**Лекция 4:**

**Построения системы информационной безопасности**

**Аннотация:**Вопросы ответственности в информационной сфере как инструменты реализации бизнес-целей предприятия.

**Основные аспекты построения системы информационной безопасности**

Вопросы ответственности в информационной сфере являются чрезвычайно важными в реализации бизнес-целей предприятия. Поскольку эти вопросы в такой постановке являются частью стратегии развития компании, то они, вне всякого сомнения, относятся к компетенции высшего руководства. Рассматривая вопросы ответственности, следует разделить их реализацию в двух ключевых областях — во внешней среде предприятия и в среде внутренней. Точно также можно ввести два вида вопросов — ответственность за нарушения ИБ и ответственность за реализацию ИБ в различных областях информационной деятельности предприятия.

*Регулирование* ответственности нарушений информационной безопасности во внешней среде с целью нанести вред владельцу информации, а также вопросы взаимоотношений между различными субъектами — обладателями информации — регулируется федеральными законами РФ, региональными, муниципальными и пр. нормативными актами (ответственность первого вида).

Ответственность за причинение вреда и ответственность за реализацию мероприятий по разработке, внедрению и использованию систем ИБ во внутренней среде устанавливается, как правило, на базе действующего законодательства РФ и страны, с которыми осуществляется бизнес, и внутренних корпоративных ("локальных правоустанавливающих") документов. Первый вид ответственности рассмотрен выше.

Ответственность второго вида (формирование и реализация ИБ в различных областях информационной деятельности предприятия) устанавливается обычно на уровне высшего руководства предприятия и включает в себя следующий круг вопросов.

* формирование единой концепции и программы работ в области информационной безопасности (ИБ);
* разработка многоуровневой политики ИБ и системы структурной и персональной ответственности за её реализацию;
* обеспечение выполнения положений политики и программы реализации ИБ;
* планирование и выделение необходимых ресурсов для системной реализации ИБ;
* формирование структурных подразделений и служб ИБ;
* контроль и аудит текущего состояния системы ИБ.

**Программа информационной безопасности**

Управленческие аспекты разработки и реализации информационной безопасности предполагают наличие совокупности организационных мер в виде развернутой программы, которую целесообразно структурировать по уровням, обычно в соответствии со структурой организации. В большинстве случаев достаточно двух уровней — верхнего (организационно-управленческого), который охватывает всю организацию и корпоративную ИС, и нижнего (или сервисного), который относится к отдельным подсистемам ИС и сервисам.

Программу верхнего уровня формирует и возглавляет лицо, отвечающее за информационную безопасность организации. Эти обязанности, как правило, входят в обязанности руководителя ИТ-подразделения (Chief Information Officer — CIO). Программа должна содержать следующие главные цели:

* стратегическое планирование в области развития информационной безопасности;
* разработку и исполнение политики в области ИБ;
* оценка рисков и управление рисками;
* координация деятельности в области информационной безопасности: выбор эффективных средств защиты, их приобретение или разработка, внедрение, эксплуатация, пополнение и распределение ресурсов, обучение персонала;
* контроль деятельности в области ИБ.

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

Контроль деятельности в области безопасности имеет двоякую направленность. Во-первых, необходимо гарантировать, что действия организации не противоречат федеральным и региональным законам и нормативным актам. Необходимо постоянно следить за изменениями во внешней среде, приводящие к возможности возникновения угроз. Во-вторых, нужно постоянно отслеживать состояние безопасности внутри организации, реагировать на все случаи нарушений, вырабатывать стратегию развития защитных мер с учетом изменения обстановки во внешней и внутренней средах.

Цель программы нижнего уровня — обеспечить надежную и экономичную защиту информационных подсистем, конкретных сервисов или групп однородных сервисов. На этом уровне решается, какие механизмы защиты использовать, закупаются и устанавливаются технические средства, выполняется повседневное администрирование, отслеживается состояние слабых мест, проводится первичное обучение персонала и т.п. Обычно за программу нижнего уровня отвечают ответственные менеджеры по обеспечению ИБ, системные администраторы и администраторы сервисов. В плане безопасности важнейшим действием на этом этапе является оценка критичности как самого сервиса, так и информации, которая с его помощью будет обрабатываться. Необходимо сформулировать ответы на следующие вопросы:

* Какие данные и информацию будет обслуживать данный сервис?
* Каковы возможные последствия нарушения конфиденциальности, целостности и доступности этой информации?
* Каковы угрозы, по отношению к которым данные, информация, сервис и пользователь будут наиболее уязвимы?
* Существуют ли какие-либо особенности сервиса, требующие принятия специальных мер — например, территориальная распределённость компонентов ИС?
* Каковы должны быть характеристики персонала, имеющие отношение к безопасности: компьютерная квалификация, дисциплинированность, благонадежность?
* Каковы законодательные положения и корпоративные правила, которым должен удовлетворять сервис?

Результаты оценки критичности являются отправной точкой в составлении спецификаций на приобретение или разработку сервисов. Кроме того, они определяют ту меру внимания, которую служба безопасности организации должна уделять сервису или группе сервисов на всех этапах его жизненного цикла.

Сделаем существенную оговорку. Программа безопасности не является воплощением простого набора технических средств, встроенных в информационную систему — у системы ИБ есть важнейшие "политический" и управленческий аспекты. Программа должна официально приниматься и поддерживаться высшим руководством, у нее должны быть определенные штаты и выделенный бюджет. Без подобной поддержки приказы, распоряжения и "призывы" к исполнению программы останутся пустым звуком.

**Модели ИБ, требования и основные этапы реализации информационной безопасности**

Главная цель мер, предпринимаемых на управленческом уровне - сформировать единую концепцию и программу работ в области информационной безопасности (ИБ) и обеспечить ее выполнение, выделяя необходимые ресурсы и контролируя текущее состояние системы ИБ.

Практически это можно осуществить, разработав концептуальную, математическую и функциональную модели представления информационной защиты, которая позволяет решать задачи создания, использования, сопровождения, развития и оценки эффективности общей системы ИБ ([рис. 4.1](https://intuit.ru/studies/professional_skill_improvements/17846/courses/1242/lecture/27501?page=1#image.4.1)).

Математическая модель представляет собой формализованное описание сценариев в виде логико-алгоритмической последовательности действий нарушителей и ответных мер. Расчетные количественные значения параметров модели характеризуют функциональные (аналитические, алгоритмические или численные) зависимости, описывающие процессы взаимодействия нарушителей с системой защиты и возможные результаты действий. Именно такой вид модели чаще всего используется для количественных оценок уязвимости объекта, построения алгоритма защиты оценки рисков и эффективности принятых мер ([рис. 4.2](https://intuit.ru/studies/professional_skill_improvements/17846/courses/1242/lecture/27501?page=1#image.4.2)).



**Рис. 4.1.**Содержание модели информационной безопасности

При построении теоретических моделей систем защиты информации (СЗИ) и информационных ресурсов необходимо опираться на следующие важнейшие обстоятельства:

* выбор математически строгих критериев для оценки оптимальности системы защиты информации для данной архитектуры ИС;
* четкая математическая формулировка задачи построения модели СЗИ, учитывающая заданные требования к системе защиты и позволяющая построить СЗИ в соответствии с этими критериями.

Такие модели для разных компаний могут быть разнообразными, но любая из них должна обладать следующими свойствами: универсальность, комплексность, наглядность, простота использования, практическая реализуемость, измеримость с помощью наборов метрик, "самообучаемость" (возможность наращивания знаний), надежное функционирование в условиях высокой неопределенности исходной информации.



**Рис. 4.2.**Место математической модели в реализации концепции и программы ИБ

Ниже указаны основные этапы построения модели:

* анализ структуры информационно-вычислительной системы и уровня необходимой защиты данных и самой ИС;
* анализ изменяющихся характеристик СЗИ, определяемых динамикой воздействия угроз (адаптивные СЗИ);
* анализ корреляционных зависимостей между различными параметрами СЗИ, являющимися результатом решения конкретных задач по защите информации;
* анализ возможного понижения общего уровня защищенности из-за наличия корреляций;
* определение совокупностей задач защиты для определения контролируемых параметров СЗИ;
* формирование требований и рекомендаций по рациональной организации структуры ИБ.

Для контроля параметров реализуемых моделей СЗИ необходимо формировать системы количественных показателей (метрик), с помощью которых оценивается:

* сложность структуры, поведение и диагностирование нормальной работы СЗИ с учетом обеспечения её устойчивости в условиях быстро изменяющихся условий внешней и внутренней среды;
* нормальное функционирование контролируемых зон СЗИ; определение и оценка направленных угроз, выявление уязвимостей, управление рисками и т.д.
* работоспособность и возможность диагностирования нарушений нормальной работы СЗИ на базе адаптивных моделей.

В настоящее время адаптивные модели с использованием нейро-нечетких классификаторов чаще всего строятся в терминах теории нечетких множеств (Fuzzy Sets) и нечеткой логики (Fuzzy Logic) по следующей схеме ([рис. 4.3](https://intuit.ru/studies/professional_skill_improvements/17846/courses/1242/lecture/27501?page=1#image.4.3)).



**Рис. 4.3.**Схема построения модели СЗИ

Адаптивность модели на базе нейронных сетей (НС) позволяет при ограниченных затратах на организацию системы ИБ обеспечить заданный уровень безопасности ИТ-системы за счет быстрой реакции системы на изменение поля угроз. При этом очень важным качеством является возможность накопления и передачи опыта системой ЗИ.

Распределенные поля нейро-четких и нейро-нечетких сетей аккумулируют знания в процессе развития защищаемой ИТ-системы, производят адаптацию к изменению поля угроз и эти знания могут передаваться в последующие версии ИТ-системы. Так формируется процесс наследования.



**Рис. 4.4.**Схема нейро-нечеткого классификатора

На [рис. 4.4](https://intuit.ru/studies/professional_skill_improvements/17846/courses/1242/lecture/27501?page=1#image.4.4) показана одна из возможных схем такого классификатора. Обозначения здесь следующие: - вектор угроз,  - вектор заключений о защищенности системы,  - совокупность формальных нейронов классификатора для выполнения операций композиции над нечеткими заключениями,  и  - нижняя и верхняя границы уровня угроз,  - совокупность весовых коэффициентов, описывающих веса связей между различными взаимодействующими нейронами классификатора.

Обучение нейро-нечеткого классификатора на наборе   векторов известных угроз (обучающая выборка) выявляет и позволяет устранить из структуры нейронной сети незначащие связи (слабые неточные заключения в системы нечетких правил, имеющие минимальные веса). Обучение такой НС в виде многослойной структуры с нечеткими связями не требует выполнения сложных математических расчетов, что позволяет снизить трудоемкость решения задачи обучения адаптивной СЗИ ([рис. 4.5](https://intuit.ru/studies/professional_skill_improvements/17846/courses/1242/lecture/27501?page=1#image.4.5)).



**Рис. 4.5.**Адаптивная модель СЗИ на базе нейронных сетей



**Рис. 4.6.**Схема работы генетического алгоритма

Минимизацию ошибки в такой адаптивной системе, построенной на базе нейронных сетей, можно эффективно осуществлять с использованием генетических алгоритмов, где в качестве генов хромосомы используются векторы итерационно перевычисляемых весов связей, ассоциированных с входными значениями  ([рис. 4.6](https://intuit.ru/studies/professional_skill_improvements/17846/courses/1242/lecture/27501?page=1#image.4.6)).

Основное назначение функциональной модели СЗИ - практическое обеспечение процесса создания системы ИБ за счет оптимизации принимаемых решений и выбора рационального варианта технической реализации ([рис. 4.7](https://intuit.ru/studies/professional_skill_improvements/17846/courses/1242/lecture/27501?page=1#image.4.7)).



**Рис. 4.7.**Формирование требований к системе информационной безопасности

На [рис. 4.8](https://intuit.ru/studies/professional_skill_improvements/17846/courses/1242/lecture/27501?page=1#image.4.8) в общем виде представлена модель требований, на основании которых формируются спецификации и организационные меры для приобретения готовых решений или разработки программно-аппаратных средств, реализующих систему информационной защиты [Симонов С., 1999].

Вне зависимости от размеров организации и специфики ее информационной системы, работы по обеспечению режима ИБ в том или ином виде должны содержать этапы, представленные на [рис. 4.8](https://intuit.ru/studies/professional_skill_improvements/17846/courses/1242/lecture/27501?page=1#image.4.8). При этом важно не упустить каких-либо существенных аспектов. Это будет гарантировать некоторый минимальный (базовый) уровень ИБ, обязательный для любой информационной технологии или информационной системы.



**Рис. 4.8.**Основные этапы обеспечения информационной безопасности

Для обеспечения базового уровня ИБ используется упрощенный подход к анализу рисков, при котором рассматривается стандартный набор наиболее распространенных угроз безопасности без детальной оценки их вероятностей. Для нейтрализации угроз применяется типовой набор контрмер, а вопросы эффективности защиты рассматриваются в отдельных важных случаях.

Подобный подход приемлем, если ценность защищаемых ресурсов с точки зрения организации не является чрезмерно высокой.

Отметим объективные трудности, с которыми можно столкнуться при моделировании системы информационной защиты:

1. Трудность построения формальных моделей СЗИ определяется, в целом, неопределенностью условий функционирования ИС.
2. Постановка задачи обеспечения защиты информации, часто оказывается некорректной, поскольку формулируется в условиях непредсказуемости поведения системы защиты в нестандартных и, особенно, экстремальных ситуациях.
3. В связи с этим, задачи обеспечения безопасности вычислительных и информационных систем, как правило, не обладают свойством единственности решения.
4. Эффективность и оптимальность определяются степенью учета ограничений, налагаемых СЗИ для конкретных ситуаций – в общем случае трудно сформировать модель, пригодную для всех возможных ситуаций, связанных с угрозами.
5. Быстрое развитие информационных технологий заставляет пересматривать концепции и программы информационной защиты, что однозначно приводит к необходимости пересматривать текущие модели СЗИ.

Однако математические и функциональное моделирование чрезвычайно важно и необходимо. В результате моделирования получаем: оценку возможности реализации различных средств защиты информации в современных системах обработки данных; архитектуру системы защиты, согласованную с архитектурой ИС и информационной инфраструктурой предприятия; количественную оценку качества функционирования СЗИ; оценку экономической и практической эффективности реализуемой модели СЗИ.

**Мероприятия по защите информации**

Мероприятия охватывают целый ряд аспектов законодательного, организационного и программно-технического характера. Для каждого из них формулируется ряд задач, выполнение которых необходимо для защиты информации. Перечислим самые общие из них.

В нормативно-законодательном аспекте необходимо решение следующих задач:

* определение круга нормативных документов международного, федерального и отраслевого уровня, применение которых требуется при проектировании и реализации системы информационной безопасности;
* определение на основе нормативных документов требований по категорированию информации;
* определения на основе нормативных документов базовых требований к системе информационной безопасности и ее компонентам.

В организационном аспекте:

* определение соответствия структурируемой и защищаемой информации подсистемам и ресурсам информационной системы, в которых производится хранение, обработка и передача информации конечному пользователю (должно быть организовано ведение реестра ресурсов, содержащих информацию, значимую по критериям конфиденциальности, целостности и доступности);
* определения набора служб, обеспечивающих доступ к информационным ресурсам системы (необходима выработка и согласование типовых профилей пользователей, ведение реестра таких профилей);
* формирования политики безопасности, включающей описание границ и способов контроля безопасного состояния системы, условия и правила доступа различных пользователей к ресурсам системы, мониторинга деятельности пользователей.

В процедурном аспекте:

* организация физической защиты помещений и компонентов информационной системы, включая сети и телекоммуникационные устройства;
* обеспечение решения задач информационной безопасности при управлении персоналом;
* формирование, утверждение и реализация плана реагирования на нарушения режима безопасности;
* внесение дополнений, связанных со спецификой ликвидации последствий несанкционированного доступа, в план восстановительных работ.

В программно-техническом аспекте:

* обеспечение архитектурной и инфраструктурной полноты решений, связанных с хранением, обработкой и передачей конфиденциальной информации;
* обеспечение проектной и реализационной непротиворечивости механизмов безопасности по отношению к функционированию информационной системы в целом;
* выработка и реализация проектных и программно-аппаратных решений по механизмам безопасности.

Рассматривая эти аспекты применительно к обеспечению безопасности современных информационных систем, можно сфокусировать их на следующих положениях [Галатенко В.А., 2006]:

* базовые требования к ИБ и техническое задание на создание защищенной ИС разрабатываются с учетом федеральных и региональных законов и нормативных документов, с использованием международных стандартов
* корпоративная ИС может иметь несколько территориально разнесенных частей, связи между которыми находятся в ведении внешнего поставщика сетевых услуг например, частные виртуальные сети (Virtual Private Net — VPN), выходящие за пределы зоны, контролируемой организацией;
* корпоративная сеть имеет одно или несколько подключений к Internet;
* на каждой из производственных площадок могут находиться критически важные серверы, в доступе к которым нуждаются сотрудники, работающие на других площадках, мобильные пользователи и, возможно, внешние пользователи;
* для доступа пользователей могут применяться не только компьютеры, но и потребительские устройства, использующие, в частности, беспроводную связь, не все пользовательские системы контролируются сетевыми и/или системными администраторами организации;
* в течение одного сеанса работы пользователю приходится обращаться к нескольким информационным сервисам, опирающимся на разные аппаратно-программные платформы;
* к доступности информационных сервисов предъявляются жесткие требования, которые обычно выражаются в необходимости круглосуточного функционирования с максимальным временем простоя порядка нескольких минут;
* ИС представляет собой сеть с активными агентами, то есть в процессе работы программные компоненты, такие как апплеты или сервлеты, передаются с одной машины на другую и выполняются в целевой среде, поддерживая связь с удаленными компонентами;
* программное обеспечение, особенно полученное по сети, не может считаться надежным, в нем могут быть ошибки, создающие проблемы в защите;
* конфигурация ИС постоянно изменяется на уровнях административных данных, программ и аппаратуры (меняется состав пользователей, их привилегии и версии программ, появляются новые сервисы, новая аппаратура и т.п.).

При формулировании требований к обеспечению информационной безопасности и построению соответствующей функциональной модели ИБ, следует учитывать следующие важные моменты.

Во-первых, для каждого сервиса основные требования к ИБ (доступность, целостность, конфиденциальность) трактуются по-своему. Целостность с точки зрения СУБД и с точки зрения почтового сервера — вещи принципиально разные. Бессмысленно говорить о безопасности локальной или иной сети вообще, если сеть включает в себя разнородные компоненты. Следует анализировать защищенность конкретных сервисов и устройств, функционирующих в сети. Для разных сервисов и защиту строят по-разному.

И, во-вторых, основная угроза ИБ организаций, как было отмечено выше, в большей степени исходит не от внешних злоумышленников, а от собственных сотрудников. В связи с этим необходима разработка и внедрения в практику работы предприятия совокупности управленческих и организационных мер по обеспечению ИБ.

**Политика информационной безопасности**

Основой программы обеспечения ИБ является многоуровневая политика информационной безопасности, отражающая подход организации к защите своих информационных активов и ресурсов ([рис. 4.9](https://intuit.ru/studies/professional_skill_improvements/17846/courses/1242/lecture/27501?page=2#image.4.9)).



**Рис. 4.9.**Системное содержание политики информационной безопасности

Под "политикой информационной безопасности" понимается совокупность документированных методологий и управленческих решений, а также распределение ролей и ответственности, направленных на защиту информации, информационных систем и ассоциированных с ними ресурсов.

Политика безопасности является важнейшим звеном в формировании ИБ, поэтому принятие решения о её разработке, внедрении и неукоснительном выполнении всегда принимается высшим руководством организации. Политика разрабатывается на основе концепции и программы информационной безопасности. Как системный документ, политика включает в себя общую (концептуально-программную) часть и совокупность частных политик, относящихся к различным аспектам деятельности компании.

В идеале политика информационной безопасности должна быть реалистичной и выполнимой, а также не приводить к существенному снижению общей производительности бизнес-подразделений компании. Политика безопасности должна содержать основные цели и задачи организации режима информационной безопасности, четко содержать описание области действия, а также указывать на контактные лица и их обязанности.

Вводная часть "Общей политики безопасности" должна быть краткой и понятной содержать не более двух-четырёх (максимум пять) страниц текста. При этом важно учитывать, как политика безопасности будет влиять на уже существующие информационные системы компании. Как только политика утверждена, она должны быть предоставлена всем сотрудникам компании для ознакомления. Наконец, политика безопасности должна пересматриваться ежегодно, чтобы отразить текущие изменения в развитии бизнеса компании и в её программно-аппаратном, сетевом и информационном обеспечении.

Формирование, актуализация и совершенствование политики ИБ является многоаспектным циклическим (итерационным) процессом ([рис. 4.10](https://intuit.ru/studies/professional_skill_improvements/17846/courses/1242/lecture/27501?page=2#image.4.10)), реализация которого сводится к следующим практическим шагам.



**Рис. 4.10.**Итерационный процесс разработки и реализации политики ИБ

1. Определение используемых руководящих документов и стандартов в области ИБ, а также основных положений политики ИБ, включая:
	* принципы администрирования системы ИБ и управление доступом к вычислительным и телекоммуникационным средствам, программам и информационным ресурсам, а также доступом в помещения, где они располагаются;
	* принципы контроля состояния систем защиты информации, способы информирования об инцидентах в области ИБ и выработку корректирующих мер, направленных на устранение угроз;
	* принципы использования информационных ресурсов персоналом компании и внешними пользователями;
	* антивирусную защиту и защиту против действий хакеров;
	* вопросы резервного копирования данных и информации;
	* проведение профилактически, ремонтных и восстановительных работ;
	* обучение и повышение квалификации персонала.
2. Разработка методологии выявления и оценки угроз и рисков их осуществления, определение подходов к управлению рисками: является ли достаточным базовый уровень защищенности или требуется проводить полный вариант анализа рисков.
3. Структуризация контрмер по уровням требований к безопасности.
4. Порядок сертификации на соответствие стандартам в области ИБ. Должна быть определена периодичность проведения совещаний по тематике ИБ на уровне руководства, включая периодический пересмотр положений политики ИБ, а также порядок обучения всех категорий пользователей информационной системы по вопросам ИБ.

С практической точки зрения политику безопасности целесообразно разделить на три уровня. К верхнему уровню можно отнести решения, затрагивающие организацию в целом. Они носят общий характер и, как правило, исходят от высшего руководства организации:

* формулировка целей, которые преследует организация в области информационной безопасности, определение общих направлений и средств для достижения этих целей;
* формирование или пересмотр комплексной программы обеспечения информационной безопасности, определение ответственных менеджеров и технических руководителей за реализацию и сопровождение программы;
* обеспечение правовой базы для соблюдения государственных законов и корпоративных правил;
* формулировка общих управленческих решений по тем вопросам реализации программы безопасности, которые должны рассматриваться на уровне организации в целом.

На верхнем уровне политики 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 случаев потерь, повреждений или искажений данных. Для организации, занимающейся продажами, вероятно, важна актуальность информации о предоставляемых услугах и ценах, а также ее доступность максимальному числу потенциальных покупателей. "Режимная" организация в первую очередь заботится о защите от несанкционированного доступа — конфиденциальности.

На верхний уровень выносится управление защитными ресурсами 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 очерчивать сферу своего влияния. Возможно, это будут все компьютерные системы организации или даже больше, если политика регламентирует некоторые аспекты использования сотрудниками своих домашних компьютеров. В политике должны быть определены обязанности должностных лиц по выработке программы безопасности и по проведению ее в жизнь.

Политика верхнего уровня имеет дело с тремя аспектами законопослушности и исполнительской дисциплины:

* организация должна соблюдать существующие законы, государственные нормативные акты, корпоративные нормативные положения и стандарты;
* следует контролировать все действия направленные на выработку программы безопасности и назначить ответственных лиц на уровне высшего менеджмента за разработку, внедрение и неукоснительное исполнение принятой программы;
* необходимо обеспечить определенную степень исполнительности и послушания персонала, а для этого нужно выработать систему общего и персонального обучения и эффективной мотивации.

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

К среднему уровню можно отнести вопросы, касающиеся отдельных аспектов информационной безопасности, но важные для различных систем, эксплуатируемых организацией. Примеры таких вопросов: широкий доступ в доступ в Internet и сочетание свободы получения информации с защитой от внешних угроз, использование домашних компьютеров, применение пользователями неофициального или несанкционированного 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 обеспечение, которое не было одобрено и/или закуплено и внедрено на уровне организации.

Область применения. Следует специфицировать, где, когда, как, по отношению к кому и чему применяется данный аспект политики безопасности. Например, касается ли организаций-субподрядчиков политика отношения к неофициальному программному обеспечению? Затрагивает ли она работников, пользующихся карманными компьютерами и ноутбуками и вынужденных переносить информацию на производственные машины?

Позиция организации. Продолжая пример с неофициальным программным обеспечением, можно обозначить позиции полного запрета или выработки процедуры приемки и использования подобного обеспечения и т.п. Позиция может быть сформулирована в общем виде, как набор целей, которые преследует организация в данном аспекте. Вообще говоря, содержание документов по политике безопасности, так и перечень таких документов, может быть существенно различным для разных организаций.

Роли, обязанности и ответственность. В документ необходимо включить информацию о должностных лицах, отвечающих за проведение политики безопасности в жизнь. Например, если для использования работником неофициального программного обеспечения нужно официальное разрешение, то должно быть известно, у кого и как его следует получать. Если должны проверяться дискеты, принесенные с других компьютеров, необходимо описать процедуру проверки. Если неофициальное программное обеспечение использовать нельзя, следует знать, кто следит за выполнением данного правила.

Законопослушность. Политика должна содержать общее описание запрещенных действий с несанкционированным ПО и наказаний за них.

Точки контакта. Должно быть известно, куда и к каким документам следует обращаться за разъяснениями, помощью и дополнительной информацией. Обычно "точкой контакта" служит должностное лицо и/или доступный раздел соответствующей библиотеки или хранилища.

Политика безопасности нижнего уровня относится к конкретным сервисам. Она включает в себя конкретные цели и задачи, правила и способы их достижения. В отличие от двух верхних уровней, рассматриваемая политика должна быть гораздо детальнее. Есть много вещей, специфичных для отдельных сервисов, которые нельзя единым образом регламентировать в рамках всей организации. В то же время эти вещи настолько важны для обеспечения режима безопасности, что решения, относящиеся к ним, должны приниматься на управленческом, а не техническом уровне. Типичные вопросы, на которые следует дать ответ при следовании политики 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?
* кто имеет право модернизировать сервис? и т.д.

При формулировке целей политика нижнего уровня может исходить из соображений целостности, доступности и конфиденциальности, но она не должна останавливаться только на них. Например, если речь идет о системе расчета заработной платы, можно поставить цель, чтобы только работникам бухгалтерии и отдела кадров позволялось вводить и модифицировать информацию. В общем случае цели должны связывать между собой объекты сервиса и осмысленные действия с ними.

Исходя из целей, формулируются правила безопасности, описывающие, кто, что и при каких условиях может делать. Чем детальнее правила, чем более формально они изложены, тем проще поддержать их выполнение программно-техническими мерами и средствами.

Для разработки и внедрения политики ИБ, как правило, создаётся рабочая группа. Формирование такой группы по информационной безопасности актуально, прежде всего, для крупных компаний, в которых процесс изменения информационных технологий является постоянным, в него вовлечено большое количество людей — поэтому так важно предусмотреть механизм, предоставляющий им возможность постоянного общения. Создание рабочей группы, имеющий свой информационный ресурс (форум) в Intranet, позволяет обеспечить соответствующую координацию комплекса вопросов по обеспечению ИБ и избежать проблем, связанных с недостаточной информированностью всех заинтересованных лиц. Фактически, с точки зрения российских реалий, такой форум является постоянно действующим органом компании, включающим в свой состав представителей наиболее значимых подразделений компании, а также сотрудников служб информационной, экономической и общей безопасности.

К компетенции этого органа относятся разработка динамической модели информационной безопасности, включающей:

* разработку, обсуждение и принятие концепции (политики) информационной безопасности, внесение изменений и принятие новой версии концепции, согласование списков ответственных лиц;
* отслеживание и анализ важных изменений в структуре информационных ресурсов компании на предмет выявления новых угроз информационной безопасности;
* изучение и анализ инцидентов, связанных с безопасностью;
* принятие важных инициатив по усилению мер безопасности.

Рабочая группа является ведущим органом по проведению организационно-режимных процессов и разработке стандартов организации, определяющих режим работы компании в части, касающейся информационной безопасности. Она отвечает за исполнение концепции (политики) информационной безопасности и может быть создана не только в рамках компании, но и в рамках ее крупных структурных подразделений. К компетенции этой рабочей группы относятся следующие вопросы:

* выработка соглашений о разграничении ответственности за обеспечение информационной безопасности внутри компании;
* выработка специальных методик и политик, связанных с информационной безопасностью: анализ рисков, классификация систем и информации по уровням безопасности;
* поддержание в организации "атмосферы" информационной безопасности, в частности, регулярное информирование персонала по этим вопросам;
* обеспечение обязательности учета вопросов информационной безопасности при стратегическом и оперативном планировании;
* обеспечение обратной связи (оценка адекватности принимаемых мер безопасности в существующих системах) и координация внедрения средств обеспечения информационной безопасности в новые системы или сервисы;
* анализ инцидентов в области информационной безопасности, выработка рекомендаций по их предотвращению.

В рабочую группу должны входить специалисты следующих подразделений: представитель высшего менеджмента в лице заместителя генерального директора или технической дирекции (департамента), службы общей безопасности, кадровой службы, служб экономической и информационной безопасности, юридической службы, представители аналитических отделов и служб, а также службы менеджмента качества.

Распределение ответственности за обеспечение безопасности включает необходимость выполнения следующих действий:

* определение ресурсов, имеющих отношение к информационной безопасности по каждой системе;
* назначение для каждого ресурса (или процесса) ответственного сотрудника из числа руководителей. Разграничение ответственности должно быть закреплено документально;
* определение и документальное закрепление для каждого ресурса списка прав доступа (матрицы доступа).

Совершенно очевидно, что реализация политики информационной безопасности вовлекает много специалистов высокого класса и требует существенных затрат. Во всех случаях необходимо найти разумный компромисс, когда за приемлемую цену будет обеспечен приемлемый уровень безопасности, а работники не окажутся чрезмерно ограничены в использовании необходимых информационных ресурсов. Обычно ввиду особой важности данного вопроса наиболее регламентировано и детально задаются права доступа к информационным объектам и устройствам.

Неоднократно отмечено, что сотрудники являются как самым сильным, так одновременно и самым слабым звеном в обеспечении информационной безопасности. Необходимо донести до сотрудников мысль о том, что обеспечение информационной безопасности — обязанность всех без исключения сотрудников. Это достигается путем введения процедуры ознакомления с требованиями политики ИБ и подписания соответствующего документа о том, что сотрудник ознакомлен, ему понятны все требования политики и он обязуется их выполнять.

Политика позволяет ввести требования по поддержанию необходимого уровня безопасности в перечень обязанностей каждого сотрудника. В процессе выполнения ими трудовых обязанностей для сотрудников необходимо периодически проводить ознакомление и обучение вопросам обеспечения информационной безопасности. Критически важным условием для успеха в области обеспечения информационной безопасности компании становится создание в компании атмосферы, благоприятной для создания и поддержания высокого приоритета информационной безопасности. Чем крупнее компания, тем более важной становится информационная поддержка и мотивация сотрудников по вопросам безопасности.