ЛЕКЦИЯ 4. ПОЛИТИКА БЕЗОПАСНОСТИ

Под ***целостностью*** подразумевается отсутствие ненадлежащих изменений. Ни одному пользователю АС, в том числе авторизованному, не должны быть разрешены такие изменения данных, которые повлекут за собой их разрушение или потерю.

При рассмотрении вопроса целостности данных используется интегрированный подход, включающий в себя девять теоретических принципов:

1) корректность транзакций;
2) минимизация привилегий;
3) аутентификация пользователей;
4) разграничение функциональных обязанностей;
5) аудит произошедших событий;
6) объективный контроль;
7) управление передачей привилегий;
8) обеспечение непрерывной работоспособности;
9) простота использования защитных механизмов.

Политика безопасности организации — совокупность документированных руководящих принципов, правил, процедур и практических приемов в области безопасности, которые регулируют управление, защиту и распределение ценной информации (рис. 6).

Политика безопасности зависит от:

– конкретной технологии обработки информации;
– используемых технических и программных средств;
– расположения организации.

Политика безопасности устанавливает правила, которые определяют конфигурацию систем, действия служащих организации в обычных условиях и в случае непредвиденных обстоятельств. Она заставляет людей делать вещи, которые они не хотят делать. Однако она имеет огромное значение для организации и является наиболее важной составляющей работы отдела информационной безопасности.

Политика безопасности определяет:

– безопасность внутри организации;
– место каждого служащего в системе безопасности.

Существуют различные политики, для которых есть три основных общепринятых раздела.

Цель. Каждая политика и процедура имеют четко определенную цель, описывающая причины, почему создана та или иная политика или процедура, и какую выгоду от этого надеется получить организация.

Область. Каждая политика и процедура имеет раздел, описывающий ее сферу приложения. Например, политика безопасности применяется ко всем компьютерным и сетевым системам. Информационная политика применяется ко всем служащим.

Рис. 6

Общая политика информационной безопасности

Ответственность. В разделе об ответственности определяются лица, ответственные за соблюдение политик или процедур, которые должны быть надлежащим образом обучены и знать все требования политики.

Политика безопасности строится на основе анализа рисков, которые признаются реальными для информационной системы организации (рис. 7). Следует выяснить, насколько серьезный ущерб может принести фирме раскрытие или иная атака на каждый конкретный информационный объект.

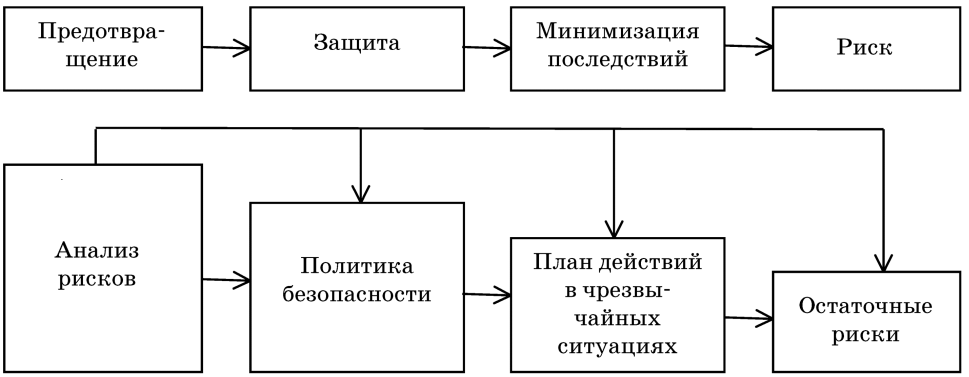

Рис. 7

Схема политики информационной безопасности

Риском называется произведение «возможного ущерба от атаки» на «вероятность такой атаки».

Ущерб от атаки может быть представлен следующим образом (табл. 2).

Таблица 2

Ущерб от атаки

Величина ущерба	Описание
0	Раскрытие информации нанесет ничтожный моральный и финансовый ущерб фирме
1	Ущерб от атаки есть, но он незначителен, основные финансовые операции и положение фирмы на рынке не затронуты
2	Финансовые операции не ведутся в течение некоторого времени, за это время фирма терпит убытки, но ее положение на рынке и количество клиентов изменяются минимально
3	Значительные потери на рынке и в прибыли. От фирмы уходит ощутимая часть клиентов
4	Потери очень значительны, фирма на период до года теряет положение на рынке. Для восстановления положения требуются крупные финансовые займы
5	Фирма прекращает существование

Вероятность атаки представляется в соответствии со следующей таблицей 3.

Таблица 3

Вероятность атаки

Вероятность	Средняя частота появления
0	данный вид атаки отсутствует
1	реже чем раз в год
2	около 1 раза в год
3	около 1 раза в месяц
4	около 1 раза в неделю
5	практически ежедневно

Необходимо отметить, что классификацию ущерба, наносимого атакой, должен оценивать владелец информации или работающий с нею персонал. А вот оценку вероятности появления атаки лучше доверить техническим сотрудникам фирмы.

Следующим этапом является составление таблицы рисков предприятия (табл. 4).

Таблица 4

Риски предприятия

Описание атаки	Ущерб	Вероятность	Риск (=Ущерб× ×Вероятность)
Спам (переполнение почтового ящика)	1	4	4
Копирование жесткого диска из центрального офиса	3	1	3
…	…	…	2
Итого:			9

На этом этапе анализа таблицы рисков задаются некоторым максимально допустимым риском, например значением 7.

Сначала проверяется каждая строка таблицы на непревышение риска этого значения. Если такое превышение имеет место, значит данная строка — это

одна из первоочередных целей разработки политики безопасности. Затем производится сравнение удвоенного значения (в нашем случае 7 × 2 = 14) с интегральным риском (ячейка «Итого»).

Если интегральный риск превышает допустимое значение, значит в системе безопасности набирается множество мелких погрешностей, которые в сумме не дадут предприятию эффективно работать. В этом случае из строк выбираются те, которые дают самый значительный вклад в значение интегрального риска, и производится попытка их уменьшить или устранить полностью.

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.

Политика безопасности организации должна иметь структуру краткого, легко понимаемого документа высокоуровневой политики, поддерживаемого рядом более конкретных документов специализированных политик и процедур безопасности.

*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 крупной 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, т. е. 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 проведению ее в жизнь, т. е. 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 частности;

– не злоупотреблять своими 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 и 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.