порядок контроля выполнения программы и т.п.

- *Для того чтобы ознакомиться с основными понятиями политик безопасности рассмотрим в качестве конкретного примера гипотетическую локальную сеть, принадлежащую некоей организации, и связанную с ней политику безопасности.*
- Политика безопасности организации должна иметь структуру краткого, легко понимаемого документа высокоуровневой политики, поддерживаемого рядом более конкретных документов специализированных политик и процедур безопасности.
- Высокоуровневая политика безопасности должна периодически пересматриваться, чтобы гарантировать, что она учитывает текущие потребности организации. Этот документ составляют таким образом, чтобы политика была относительно независимой от конкретных технологий. В таком случае этот документ политики не потребуется изменять слишком часто.
- Политика безопасности обычно оформляется в виде документа, включающего такие разделы, как: *описание проблемы, область применения, позиция организации, распределение ролей и обязанностей, санкции и др.*
- *Описание проблемы.* Информация, циркулирующая в рамках локальной сети, является критически важной. Локальная сеть позволяет пользователям совместно использовать программы и данные, что увеличивает угрозу безопасности. Поэтому каждый из компьютеров, входящих в сеть, нуждается в более сильной защите. Эти повышенные меры безопасности и являются темой данного документа. Документ преследует следующие цели: продемонстрировать сотрудникам организации важность защиты сетевой среды, описать их роль в обеспечении безопасности, а также распределить конкретные обязанности по защите информации, циркулирующей в сети.
- *Область применения.* В сферу действия данной политики попадают все аппаратные, программные и информационные ресурсы, входящие в локальную сеть предприятия. Политика ориентирована также на людей, работающих с сетью, в том числе на пользователей, субподрядчиков и поставщиков.

Позиция организации. Целью организации является обеспечение целостности, доступности и конфиденциальности данных, а также их полноты и актуальности.

Более частными целями являются:

- обеспечение уровня безопасности, соответствующего нормативным документам;
- следование экономической целесообразности в выборе защитных мер (расходы на защиту не должны превосходить предполагаемый ущерб от нарушения информационной безопасности);
- обеспечение безопасности в каждой функциональной области локальной сети;
- обеспечение подотчетности всех действий пользователей с информацией и ресурсами;
- обеспечение анализа регистрационной информации;
- предоставление пользователям достаточной информации для сознательного поддержания режима безопасности;
- выработка планов восстановления после аварий и иных критических ситуаций для всех функциональных областей с целью обеспечения непрерывности работы сети;
- обеспечение соответствия с имеющимися законами и общеорганизационной политикой безопасности.

Распределение ролей и обязанностей. За реализацию сформулированных выше целей отвечают соответствующие должностные лица и пользователи сети.

- *Руководители подразделений* отвечают за доведение положений политики безопасности до пользователей и за контакты с ними.
- *Администраторы локальной сети* обеспечивают непрерывное функционирование сети и отвечают за реализацию технических мер, необходимых для проведения в жизнь политики безопасности.
- *Администраторы сервисов* отвечают за конкретные сервисы и, в частности, за то, чтобы защита была построена в соответствии с общей политикой безопасности.

- *Пользователи* обязаны работать с локальной сетью в соответствии с политикой безопасности, подчиняться распоряжениям лиц, отвечающих за отдельные аспекты безопасности, ставить в известность руководство обо всех подозрительных ситуациях.
- *Санкции.* Нарушение политики безопасности может подвергнуть локальную сеть и циркулирующую в ней информацию недопустимому риску. Случаи нарушения безопасности со стороны персонала должны оперативно рассматриваться руководством для принятия дисциплинарных мер вплоть до увольнения.
- *Дополнительная информация.* Конкретным группам исполнителей могут потребоваться для ознакомления какие-то дополнительные документы, в частности документы специализированных политик и процедур безопасности, а также другие руководящие указания. Необходимость в дополнительных документах политик безопасности в значительной степени зависит от размеров и сложности организации. Для достаточно большой организации могут потребоваться в дополнение к базовой политике специализированные политики безопасности. Организации меньшего размера нуждаются только в некотором подмножестве специализированных политик. Многие из этих документов поддержки могут быть довольно краткими - объемом в одну - две страницы.

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

Верхний уровень политики безопасности определяет решения, затрагивающие организацию в целом. Эти решения носят весьма общий характер и исходят, как правило, от руководства организации.

Такие решения могут включать в себя следующие элементы:

- формулировка целей, которые преследует организация в области информационной безопасности, определение общих направлений в достижении этих целей;
- формирование или пересмотр комплексной программы обеспечения информационной безопасности, определение ответственных лиц за продвижение программы;
- обеспечение материальной базы для соблюдения законов и правил;
- формулировка управленческих решений по вопросам реализации программы безопасности, которые должны рассматриваться на уровне организации в целом.
- Политика безопасности *верхнего уровня* формулирует цели организации в области информационной безопасности в терминах целостности, доступности и конфиденциальности. Если организация отвечает за поддержание критически важных баз данных, на первом плане должна стоять целостность данных. Для организации, занимающейся продажами, важна актуальность информации о предоставляемых услугах и ценах, а также ее доступность максимальному числу потенциальных покупателей. Режимная организация в первую очередь будет заботиться о конфиденциальности информации, то есть о ее защите от несанкционированного доступа.
- На верхний уровень выносится управление ресурсами безопасности и координация использования этих ресурсов, выделение специального персонала для защиты критически важных систем, поддержание контактов с другими организациями, обеспечивающими или контролирующими режим безопасности.
- Политика верхнего уровня должна четко определять сферу своего влияния. Это могут быть все компьютерные системы организации или даже больше, если политика регламентирует некоторые аспекты использования сотрудниками своих домашних компьютеров. Возможна и такая ситуация, когда в сферу влияния включаются лишь наиболее важные системы.
- В политике должны быть определены обязанности должностных лиц по выработке программы безопасности и по проведению ее в жизнь, то есть политика может служить основой подотчетности персонала.
- Политика верхнего уровня имеет дело с тремя аспектами законопослушности и исполнительской дисциплины. Во-первых, организация должна *соблюдать существующие законы*. Во-вторых, следует *контролировать действия лиц, ответственных за выработку*

программы безопасности. В-третьих, *необходимо обеспечить исполнительскую дисциплину персонала* с помощью системы поощрений и наказаний.

Средний уровень политики безопасности определяет решение вопросов, касающихся отдельных аспектов информационной безопасности, но важных для различных систем, эксплуатируемых организацией.

Примеры таких вопросов - отношение к доступу в Интернет (проблема сочетания свободы получения информации с защитой от внешних угроз), использование домашних компьютеров и т.д.

Политика безопасности среднего уровня должна определять для каждого аспекта информационной безопасности следующие моменты:

- описание аспекта - позиция организации может быть сформулирована в достаточно общем виде как набор целей, которые преследует организация в данном аспекте;
- область применения - следует специфицировать, где, когда, как, по отношению к кому и чему применяется данная политика безопасности;
- роли и обязанности - документ должен содержать информацию о должностных лицах, отвечающих за проведение политики безопасности в жизнь;
- санкции - политика должна содержать общее описание запрещенных действий и наказаний за них;
- точки контакта - должно быть известно, куда следует обращаться за разъяснениями, помощью и дополнительной информацией. Обычно «точкой контакта» служит должностное лицо.

Нижний уровень политики безопасности относится к конкретным сервисам. Эта политика включает в себя два аспекта: цели и правила их достижения, — поэтому ее порой трудно отделить от вопросов реализации. В отличие от двух верхних уровней, рассматриваемая политика должна быть более детальной.

Приведем несколько примеров вопросов, на которые следует дать ответ при следовании политике безопасности нижнего уровня:

- кто имеет право доступа к объектам, поддерживаемым сервисом;
- при каких условиях можно читать и модифицировать данные;
- как организован удаленный доступ к сервису.

Политика безопасности нижнего уровня может исходить из соображений целостности, доступности и конфиденциальности, но она не должна на них останавливаться. В общем случае цели должны связывать между собой объекты сервиса и осмысленные действия с ними.

Из целей выводятся правила безопасности, описывающие, кто, что и при каких условиях может делать. Чем детальнее правила, чем более четко и формально они изложены, тем проще поддержать их выполнение программно-техническими мерами. Обычно наиболее формально задаются права доступа к объектам.

Приведем более детальное описание обязанностей каждой категории персонала.

Руководители подразделений отвечают за доведение положений политики безопасности до пользователей. Они обязаны:

- постоянно держать в поле зрения вопросы безопасности. Следить за тем, чтобы то же самое делали их подчиненные;
- проводить анализ рисков, выявляя активы, требующие защиты, и уязвимые места систем, оценивая размер возможного ущерба от нарушения режима безопасности и выбирая эффективные средства защиты;
- организовать обучение персонала мерам безопасности. Обратить особое внимание на вопросы, связанные с антивирусным контролем;
- информировать администраторов локальной сети и администраторов сервисов об изменении статуса каждого из подчиненных (переход на другую работу, увольнение и т.п.);

- обеспечить, чтобы каждый компьютер в их подразделениях имел хозяина или системного администратора, отвечающего за безопасность и обладающего достаточной квалификацией для выполнения этой роли.

Администраторы локальной сети обеспечивают непрерывное функционирование сети и отвечают за реализацию технических мер, необходимых для проведения в жизнь политики безопасности. Они обязаны:

- обеспечить защиту оборудования локальной сети, в том числе интерфейсов с другими сетями;
- оперативно и эффективно реагировать на события, таящие угрозу. Информировать администраторов сервисов о попытках нарушения защиты;
- использовать проверенные средства аудита и обнаружения подозрительных ситуаций.
- Ежедневно анализировать регистрационную информацию, относящуюся к сети в целом и к файловым серверам в особенности;
- не злоупотреблять своими большими полномочиями. Пользователи имеют право на тайну;
- разработать процедуры и подготовить инструкции для защиты локальной сети от вредоносного программного обеспечения. Оказывать помощь в обнаружении и ликвидации вредоносного кода;
- регулярно выполнять резервное копирование информации, хранящейся на файловых серверах;
- выполнять все изменения сетевой аппаратно-программной конфигурации;
- гарантировать обязательность процедуры идентификации и аутентификации для доступа к сетевым ресурсам. Выделять пользователям входные имена и начальные пароли только после заполнения регистрационных форм;
- периодически производить проверку надежности защиты локальной сети. Не допускать получения привилегий неавторизованными пользователями.

Администраторы сервисов отвечают за конкретные сервисы и, в частности, за то, чтобы защита была построена в соответствии с общей политикой безопасности. Они обязаны:

- управлять правами доступа пользователей к обслуживаемым объектам;
- оперативно и эффективно реагировать на события, таящие угрозу.
- Оказывать помощь в отражении угрозы, выявлении нарушителей и предоставлении информации для их наказания;
- регулярно выполнять резервное копирование информации, обрабатываемой сервисом;
- выделять пользователям входные имена и начальные пароли только после заполнения регистрационных форм;
- ежедневно анализировать регистрационную информацию, относящуюся к сервису. Регулярно контролировать сервис на предмет вредоносного программного обеспечения;
- периодически производить проверку надежности защиты сервиса. Не допускать получения привилегий неавторизованными пользователями.

Пользователи обязаны работать с локальной сетью в соответствии с политикой безопасности, подчиняться распоряжениям лиц, отвечающих за отдельные аспекты безопасности, ставить в известность руководство обо всех подозрительных ситуациях. Они обязаны:

- знать и соблюдать законы, правила, принятые в данной организации, политику безопасности, процедуры безопасности. Использовать доступные защитные механизмы для обеспечения конфиденциальности и целостности своей информации;
- использовать механизм защиты файлов и должным образом задавать права доступа;
- выбирать качественные пароли, регулярно менять их. Не записывать пароли на бумаге, не сообщать их другим лицам;
- информировать администраторов или руководство о нарушениях безопасности и иных подозрительных ситуациях;

- не использовать слабости в защите сервисов и локальной сети в целом. Не совершать неавторизованной работы с данными, не создавать помех другим пользователям;
- всегда сообщать корректную идентификационную и аутентификационную информацию, не пытаться работать от имени других пользователей;
- обеспечивать резервное копирование информации с жесткого диска своего компьютера;
- знать принципы работы вредоносного программного обеспечения, пути его проникновения и распространения. Знать и соблюдать процедуры для предупреждения проникновения вредоносного кода, его обнаружения и уничтожения;
- знать и соблюдать правила поведения в экстренных ситуациях, последовательность действий при ликвидации последствий аварий.

Управленческие меры обеспечения информационной безопасности.

Главной целью мер, предпринимаемых на управленческом уровне, является формирование программы работ в области информационной безопасности и обеспечение ее выполнения путем выделения необходимых ресурсов и осуществления регулярного контроля состояния дел.

Основой этой программы является многоуровневая политика безопасности, отражающая комплексный подход организации к защите своих ресурсов и информационных активов.