

6. Лекция: Административный уровень информационной безопасности

Основные понятия

К **административному уровню информационной безопасности** относятся действия общего характера, предпринимаемые руководством организации.

Главная цель мер **административного уровня** - сформировать программу работ в области информационной безопасности и обеспечить ее выполнение, выделяя необходимые ресурсы и контролируя состояние дел.

Основой программы является **политика безопасности**, отражающая подход организации к защите своих информационных активов. Руководство каждой организации должно осознать необходимость поддержания режима безопасности и выделения на эти цели значительных ресурсов.

Политика безопасности строится на основе **анализа рисков**, которые признаются реальными для информационной системы организации. Когда риски проанализированы и стратегия защиты определена, составляется программа обеспечения информационной безопасности. Под эту программу выделяются ресурсы, назначаются ответственные, определяется порядок контроля выполнения программы и т.п.

Термин "**политика безопасности**" является не совсем точным переводом английского словосочетания "security policy", однако в данном случае калька лучше отражает смысл этого понятия, чем лингвистически более верные "правила безопасности". Мы будем иметь в виду не отдельные правила или их наборы (такого рода решения выносятся на процедурный уровень, речь о котором впереди), а стратегию организации в области информационной безопасности. Для выработки стратегии и проведения ее в жизнь нужны, несомненно, политические решения, принимаемые на самом высоком уровне.

Под **политикой безопасности** мы будем понимать совокупность документированных решений, принимаемых руководством организации и направленных на защиту информации и ассоциированных с ней ресурсов.

Такая трактовка, конечно, гораздо шире, чем набор **правил разграничения доступа** (именно это означал термин "security policy" в "Оранжевой книге" и в построенных на ее основе нормативных документах других стран).

ИС организации и связанные с ней интересы субъектов - это сложная система, для рассмотрения которой необходимо применять объектно-ориентированный подход и понятие уровня детализации. Целесообразно выделить, по крайней мере, три таких уровня, что мы уже делали в примере и сделаем еще раз далее.

Чтобы рассматривать ИС предметно, с использованием актуальных данных, следует составить **карту информационной системы**. Эта **карта**, разумеется, должна быть изготовлена в объектно-ориентированном стиле, с возможностью варьировать не только **уровень детализации**, но и видимые грани объектов. Техническим средством составления, сопровождения и визуализации подобных **карт** может служить свободно распространяемый каркас какой-либо системы управления.

Политика безопасности

С практической точки зрения политику безопасности целесообразно рассматривать на трех уровнях детализации. К верхнему уровню можно отнести решения, затрагивающие организацию в целом. Они носят весьма общий характер и, как правило, исходят от руководства организации. Примерный список подобных решений может включать в себя следующие элементы:

- решение сформировать или пересмотреть комплексную программу обеспечения информационной безопасности, назначение ответственных за продвижение программы;

- формулировка целей, которые преследует организация в области информационной безопасности, определение общих направлений в достижении этих целей;
- обеспечение базы для соблюдения законов и правил;
- формулировка административных решений по тем вопросам реализации программы безопасности, которые должны рассматриваться на уровне организации в целом.

Для политики верхнего уровня цели организации в области информационной безопасности формулируются в терминах целостности, доступности и конфиденциальности. Если организация отвечает за поддержание критически важных баз данных, на первом плане может стоять уменьшение числа потерь, повреждений или искажений данных. Для организации, занимающейся продажей компьютерной техники, вероятно, важна актуальность информации о предоставляемых услугах и ценах и ее доступность максимальному числу потенциальных покупателей. Руководство режимного предприятия в первую очередь заботится о защите от несанкционированного доступа, то есть о конфиденциальности.

На верхний уровень выносятся **управление защитными ресурсами и координация использования этих ресурсов**, выделение специального персонала для защиты критически важных систем и взаимодействие с другими организациями, обеспечивающими или контролирующими режим безопасности.

Политика верхнего уровня должна четко очерчивать сферу своего влияния. Возможно, это будут все компьютерные системы организации (или даже больше, если политика регламентирует некоторые аспекты использования сотрудниками своих домашних компьютеров). Возможна, однако, 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. В этом смысле *политика безопасности* является 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. **Наконец**, необходимо обеспечить определенную степень исполнительности персонала, а для этого нужно выработать систему поощрений и наказаний.

Вообще говоря, **на верхний уровень следует выносить минимум вопросов**. Подобное вынесение целесообразно, когда оно сулит значительную экономию средств или когда иначе поступить просто невозможно.

Британский стандарт BS 7799:1995 рекомендует включать в документ, характеризующий политику безопасности организации, следующие разделы:

- **вводный, подтверждающий озабоченность** высшего руководства проблемами информационной безопасности;
- **организационный, содержащий описание подразделений, комиссий, групп и т.д.**, отвечающих за работы в области информационной безопасности;
- классификационный, описывающий имеющиеся в организации материальные и информационные ресурсы и необходимый уровень их защиты;
- **штатный**, характеризующий меры безопасности, применяемые к персоналу (описание должностей с точки зрения информационной безопасности, организация обучения и переподготовки персонала, порядок реагирования на нарушения режима безопасности и т.п.);
- раздел, освещающий **вопросы физической защиты**;

- **управляющий** раздел, описывающий **подход к управлению компьютерами** и компьютерными сетями;
- раздел, описывающий **правила разграничения доступа** к производственной информации;
- раздел, характеризующий **порядок разработки и сопровождения систем**;
- раздел, описывающий меры, направленные на **обеспечение непрерывной работы** организации;
- **юридический** раздел, подтверждающий соответствие политики безопасности действующему законодательству.

К среднему уровню можно отнести вопросы, касающиеся отдельных аспектов информационной безопасности, но важные для различных эксплуатируемых организацией систем. Примеры таких вопросов - отношение к передовым (но, возможно, недостаточно проверенным) технологиям, доступ в Internet (как совместить свободу доступа к информации с защитой от внешних угроз?), использование домашних компьютеров, применение пользователями неофициального программного обеспечения и т.д.

Политика среднего уровня должна для каждого аспекта освещать следующие темы:

Описание аспекта. Например, если рассмотреть применение пользователями неофициального программного обеспечения, последнее можно определить как ПО, которое не было одобрено и/или закуплено на уровне организации.

Область применения. Следует определить, где, когда, как, по отношению к кому и чему применяется данная *политика безопасности*. Например, касается ли политика, связанная с использованием неофициального программного обеспечения, организаций-субподрядчиков? Затрагивает ли она сотрудников, пользующихся портативными и домашними компьютерами и вынужденных переносить информацию на производственные машины?

Позиция организации по данному аспекту. Продолжая пример с неофициальным программным обеспечением, можно представить себе позиции полного запрета, выработки процедуры приемки подобного ПО и т.п. Позиция может быть сформулирована и в гораздо более общем виде, как набор целей, которые преследует организация в данном аспекте. Вообще стиль документов, определяющих политику безопасности (как и их перечень), в разных организациях может сильно отличаться.

Роли и обязанности. В "политический" документ необходимо включить информацию о должностных лицах, ответственных за реализацию политики безопасности. Например, если для использования неофициального программного обеспечения сотрудникам требуется разрешение руководства, должно быть известно, у кого и как его можно получить. Если неофициальное программное обеспечение использовать нельзя, следует знать, кто следит за выполнением данного правила.

Законопослушность. 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 определенное должностное лицо, а не конкретный человек, занимающий в данный момент данный пост.

Политика безопасности нижнего уровня относится к конкретным информационным сервисам. Она 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 определена более подробно. Есть много вещей, специфичных для отдельных видов услуг, которые нельзя единым образом регламентировать в рамках всей организации. В то же время, эти вещи настолько важны для обеспечения режима безопасности, что относящиеся к ним решения должны приниматься на управленческом, а не техническом уровне. Приведем несколько

примеров вопросов, на которые следует дать ответ в 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?

При формулировке целей политики нижнего уровня можно исходить из соображений целостности, доступности и конфиденциальности, но нельзя на этом останавливаться. Ее цели должны быть более конкретными. Например, если речь идет о системе расчета заработной платы, можно поставить цель, чтобы только сотрудникам отдела кадров и бухгалтерии позволялось вводить и модифицировать информацию. В более общем случае цели должны связывать между собой объекты сервиса и действия с ними.

Из целей выводятся правила безопасности, описывающие, кто, что и при каких условиях может делать. Чем подробнее правила, чем более формально они изложены, тем проще поддержать их выполнение программно-техническими средствами. С другой стороны, слишком жесткие правила могут мешать работе пользователей, вероятно, их придется часто пересматривать. Руководству предстоит найти разумный компромисс, когда за приемлемую цену будет обеспечен приемлемый уровень безопасности, а сотрудники не окажутся чрезмерно связаны. Обычно наиболее формально задаются права доступа к объектам ввиду особой важности данного вопроса.

Программа безопасности

После того, как сформулирована *политика безопасности*, можно приступить к составлению программы ее реализации и собственно к реализации.

Чтобы понять и реализовать какую-либо программу, ее нужно структурировать по уровням, обычно в соответствии со структурой организации. В простейшем и самом распространенном случае достаточно двух уровней - верхнего, или центрального, который охватывает всю организацию, и нижнего, или служебного, который относится к отдельным услугам или группам однородных сервисов.

Программу верхнего уровня возглавляет лицо, отвечающее за информационную безопасность организации. У этой программы следующие главные цели:

- управление рисками (*оценка рисков*, выбор эффективных средств защиты);
- **координация** деятельности в области информационной безопасности, пополнение и распределение ресурсов;
- **стратегическое планирование**;
- **контроль** деятельности в области информационной безопасности.

В рамках программы верхнего уровня принимаются стратегические решения по обеспечению безопасности, оцениваются **технологические новинки**. Информационные технологии развиваются очень быстро, и необходимо иметь четкую политику отслеживания и внедрения новых средств.

Контроль деятельности в области безопасности имеет двустороннюю направленность. Во-первых, необходимо гарантировать, что действия организации не противоречат законам. При этом следует поддерживать контакты с внешними контролирующими организациями. Во-вторых, нужно постоянно отслеживать состояние безопасности внутри организации, реагировать на случаи нарушений и дорабатывать защитные меры с учетом изменения обстановки.

Следует подчеркнуть, что программа верхнего уровня должна занимать строго определенное место в деятельности организации, она должна официально приниматься и поддерживаться руководством, а также **иметь определенный штат и бюджет**.

Цель программы нижнего уровня - обеспечить надежную и экономичную защиту конкретного сервиса или группы однородных сервисов. На этом уровне решается, какие следует использовать механизмы защиты; закупаются и устанавливаются технические

средства; выполняется повседневное администрирование; отслеживается состояние слабых мест и т.п. Обычно за программу нижнего уровня отвечают администраторы сервисов.

Синхронизация программы безопасности с жизненным циклом систем

Если синхронизировать программу безопасности нижнего уровня с *жизненным циклом* защищаемого сервиса, можно добиться большего эффекта с меньшими затратами. Программисты знают, что добавить новую возможность к уже готовой системе на порядок сложнее, чем изначально спроектировать и реализовать ее. То же справедливо и для информационной безопасности.

В *жизненном цикле* информационного сервиса можно выделить следующие этапы:

Инициация. На данном этапе выявляется необходимость в приобретении нового сервиса, документируется его предполагаемое назначение.

Закупка. На данном этапе составляются спецификации, прорабатываются варианты приобретения, выполняется собственно *закупка*.

Установка. Сервис устанавливается, конфигурируется, тестируется и вводится в *эксплуатацию*.

Эксплуатация. На данном этапе сервис не только работает и администрируется, но и подвергается модификациям.

Выведение из эксплуатации. Происходит переход на новый сервис.

Рассмотрим действия, выполняемые на каждом из этапов, более подробно.

На этапе *инициации* оформляется понимание того, что необходимо приобрести новый или значительно модернизировать существующий сервис; определяется, какими характеристиками и какой функциональностью он должен обладать; оцениваются финансовые и иные ограничения.

С точки зрения безопасности важнейшим действием здесь является оценка критичности как самого сервиса, так и информации, которая с его помощью будет обрабатываться. Требуется сформулировать ответы на следующие вопросы:

- какого рода информация предназначена для обслуживания новым сервисом?
- каковы возможные последствия нарушения конфиденциальности, целостности и доступности этой информации?
- каковы угрозы, по отношению к которым сервис и информация будут наиболее уязвимы?
- есть ли какие-либо особенности нового сервиса (например, территориальная распределенность компонентов), требующие принятия специальных процедурных мер?
- каковы характеристики персонала, имеющие отношение к безопасности (квалификация, благонадежность)?
- каковы законодательные положения и внутренние правила, которым должен соответствовать новый сервис?

Результаты оценки критичности являются отправной точкой в составлении спецификаций. Кроме того, они определяют ту меру внимания, которую служба безопасности организации должна уделять новому сервису на последующих этапах его *жизненного цикла*.

Этап *закупки* - один из самых сложных. Нужно окончательно сформулировать требования к защитным средствам нового сервиса, к компании, которая может претендовать на роль поставщика, и к квалификации, которой должен обладать персонал, использующий или обслуживающий покупаемый продукт. Все эти сведения оформляются в виде спецификации, куда входят не только аппаратура и программы, но и документация, обслуживание, обучение персонала. Разумеется, особое внимание должно уделяться вопросам совместимости нового сервиса с существующей конфигурацией. Подчеркнем также, что нередко средства безопасности являются необязательными компонентами

коммерческих продуктов, и нужно проследить, чтобы соответствующие пункты не выпали из спецификации.

Когда продукт закуплен, его необходимо *установить*. Несмотря на кажущуюся простоту, *установка* является очень ответственным делом. Во-первых, новый продукт следует сконфигурировать. Как правило, коммерческие продукты поставляются с отключенными средствами безопасности; их необходимо включить и должным образом настроить. Для большой организации, где много пользователей и данных, начальная настройка может стать весьма трудоемким и ответственным делом.

Во-вторых, новый сервис нуждается в процедурных регуляторах. Следует позаботиться о чистоте и охране помещения, о документах, регламентирующих использование сервиса, о подготовке планов на случай экстренных ситуаций, об организации обучения пользователей и т.п.

После принятия перечисленных мер необходимо провести тестирование. Его полнота и комплексность могут служить гарантией безопасности *эксплуатации* в штатном режиме.

Период *эксплуатации* - самый длительный и сложный. С психологической точки зрения наибольшую опасность в это время представляют незначительные изменения в конфигурации сервиса, в поведении пользователей и администраторов. Если безопасность не поддерживать, она ослабевает. Пользователи не столь ревностно выполняют должностные инструкции, администраторы менее тщательно анализируют регистрационную информацию. То один, то другой пользователь получает дополнительные привилегии. Кажется, что в сущности ничего не изменилось; на самом же деле от былой безопасности не осталось и следа.

Для борьбы с эффектом медленных изменений приходится прибегать к периодическим проверкам безопасности сервиса. Разумеется, после значительных модификаций подобные проверки являются обязательными.

При *выведении из эксплуатации* затрагиваются аппаратно-программные компоненты сервиса и обрабатываемые им данные. Аппаратура продается, утилизируется или выбрасывается. Только в специфических случаях необходимо заботиться о физическом разрушении аппаратных компонентов, хранящих конфиденциальную информацию. Программы, вероятно, просто стираются, если иное не предусмотрено лицензионным соглашением.

При *выведении данных из эксплуатации* их обычно переносят на другую систему, архивируют, выбрасывают или уничтожают. Если архивирование производится с намерением впоследствии прочитать данные в другом месте, следует позаботиться об аппаратно-программной совместимости средств чтения и записи. Информационные технологии развиваются очень быстро, и через несколько лет устройств, способных прочитать старый носитель, может просто не оказаться. Если данные архивируются в зашифрованном виде, необходимо сохранить ключ и средства расшифровки. При архивировании и хранении архивной информации нельзя забывать о поддержании конфиденциальности данных.