

7. АДМИНИСТРАТИВНЫЙ УРОВЕНЬ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

7.1 Основные понятия административного уровня информационной безопасности

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.

«Политика безопасности» (является не совсем точным переводом английского словосочетания «security policy»), имеет в виду не отдельные правила или их наборы, а стратегию организации в области информационной безопасности.

Политика безопасности - совокупность документированных решений, принимаемых руководством организации и направленных на защиту информации и ассоциированных с ней ресурсов.

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.

7.2 Политика безопасности

Политика безопасности определяет архитектуру системы защиты и реализуется посредством:

- административно-организационных мер,
- физических и программно-технических средств.

Для конкретной организации политика безопасности должна носить индивидуальный характер и зависеть от конкретной технологии обработки информации и используемых программных и технических средств.

Политика безопасности определяется способом управления доступом, определяющим порядок доступа к объектам системы.

Различают два основных вида политики безопасности.

- ***Избирательная политика безопасности*** основана на избирательном способе управления доступом и характеризуется заданным администратором множеством разрешенных отношений доступа (например, в виде троек «объект, субъект, тип доступа»). Обычно для описания свойств избирательного управления доступом применяют математическую модель на основе матрицы доступа.
- ***Полномочная политика безопасности*** основана на полномочном (мандатном) способе управления доступом и характеризуется совокупностью правил предоставления доступа, определенных на множестве атрибутов безопасности субъектов и объектов, например, в зависимости от метки конфиденциальности информации и уровня допуска пользователя. ***Полномочное управление доступом подразумевает, что:***
 - все субъекты и объекты системы однозначно идентифицированы;
 - каждому объекту системы присвоена метка конфиденциальности информации, определяющая ценность содержащейся в нем информации;
 - каждому субъекту системы присвоен определенный уровень допуска, определяющий максимальное значение метки конфиденциальности информации объектов, к которым субъект имеет доступ.

С практической точки зрения политику безопасности целесообразно рассматривать на трех уровнях детализации.

1. Верхний уровень. К верхнему уровню можно отнести решения, затрагивающие организацию в целом. 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.

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 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.

2. Средний уровень. К данному уровню можно отнести вопросы, касающиеся отдельных аспектов информационной безопасности, но важные для различных эксплуатируемых организацией систем. 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.
- **Роли и обязанности.** 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.

3. 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.

7.3 Программа безопасности

После того, как сформулирована политика безопасности, можно приступать 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 –

1. *верхнего, или центрального, который охватывает всю организацию,*

2. *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.

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.

7.4 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. В жизненном цикле информационного сервиса можно выделить следующие этапы:

1. **Инициация.** На данном этапе выявляется необходимость в приобретении нового сервиса, документируется его предполагаемое назначение.
2. **Закупка.** На данном этапе составляются спецификации, прорабатываются варианты приобретения, выполняется собственно закупка.
3. **Установка.** Сервис устанавливается, конфигурируется, тестируется и вводится в эксплуатацию.
4. **Эксплуатация.** На данном этапе сервис не только работает и администрируется, но и подвергается модификациям.
5. **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.

Требуется сформулировать ответы на следующие вопросы:

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

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 закупаемый 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. Нередко средства безопасности являются необязательными компонентами коммерческих продуктов, и нужно проследить, чтобы соответствующие пункты не выпали из спецификации.

Установка. 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.
- 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.

- Тестирование - проводится после принятия перечисленных мер необходимо провести. 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. 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.

7.5 Понятие об управлении рисками

Управление рисками рассматривается нами на административном уровне ИБ, поскольку только руководство организации способно выделить необходимые ресурсы, инициировать и контролировать выполнение соответствующих программ.

Использование информационных систем связано с определенной совокупностью рисков. Когда возможный ущерб неприемлемо велик, необходимо принять экономически оправданные меры защиты. Периодическая (пере)оценка рисков необходима для контроля эффективности деятельности в области безопасности и для учета изменений обстановки.

Уровень риска является количественной функцией вероятности реализации определенной угрозы (использующей некоторые уязвимые места), а также величины возможного ущерба.

Суть мероприятий по управлению рисками состоит в том, чтобы оценить их размер, выработать эффективные и экономичные меры снижения рисков, а затем убедиться, что риски заключены в приемлемые

рамки (и остаются таковыми). Следовательно, управление рисками включает в себя два вида деятельности, которые чередуются циклически:

1. (пере)оценка (измерение) рисков;
2. выбор эффективных и экономичных защитных средств (нейтрализация рисков).

По отношению к выявленным рискам возможны следующие действия:

- ликвидация риска (например, за счет устранения причины);
- уменьшение риска (например, за счет использования дополнительных защитных средств);
- принятие риска (и выработка плана действия в соответствующих условиях);
- переадресация риска (например, путем заключения страхового соглашения).

Процесс управления рисками можно разделить на следующие этапы:

1. *Выбор анализируемых объектов и уровня детализации их рассмотрения.* Для небольшой организации допустимо рассматривать всю информационную инфраструктуру; однако если организация крупная, всеобъемлющая оценка может потребовать неприемлемых затрат времени и сил. В таком случае следует сосредоточиться на наиболее важных сервисах, заранее соглашаясь с приближенностью итоговой оценки.
2. *Выбор методологии оценки рисков.* Целью оценки является получение ответа на два вопроса: приемлемы ли существующие риски, и если нет, то какие защитные средства стоит использовать. Значит, оценка должна быть количественной, допускающей сопоставление с заранее выбранными границами допустимости и расходами на реализацию новых регуляторов безопасности.
3. *Идентификация активов.* При идентификации активов, то есть тех ресурсов и ценностей, которые организация пытается защитить, следует, конечно, учитывать не только компоненты информационной системы, но и поддерживающую инфраструктуру, персонал, а также нематериальные ценности, такие как репутация организации.
4. *Анализ угроз и их последствий, выявление уязвимых мест в защите.* Первый шаг в анализе угроз - их идентификация. Целесообразно выявлять не только сами угрозы, но и **источники** их возникновения - это поможет в выборе дополнительных средств защиты. После идентификации угрозы необходимо оценить вероятность ее осуществления. Кроме вероятности осуществления, важен размер потенциального ущерба. Оценивая размер ущерба, необходимо иметь в виду не только непосредственные расходы на замену оборудования или восстановление информации, но и более

отдаленные, такие как подрыв репутации, ослабление позиций на рынке и т.п.

5. *Оценка рисков.* После того, как накоплены исходные данные и оценена степень неопределенности, можно переходить к обработке информации, то есть собственно к оценке рисков. Вполне допустимо применить такой простой метод, как умножение вероятности осуществления угрозы на предполагаемый ущерб.
6. *Выбор защитных мер.* Как правило, для ликвидации или нейтрализации уязвимого места, сделавшего угрозу реальной, существует несколько механизмов безопасности, различных по эффективности и стоимости. Оценивая стоимость мер защиты, приходится, разумеется, учитывать не только прямые расходы на закупку оборудования и/или программ, но и расходы на внедрение новинки и, в частности, обучение и переподготовку персонала. Важным обстоятельством является совместимость нового средства со сложившейся организационной и аппаратно-программной структурой, с традициями организации.
7. *Реализация и проверка выбранных мер.* Когда намеченные меры приняты, необходимо проверить их действенность, то есть убедиться, что остаточные риски стали приемлемыми. Если это на самом деле так, значит, можно спокойно намечать дату ближайшей переоценки.
8. *Оценка остаточного риска.* Если остаточные риски не соответствуют заданным необходимо проанализировать допущенные ошибки и провести повторный сеанс управления рисками немедленно.