

1 Предпосылки к управлению информационной безопасностью предприятия

Обеспечение собственной информационной безопасности на предприятиях, как правило, является неотъемлемой частью общей системы управления, необходимой для достижения уставных целей и задач. Значимость систематической целенаправленной деятельности по обеспечению информационной безопасности становится тем более высокой, чем выше степень автоматизации бизнес-процессов предприятия и чем больше «интеллектуальная составляющая» в его конечном продукте, т.е. чем в большей степени успешность деятельности зависит от наличия и сохранения определенной информации (технологий, ноу-хау, коммерческих баз данных, маркетинговой информации, результатов научных исследований и пр.), обеспечения ее конфиденциальности и доступности для владельцев и пользователей. Роль информации и, в частности, т.н. «знаниевых активов» в деятельности предприятий возрастает по мере либерализации мировых рынков, когда материальные активы во все меньшей степени являются источниками конкурентных преимуществ в силу значительного уменьшения торговых барьеров. Нематериальные активы, существующие обычно в виде информации, в этих условиях начинают играть роль одной из ведущих основ для повышения конкурентоспособности и развития бизнеса.

Обеспечение информационной безопасности также, как правило, имеет большое значение не только для стратегического развития предприятия и создания основного продукта, но и для отдельных (иногда вспомогательных) направлений деятельности и бизнес-процессов, таких как коммерческие переговоры и условия контрактов, ценовая политика и пр.

Кроме того, значимость обеспечения информационной безопасности в некоторых случаях может определяться наличием в общей системе информационных потоков предприятия сведений, составляющих не только коммерческую, но и государственную тайну, а также другие виды

конфиденциальной информации (сведения, составляющие банковскую тайну, врачебную тайну, интеллектуальную собственность компаний-партнеров и пр.). Обеспечение информационной безопасности в этой сфере и, в частности, основные требования, организационные правила и процедуры непосредственно регламентируются федеральным законодательством, и надзор за выполнением требований осуществляется федеральными органами власти:

1) Для сведений, составляющих государственную тайну – Федеральный закон РФ от 21 июля 1993 года №5485-1 «О государственной тайне» и связанные с ним подзаконные акты.

2) Для сведений, составляющих банковскую тайну – Федеральный закон «О банках и банковской деятельности» и связанные с ним смежные законы и подзаконные акты.

3) Для сведений, составляющих врачебную тайну – Основы законодательства РФ «Об охране здоровья граждан» (ст.61) и Закон РФ «О трансплантации органов и (или) тканей человека» (ст.14).

4) Для сведений, относящихся к некоторым другим видам тайны, таких как военная тайна, нотариальная тайна, адвокатская тайна, тайна страхования, тайна усыновления, налоговая тайна, тайна следствия и судопроизводства и пр.

Соответственно, лица, нарушающие требования информационной безопасности, могут быть не только подвергнуты дисциплинарным взысканиям, но и подлежат уголовному и административному преследованию.

Так же, как и на государственном уровне, управление информационной безопасностью на уровне предприятий направлено на нейтрализацию различных видов угроз:

– внешних, таких как неправомерные действия государственных органов (в том числе и зарубежных), противоправная деятельность преступников и преступных группировок, незаконные действия компаний-конкурентов и других хозяйствующих субъектов, недобросовестные действия компаний-партнеров, несоответствие действующей нормативно-правовой базы фактическому развитию технологий и общественных отношений, сбои и нарушения в работе

Тема 2.6 – Управление информационной безопасностью предприятия
(Управление информационной безопасностью)

глобальных информационных и телекоммуникационных систем и информационных систем компаний-партнеров (контрагентов) и пр.;

– внутренних, таких как ошибки и халатность персонала предприятия, а также намеренно допускаемые нарушения, сбои и нарушения в работе собственных информационных систем и пр.

Таким образом, управление информационной безопасностью на каждом отдельном предприятии должно осуществляться в контексте его общей хозяйственной деятельности: с учетом характера деятельности компании (технологии производства, специфики рынков сбыта и пр.), а также фактически складывающейся ситуации в рыночной конкурентной борьбе, государственной политике, развития правовой и правоохранительной системы, уровня развития отдельных используемых информационных и телекоммуникационных технологий и других факторов, формирующих общие условия текущей деятельности.

Формальным основанием (предпосылкой) для осуществления целенаправленной деятельности в сфере защиты информации, помимо общегосударственных требований к защите информации, составляющей государственную, военную, врачебную и банковскую тайну, также является перечень сведений, составляющих коммерческую тайну предприятия, который определяется предприятием самостоятельно с учетом требований действующего законодательства.

Тема 2.6 – Управление информационной безопасностью предприятия
(Управление информационной безопасностью)



Рисунок 1 – Предпосылки разработки политики безопасности предприятия

Кроме того, необходимость разработки и внедрения политики информационной безопасности может быть обусловлена такими обстоятельствами, как:

- необходимость уменьшения стоимости страхования информационных рисков или определенных бизнес-рисков;
- необходимость внедрения международных стандартов, таких как ISO 17799 или BS 7799.

Предпосылки разработки политики безопасности предприятия представлены на рисунке 1.

2 Структура управления информационной безопасностью предприятия

Для нейтрализации существующих угроз и обеспечения информационной безопасности предприятия организуют систему менеджмента в сфере информационной безопасности, в рамках которой (системы) проводят работу по нескольким направлениям:

- формирование и практическая реализация комплексной многоуровневой политики информационной безопасности предприятия и системы внутренних требований, норм и правил;
- организация департамента (службы, отдела) информационной безопасности;

Тема 2.6 – Управление информационной безопасностью предприятия
(Управление информационной безопасностью)

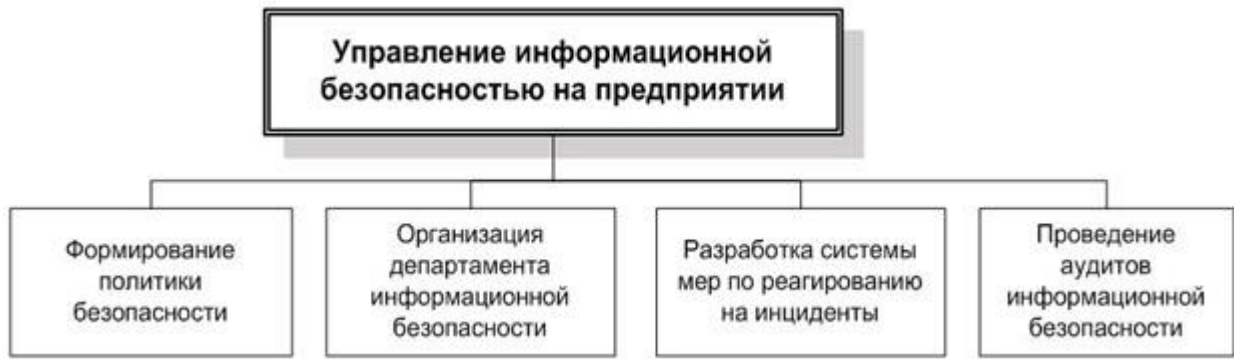


Рисунок 2 – Структура управления информационной безопасностью предприятия

- разработка системы мер и действий на случай возникновения непредвиденных ситуаций («Управление инцидентами»);
- проведение аудитов (комплексных проверок) состояния информационной безопасности на предприятии.

Каждое из этих направлений организационной работы имеет свои особенности и должно реализовываться с использованием специфических методов менеджмента и в соответствии со своими правилами. Политики и правила информационной безопасности являются организационными документами, регулирующими деятельность всей организации или отдельных подразделений (категорий сотрудников) в части обращения с информационными системами и информационными потоками. Департамент информационной безопасности является узкоспециализированным подразделением, решающим специфические вопросы защиты информации.

Система мер по реагированию на инциденты обеспечивает готовность всей организации (включая Департамент информационной безопасности) к осмысленным целенаправленным действиям в случае каких-либо происшествий, связанных с информационной безопасностью. Проведение внутренних аудитов информационной безопасности (периодических или связанных с определенными событиями) должно обеспечить контроль за текущим состоянием системы мер по защите информации и, в частности, независимую проверку соответствия реального положения дел установленным правилам и требованиям.

При этом каждое из направлений деятельности должно постоянно совершенствоваться по мере развития организации, а конкретные задачи должны постоянно уточняться в соответствии с изменением в организационной структуре, производственных процессах или внешней среде. Так, например, если предприятие начинает выпуск продукции военного назначения параллельно с выпуском гражданской продукции, то это может потребовать изменений всех основных направлений организационной работы в сфере обеспечения информационной безопасности:

- корректировки стратегии и основных положений политики информационной безопасности (на всех ее уровнях);
- изменения организационной структуры и функциональных задач департамента информационной безопасности;
- совершенствования системы реагирования на инциденты;
- использование более совершенных методик проведения аудитов информационной безопасности.

Структура управления информационной безопасностью предприятия представлена на рисунке 2.

3 Политика информационной безопасности предприятия

3.1 Структура политики информационной безопасности и процесс ее разработки.

Политика информационной безопасности представляет собой комплекс документов, отражающих все основные требования к обеспечению защиты информации и направления работы предприятия в этой сфере. При построении политики безопасности можно условно выделить три ее основных уровня: верхний, средний и нижний.

Верхний уровень политики информационной безопасности предприятия служит:

- для формулирования и демонстрации отношения руководства предприятия к вопросам информационной безопасности и отражения общих целей всего предприятия в этой области;
- основой для разработки индивидуальных политик безопасности (на более низких уровнях), правил и инструкций, регулирующих отдельные вопросы;
- средством информирования персонала предприятия об основных задачах и приоритетах предприятия в сфере информационной безопасности.

Политики информационной безопасности среднего уровня определяют отношение предприятия (руководства предприятия) к определенным аспектам его деятельности и функционирования информационных систем:

- отношение и требования (более детально по сравнению с политикой верхнего уровня) предприятия к отдельным информационным потокам и информационным системам, обслуживающим различные сферы деятельности, степень их важности и конфиденциальности, а также требования к надежности (например, в отношении финансовой информации, а также информационных систем и персонала, которые относятся к ней);
- отношение и требования к определенным информационным и телекоммуникационным технологиям, методам и подходам к обработке информации и построения информационных систем;
- отношение и требования к сотрудникам предприятия как к участникам процессов обработки информации, от которых напрямую зависит эффективность многих процессов и защищенность информационных ресурсов, а также основные направления и методы воздействия на персонал с целью повышения информационной безопасности.

Политики безопасности на самом низком уровне относятся к отдельным элементам информационных систем и участкам обработки и хранения

информации и описывают конкретные процедуры и документы, связанные с обеспечением информационной безопасности.

Разработка политики безопасности предполагает осуществление ряда предварительных шагов:

- оценку личного (субъективного) отношения к рискам предприятия его собственников и менеджеров, ответственных за функционирование и результативность работы предприятия в целом или отдельные направления его деятельности;
- анализ потенциально уязвимых информационных объектов;
- выявление угроз для значимых информационных объектов (сведений, информационных систем, процессов обработки информации) и оценку соответствующих рисков.

Осуществление предварительных шагов (анализа) позволяет определить, насколько информационная безопасность в целом важна для устойчивого осуществления основной деятельности предприятия, его экономической безопасности. На основе этого анализа с учетом оценок менеджеров и собственников определяются конкретные направления работы по обеспечению информационной безопасности. При этом в некоторых случаях личное мнение отдельных руководителей может и не иметь решающего значения. Например, в том случае, когда в распоряжении компании имеются сведения, содержащие государственную, врачебную, банковскую или военную тайну, основные процедуры обращения информации определяются федеральным законодательством, а также директивами и инструкциями тех федеральных органов, в чьей компетенции находятся вопросы обращения такой информации.

Таким образом, политика информационной безопасности (практически на всех уровнях) в части работы с такими данными будет основана на общих строго формализованных правилах, процедурах и требованиях (таких, как использование сертифицированного оборудования и программного

обеспечения, прохождение процедур допуска, оборудование специальных помещений для хранения информации и пр.).

При разработке политик безопасности всех уровней необходимо придерживаться следующих основных правил.

1) Политики безопасности на более низких уровнях должны полностью подчиняться соответствующей политике верхнего уровня, а также действующему законодательству и требованиям государственных органов.

2) Текст политики безопасности должен содержать только четкие и однозначные формулировки, не допускающие двойного толкования.

3) Текст политики безопасности должен быть доступен для понимания тех сотрудников, которым он адресован.

В целом политика информационной безопасности должна давать ясное представление о требуемом поведении пользователей, администраторов и других специалистов при внедрении и использовании информационных систем и средств защиты информации, а также при осуществлении информационного обмена и выполнении операций по обработке информации. Кроме того, из политики безопасности, если она относится к определенной технологии и/или методологии защиты информации, должны быть понятны основные принципы работы этой технологии. Важной функцией политики безопасности является четкое разграничение ответственностей в процедурах информационного обмена: все заинтересованные лица должны ясно осознавать границы, как своей ответственности, так и ответственности других участников соответствующих процедур и процессов. Также одной из задач политики безопасности является защита не только информации и информационных систем, но и защита самих пользователей (сотрудников предприятия и его клиентов и контрагентов).



Рисунок 3 – Жизненный цикл политики ИБ предприятия

Общий жизненный цикл политики информационной безопасности включает в себя ряд основных шагов:

- 1) Проведение предварительного исследования состояния информационной безопасности.
- 2) Собственно, разработку политики безопасности.
- 3) Внедрение разработанных политик безопасности.
- 4) Анализ соблюдения требований внедренной политики безопасности и формулирование требований по ее дальнейшему совершенствованию (возврат к первому этапу, на новый цикл совершенствования).

Этот цикл (Рисунок 3) может повторяться несколько раз с целью совершенствования организационных мер в сфере защиты информации и устранения выявляемых недоработок.

3.2 Политика информационной безопасности предприятия – верхний уровень

Политика информационной безопасности верхнего уровня фактически является декларацией руководителей и/или собственников предприятия о необходимости вести целенаправленную работу по защите информационных ресурсов, что должно стать основой для более успешного функционирования предприятия в основном направлении его деятельности, а также устранить различные риски, которые могут привести к финансовым потерям, ущербу для репутации предприятия, административному и уголовному преследованию руководителей и другим негативным последствиям.

Политика информационной безопасности на этом уровне может определять и описывать:

- собственно, решение об осуществлении целенаправленной систематической деятельности по обеспечению информационной безопасности предприятия;
- перечень основных информационных ресурсов, таких как информационные системы, массивы данных, информация об отдельных фактах и явлениях (конструкторских разработках, коммерческих сделках, результатах НИОКР и пр.), защита которых имеет наибольший приоритет для всего предприятия;
- общий подход к распределению ответственности за обеспечение информационной безопасности внутри организации;
- указание на необходимость для всего персонала соблюдать определенные меры предосторожности при работе с информацией и информационными системами, повышать свою квалификацию в данной области и осознавать меру ответственности за возможные нарушения;
- отношение руководства предприятия к фактам нарушения требований по обеспечению информационной безопасности и лицам, совершающим такие

нарушения, а также общий подход к их преследованию в случае выявления таких фактов.

Одной из задач политики верхнего уровня является формулирование и демонстрация того, что защита информации является одним из ключевых механизмов обеспечения конкурентоспособности предприятия и обуславливает, как его способность достигать поставленные цели, так иногда и способность выживания и сохранения возможности продолжать деятельность. Для этого могут быть обозначены приоритетные направления хозяйственной деятельности и соответствующие им информационные системы и потоки информации, описана причинно-следственная связь между возможными нарушениями конфиденциальности и/или нарушениями в стабильной работе информационных систем, с одной стороны, и нарушениями нормального хода текущих хозяйственных операций, с другой стороны. На основе этого могут быть определены приоритетные направления деятельности по обеспечению информационной безопасности. В наибольшей степени зависимость общей эффективности деятельности от информационной безопасности характерна для таких компаний, которые:

- занимаются т.н. электронной коммерцией или работают в смежных сферах (электронные платежи, Интернет-реклама и пр.);
- непосредственно связаны с оборотом (созданием, куплей-продажей, охраной, оценкой) объектов интеллектуальной собственности и, в частности, наукоемких технологий;
- непосредственно связаны с обращением больших объемов информации, составляющей тайну других лиц (банки, медицинские учреждения, аудиторские компании и пр.).

При этом работа над политикой информационной безопасности должна включать в себя не только ее начальную разработку, но и постоянный мониторинг угроз, изменений во внешней среде для последующего уточнения

(или даже полной переработки) политики в соответствии с изменившимися условиями работы.

3.3 Политика информационной безопасности предприятия – средний уровень

Политики информационной безопасности среднего уровня непосредственно детализируют требования, задачи и правила, обозначенные в политике верхнего уровня, и отдельно описывают основные сферы, в которых необходимо системное осуществление тех или иных организационных и/или технических мероприятий.

Политика информационной безопасности среднего уровня должна содержать следующие основные разделы.

1) Общее описание той сферы деятельности (информационной технологии, аспекта информационной системы, бизнес-процессов предприятия), на которую она распространяется.

2) Область применения политики безопасности – перечень всех лиц, организаций, информационных систем, к которым она применяется или которые исключаются из сферы ее применения.

3) Непосредственное отношение предприятия к данному аспекту информационных технологий и информационной безопасности – основная часть политики безопасности, определяющая конкретные правила, критерии и требования к процедурам обращения информации, элементам информационной инфраструктуры, программным и аппаратным средствам и пр.

4) Распределение ролей и функций, необходимых для разрешения конкретных вопросов – закрепление за определенными сотрудниками (специалистами, руководителями) обязанностей по выполнению необходимой работы с целью решения задач в рамках данной политики безопасности.

5) Порядок разрешения возникающих вопросов – основные процедуры разрешения появляющихся затруднений в текущей работе и принятия решений о возможных исключениях из общих правил, а также перечень лиц

(подразделений), ответственных за непосредственную работу с персоналом предприятия по вопросам, относящимся к данной политике безопасности.

Одной из основ для реализации мероприятий в сфере информационной безопасности и детальной разработки политики безопасности является укрупненная классификация информационных ресурсов, имеющихся у предприятия. Все имеющиеся у предприятия информационные объекты (и соответствующие элементы информационной инфраструктуры), как правило, могут быть разделены на пять или шесть основных групп по уровню своей значимости и конфиденциальности.

1) Критически важная (абсолютно секретная) информация – информация, требующая особых гарантий безопасности.

2) Важная информация (информация, составляющая коммерческую тайну) – информация, используемая только внутри предприятия, нарушение конфиденциальности которой может нанести серьезный ущерб самому предприятию или его партнерам.

3) Значимая (конфиденциальная) информация – информация, предназначенная для использования ограниченным кругом сотрудников и руководителей предприятия.

4) Персональная информация – информация о сотрудниках, не подлежащая разглашению.

5) Информация для внутреннего использования – информация для использования внутри предприятия, нарушение конфиденциальности которой не может нанести вреда.

6) Прочая информация – открытая информация, конфиденциальность которой не имеет особого значения для деятельности предприятия.

Во всем объеме политик среднего уровня необходимо выделить два их основных вида.

1) Политики, относящиеся к определенным сферам деятельности предприятия и соответствующим информационным потокам (финансам, коммерческой деятельности и пр.).

2) Политики, относящиеся к определенным аспектам использования информационных технологий, организации информационных потоков и организации работы персонала на всем предприятии – вне зависимости от той сферы, где используются эти технологии или занят персонал.

К политикам первого типа могут относиться:

- политики обращения с информацией, составляющей государственную тайну;
- политики обращения с результатами НИОКР, конструкторской и технологической документацией, составляющей «ноу-хау» предприятия или его партнеров и пр.

Политики безопасности такого типа уточняют и дополняют общие для всего предприятия правила, распространяющиеся на все остальные информационные системы и объекты, и, соответственно, имеют наибольший приоритет. Они, например, могут содержать:

- специальные требования к резервному копированию информации (такие как более высокая частота резервного копирования и использование более надежных носителей для этого);
- специальные требования к идентификации и аутентификации пользователей (такие как комбинирование биометрической идентификации и идентификации при помощи паролей);
- специальные требования к копировально-множительной технике, используемой для работы с конфиденциальной информацией;
- специальные требования к помещениям, в которых проводятся совещания по секретной тематике, и обрабатывается соответствующая информация (толщина и материал стен, расположение помещений в зданиях, защищенность окон, надежность дверей и запоров, а также охранной и пожарной сигнализации, обследования на предмет выявления подслушивающих устройств и пр.).

К политикам второго типа могут относиться:

- политика опубликования открытых информационных материалов, в том числе политика организации веб-сайта предприятия и его внутреннего информационного портала (в части предотвращения возможных утечек и искажений информации);
- политика использования сети Интернет (в части предотвращения возможных утечек информации);
- политики использования отдельных информационных и коммуникационных технологий, в том числе общие для всего предприятия правила использования мобильных компьютеров и КПК, удаленного доступа к корпоративным информационным системам, а также использования личных компьютеров сотрудников предприятия в служебных целях;
- классификации информационных систем, информационных ресурсов и объектов информации с точки зрения их значимости и усилий, которые необходимо предпринимать для их защиты;
- политика приобретения, установки, модификации и обновления программного обеспечения, а также аутсорсинга разработки и проектирования программного обеспечения;
- политика закупки аппаратных средств информационных систем, систем информационной безопасности;
- политика использования пользователями собственного программного обеспечения (т.е. ПО, самостоятельно разрабатываемого предприятием);
- общие для всего предприятия правила использования паролей и других средств персональной идентификации;
- политика использования электронно-цифровой подписи и инфраструктуры публичных ключей;
- политика (регламент) обеспечения внутриобъектового режима и физической защищенности информационных активов;

- политика доступа к внутренним информационным ресурсам сторонних пользователей (организаций);
- общий для всего предприятия порядок привлечения к ответственности за нарушение определенных правил информационной безопасности.

3.4 Политика информационной безопасности предприятия – нижний уровень

Данный уровень включает в себя документы, являющиеся инструкциями и методиками прямого действия, используемыми в повседневной деятельности сотрудников предприятия. Эти документы относятся к отдельным сервисам, процедурам и информационным системам. Основной задачей разработки организационной документации на этом уровне является обеспечение как можно более детального и формализованного описания всех процедур и требований, относящихся к обеспечению безопасности отдельных элементов информационных систем, информационных потоков и массивов информации. В частности, для обеспечения полноты формирования политики информационной безопасности предприятия необходимо сформировать как можно более полный комплект организационной документации, включающий в себя:

- бланки типовых заявок на предоставление доступа отдельных сотрудников к определенным информационным ресурсам и информационным системам, а также регламенты предоставления такого доступа;
- регламенты (процедуры) работы с определенными информационными и телекоммуникационными системами, программным обеспечением и базами данных;
- должностные обязанности отдельных категорий сотрудников в отношении обеспечения информационной безопасности, а также требования, предъявляемые к персоналу;
- типовые договоры с внешними контрагентами, связанные с передачей или получением информации, или основные требования, предъявляемые к таким договорам.

Процедурные документы, относящиеся к предоставлению доступа к ресурсам (таким как сеть Интернет, корпоративные информационные системы и базы данных, аппаратные средства, средства передачи информации и пр.) могут включать как типовые бланки заявок на предоставление доступа, так и описание основных процедур (регламента) принятия решений о предоставлении такого доступа и предоставлении конкретных прав при работе с информационными ресурсами, а также перечни критериев, необходимых для предоставления тех или иных прав в информационных системах.

Процедуры работы с отдельными информационными системами и/или модулями информационных систем (базами данных, модулями корпоративной ERP-системы, системами электронного документооборота и пр.) могут перечислять все основные требования, правила и ограничения, например, запрет, использовать дискеты для копирования и переноса информации или ограничения, налагаемые на возможность удаленного доступа к тем или иным информационным сервисам. Требования и правила, связанные с обеспечением информационной безопасности, могут быть, как включены в общие инструкции по использованию информационных систем или регламенты осуществления бизнес-процессов, так и оформлены в виде специальных инструкций и памяток, содержащих исключительно требования и правила информационной безопасности.

Должностные обязанности персонала предприятия, связанные с обеспечением информационной безопасности, должны входить как составная часть в должностные инструкции для каждого сотрудника. Кроме того, политика безопасности может предусматривать подписание (как при поступлении на работу или переводе на определенную должность, так и при увольнении с нее) отдельными категориями персонала дополнительных соглашений, обязательств и подписок о неразглашении определенной информации. Также политика безопасности может вводить дополнительные требования к персоналу, работающему с определенными сведениями или информационными системами. Примерами таких ограничений могут быть отсутствие судимости, наличие

определенных навыков или специальной квалификации, прохождение профессиональной сертификации или психологической проверки.

Политики безопасности, относящиеся к работе с внешними контрагентами, могут предусматривать типовые формы и отдельные инструкции по составлению коммерческих контрактов (для каждого типа контрактов, а также для отдельных групп контрагентов) и обмену информацией с поставщиками, покупателями, консультантами, посредниками, субподрядчиками, поставщиками финансовых и информационных услуг и другими участниками хозяйственной деятельности. В частности, в политике для каждой из этих категорий может предусматриваться специфический порядок информационного обмена, взаимные требования по обеспечению конфиденциальности и возможные меры ответственности в случае нарушения согласованных требований какой-либо из сторон.

3.5 Заключительные положения

В тех случаях, когда определенная политика безопасности описывает сложную информационную систему и систему защиты информации, предназначенную для выполнения наиболее ответственных операций (таких как, например, электронные денежные переводы), она может быть разделена на две составляющие:

- внутренний регламент работы подразделений (групп, администраторов), отвечающих за выполнение наиболее важных административных функций (например, выдача и обслуживание электронных сертификатов Инфраструктуры публичных ключей);
- политику, непосредственно отражающую требования к пользователям и процессам, а также описания процедур работы и взаимодействия всех участников информационного обмена.

В этом случае внутренний регламент может содержать подробное описание тех правил и требований, которые должны выполнять ответственные подразделения (ИТ-служба, Департамент информационной безопасности или

Служба безопасности предприятия) в процессе выполнения своих функций. Такой регламент может быть необходим для демонстрации надежности наиболее важных и ответственных элементов инфраструктуры информационной безопасности. Это особенно важно в том случае, если предприятие осуществляет информационный обмен с внешними контрагентами (и, в частности, клиентами) и демонстрация надежности внутренних процедур сервисов информационной безопасности может обеспечить расширение бизнеса и повышение эффективности отдельных операций.

В некоторых случаях объем таких документов (политик, регламентов) может достигать нескольких десятков страниц (как правило, не более 100-150 страниц). Документы такого размера, как правило, составляются в тех случаях, когда может понадобиться их использование в судебных процессах для установления степени вины и ответственности различных участников процедур информационного обмена. В том случае, если отдельные политики представляют собой сложные объемные документы, изобилующие юридическими и техническими терминами, они могут сопровождаться дополнительным документом, кратко раскрывающим основные требования и положения для большинства пользователей. Такой документ должен иметь относительно небольшой объем (например, не более двух страниц) и содержать описание наиболее важных аспектов предмета политики: практически важные ограничения, ответственность и основные правила, знание которых необходимо для повседневной деятельности.

К числу документов на среднем и нижнем уровне детализации, помимо собственно политик безопасности, можно отнести также юридическое заключение, формально подтверждающее, что все меры информационной безопасности, предпринимаемые на предприятии, соответствуют требованиям действующего законодательства и/или стандартов.