3. ПОЛИТИКА ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

В данной главе определяются понятия политики ОИБ вообще и политики ИБ организации, а также дается систематическое и обобщенное изложение с необходимыми обоснованиями детальных практических рекомендаций, воспользовавшись которыми обучающиеся смогут самостоятельно разработать ПолИБ любого уровня. Излагаются причины выработки политики для организации, основные требования к ней и принципы ее разработки и внедрения. Подробно рассматриваются содержания всех разделов корпоративной и частных политик ИБ. Описываются основные шаги, необходимые для выполнения на различных стадиях жизненного цикла политики. Глава дополнена обширным приложением, в котором приведены примеры некоторых типовых частных ПолИБ.

3.1. Понятия политики обеспечения ИБ и политики ИБ организации

Термин «политика» (от греч. *politika – государственные или общественные дела, polis – государство*) давно используется в человеческом обществе. Существует много трактовок этого понятия, из которых чаще всего используются следующие:

1) сфера деятельности, связанная с отношениями между социальными группами, сутью которой является определение форм, задач, содержания деятельности государства[1];

2) направление деятельности государства или каких-либо социальных групп в той или иной области в определенный период[2];

3) образ действий, направленных на достижение чего-либо, поведение, определяющее отношения с людьми[3];

4) общее намерение и направление, официально выраженное руководством [22].

В англоязычной литературе при рассмотрении вопросов ОИБ кроме политики используются и другие термины – стандарты, базис, руководства и процедуры [80].

Политика (англ. *policy*) определяется как расширенная формулировка принципа, который отражает позицию руководства организации

---

[1] *Большой Энциклопедический словарь. М: Астрель, 2008.*

[2] *Ефремова Т. Ф. Новый словарь русского языка. Толково-словообразовательный. М.: Русский язык, 2000.*

[3] *Ефремова Т. Ф. Новый словарь русского языка. Толково-словообразовательный. М.: Русский язык, 2000. Ожегов С. И., Шведова Н. Ю. Толковый словарь русского языка. М.: Азъ, 1992.*

в отношении определенной области управления. Это директивы высшего руководства по созданию программы ОИБ, установке ее целей и распределению обязанностей. Политики обычно рассчитаны на долгий срок и содержат руководство по разработке более конкретных правил для ситуаций и систем. Политики могут относиться к совершенно различным вопросам, таким как управленческие решения по настройке электронной почты организации, обеспечению режима секретности или защите факсов. Политики интерпретируются и поддерживаются стандартами, основными направлениями, процедурами и руководствами. В них должно содержаться общее руководство для организации. По своей природе политики обязательны для исполнения. Они должны быть одобрены и поддержаны их основными исполнителями. Невозможность соблюдать политику должна быть санкционирована в виде исключения. Примеры областей, для которых необходимы политики: физическая защита, ИБ, персональные данные, безопасность персонала, безопасность оборудования, защита ПО, безопасность сетей, безопасность беспроводного доступа, УНБ, управление рисками ИБ, управление инцидентами ИБ.

Стандарт (англ. *standard*) представляет собой правило, указывающее конкретное направление действий или ответную реакцию на данную ситуацию. Стандарты являются обязательными директивными указаниями (директивами), которые должны выполняться в соответствии с политиками и которые используются для определения соответствия этим политикам. Стандарты служат спецификациями для осуществления политик. Стандарты разработаны в целях содействия осуществлению высокоуровневой политики организации, а не для создания новых политик.

Базис (линии отсчета, базовые линии) (англ. *baselines*) устанавливает, как для конкретных технологий должны быть реализованы средства управления. Базис – это зависящее от конкретной платформы правило защиты, которое принято во всей отрасли как обеспечивающее наиболее эффективный подход к данной реализации защиты. Базис создан для обеспечения того, чтобы функции защиты наиболее часто используемых систем были настроены и управлялись единым образом, поддерживающим постоянный уровень безопасности в пределах всей организации.

Процедуры (англ. *procedures*) определяют конкретно, как политики, стандарты, базисы и руководства будут реализованы в данной ситуации. Процедуры – это технологии или процессы, зависимые и имеющие отношение к конкретным платформам, приложениям или процессам. Они используются для выработки шагов, которые должны быть предприняты на организационном уровне для обеспечения безопасности отдельных систем и процессов. Процедуры, как правило, разработаны, реализованы и обеспечены организацией, владеющей процессом или системой. С целью обеспечения конкретных технических или процедурных

требований внутри организации, где они применяются, процедуры как можно точнее должны поддерживать организационные политики, стандарты, базисы и руководства. Примеры процедур: сертификация и аккредитация, оценка рисков ИБ, обнаружение вторжений, тесты на проникновение, реагирование на чрезвычайные ситуации, восстановление после аварий, резервирование, реагирование на инциденты ИБ.

Руководства (руководящие принципы, директивы) (англ. *guidelines*) содержат рекомендации по тому, как должны выполняться другие требования. Руководство является общим заявлением, используемым в качестве рекомендации или предлагающим подход к осуществлению политики, стандартов и базисов. По существу это рекомендации, которые необходимо учитывать при осуществлении защиты. По своей природе не являясь обязательными, они должны соблюдаться, если нет документированных и одобренных причин не делать этого.

Взаимосвязь введенных терминов можно проиллюстрировать рис. 3.1.

Рис. 3.1. Взаимосвязь понятий «политика», «стандарт», «процедура» и «руководство» в области ОИБ

Описательный пример – ПолИБ организации в отношении использования электронной почты. Эта необъемлемая часть деятельности сотрудников организации подкрепляется различными стандартами, включая и требование регулярно удалять сообщения электронной почты через 90 дней после их появления. В этом примере базис связан с тем, как будут конфигурироваться средства управления для сервиса электронной почты, работающей на различных системах (например, OpenVMS, UNIX и т. п.). Процедуры – это конкретные требования применения в данной организации ПолИБ для электронной почты и обеспечивающих ее стандартов. И, наконец, руководства, разработанные в соответствии с лучшими практиками защиты информации, отправляемой или получаемой посредством электронной почты, предназначены для пользователей и администраторов.

Для организаций общий подход и намерения в области ОИБ, официально выраженные руководством, отражаются в разработанном, утвержденном им и строго выполняемом на практике всеми ее сотрудниками

и бизнес-партнерами документе – *политике ОИБ организации*, для краткости далее называемой ***политикой ИБ*** (ПолИБ) (англ. *security policy*).

ПолИБ содержит позицию организации по отношению к деятельности в области ОИБ, её стремление соответствовать государственным, международным требованиям и стандартам в этой области. ПолИБ определяет стратегию и тактику построения в организации системы защиты информации. (В российской терминологии документ, определяющий стратегию, часто называют концепцией, а документ, определяющий тактику, – политикой. За рубежом принято создавать единый документ, включающий в себя стратегию и тактику защиты одновременно.) ПолИБ организации является основой для разработки целого ряда документов в области ОИБ: стандартов, руководств, процедур, практик, регламентов, должностных инструкций и пр.

Согласно самому первому определению, приведенному в стандарте «Оранжевая книга» (Trusted Compute System Evaluation Criteria), *ПолИБ* – это набор норм, правил и практических приемов, которые регулируют управление, защиту и распределение ценной информации [81]. Гостехкомиссия России определила такую ПолИБ как правила разграничения доступа, представляющие собой совокупность правил, регламентирующих права доступа субъектов доступа к объектам доступа [76]. После этого данный термин определялся как в международных, так и российских стандартах и руководящих документах в основном как *ПолИБ организации*:

- совокупность требований и правил по ОИБ для объекта ИБ, выработанных в соответствии с требованиями руководящих и нормативных документов в целях противодействия заданному множеству угроз ИБ, с учетом ценности защищаемой информационной сферы и стоимости СОИБ [82];
- документированные решения в области ОИБ [83];
- совокупность (одно или несколько) документированных правил, процедур, практических приемов в области безопасности, которыми руководствуется организация в своей деятельности [10, 61].

СТО БР ИББС-1.0 вводит понятие *ПолИБ организации БС РФ*. Это документация, определяющая высокоуровневые цели, содержание и основные направления деятельности по ОИБ, предназначенная для организации БС РФ в целом [11].

Различают ПолИБ организации в целом (тогда она называется *корпоративной ПолИБ*) или ее подразделения. Такие политики называют также *ПолИБ верхнего, или программного, уровня* (англ. *program-level*) [83].

В ГОСТ Р ИСО/МЭК 13335–1–2006 была отдельно выделена *ПолИБ ИТТ* (англ. *ICT security policy*) – правила, директивы, сложившаяся практика, которые определяют, как в пределах организации и ее ИТТ управлять, защищать и распределять активы, в том числе критичную информацию [54].

ПолИБ сети (англ. *network security policy*) определяется как документ, в рамках единой информационной инфраструктуры и СОИБ организации формально устанавливающий правила доступа к ее компьютерной сети, на основе которых пользователи этой сети (сотрудники и бизнес-партнеры организации) накапливают, применяют и распоряжаются ее активами.

В современной практике ОИБ термин ПолИБ может употребляться как в широком, так и в узком смысле [83]. *В широком смысле ПолИБ* определяется как система документированных управленческих решений по ОИБ организации. *В узком смысле ПолИБ* – отдельный нормативный документ, определяющий требования безопасности, систему мер и/или порядок действий, а также ответственность сотрудников организации и средства управления для определенной области ОИБ.

Также известно понятие «*частная ПолИБ*» [11], или *ПолИБ по конкретным вопросам или проблемам* (англ. *issue-specific*) или *ПолИБ по конкретным системам* (англ. *system-specific*) [84], ориентированная на отдельную область ОИБ или технологию, используемую в организации или ее подразделении. Например, это ОНБ (в части, касающейся ИБ), ОИБ телекоммуникационных систем и сервисов, антивирусная защита, доступ в Интернет, использование средств криптографической защиты и т. д. В них формулируются требования на создание и эксплуатацию СЗИ, организацию информационных и бизнес-процессов организации по конкретному направлению ОИБ. Таким образом, частные ПолИБ являются составляющими корпоративной ПолИБ организации, поскольку конкретизируют ее. Согласно [11] *частная ПолИБ* – это документация, детализирующая положения ПолИБ применительно к одной или нескольким областям ИБ, видам и технологиям деятельности организации. Таким образом, частная ПолИБ – это ПолИБ в узком смысле.

Поскольку основу ПолИБ составляет, как правило, конкретный способ управления каким-либо видом доступа, определяющим порядок обращения субъектов системы к ее объектам, название этого способа и определяет название частной ПолИБ. Как показывает опыт, наиболее часто разрабатываемыми в организациях частными ПолИБ являются политики для следующих областей и технологий, имеющие аналогичные названия:

1. Физической защиты (включая вопросы организации пропускного режима, регистрации сотрудников и посетителей, использования средств сигнализации и видеонаблюдения и т. п.).
2. Организации режима секретности.
3. ОИБ при процессе транспортировки носителей информации.
4. Обращения с информацией, составляющей государственную тайну.
5. Опубликования материалов в открытых источниках.
6. Доступа сторонних пользователей (организаций) в ИС организации.
7. Оценки рисков ИБ.

8. Управления паролями.

9. Контроля доступа и защиты от несанкционированного доступа.

10. Назначения и распределения ролей и обеспечение доверия к персоналу.

11. Использования Интернета.

12. Разработки и лицензирования ПО.

13. Установки и обновления версий ПО.

14. Приобретения ИС и их элементов (программных и аппаратных средств).

15. Использования отдельных универсальных ИТ в масштабе организации:

- электронной почты;
- сетевых сервисов;
- программно-технических средств защиты;
- межстевых экранов (МЭ);
- технологии ВЧС;
- средств антивирусной защиты;
- средств криптографической защиты информации;
- электронной цифровой подписи (ЭЦП);
- инфраструктуры открытых ключей;
- модемов и других коммуникационных средств;
- мобильных аппаратных средств и т. д.

16. Проведения внешних и внутренних аудитов ИБ.

17. Резервирования информации и т. п.

В РС БР ИББС-2.0 по документации в области ОИБ отмечается, что деятельность организации БС РФ по ОИБ осуществляется на основе действующих законодательных актов и нормативных документов РФ по ОИБ, нормативных актов Банка России и внутренних документов самой организации по ОИБ [75]. В состав внутренних документов рекомендуется включать следующие виды документов (документированной информации), организованных в виде приведенной на рис. 3.2 иерархической структуры:

1) документы 1-го уровня, содержащие положения корпоративной ПолИБ организации и определяющие высокоуровневые цели, содержание и основные направления деятельности по ОИБ, предназначенные для организации в целом;

2) документы 2-го уровня, содержащие положения частных ПолИБ и детализирующие положения корпоративной ПолИБ применительно к одной или нескольким областям ИБ, видам и технологиям деятельности организации;

3) документы 3-го уровня, содержащие положения ИБ, применяемые к процедурам (порядку выполнения действий или операций) ОИБ, правила и параметры, устанавливающие способ осуществления и выполне-

ния конкретных действий, связанных с ИБ в рамках технологических процессов, используемых в организации, либо ограничения по выполнению отдельных действий, связанных с реализацией защитных мер в используемых технологических процессах (технические задания, регламенты работ, порядки, инструкции по эксплуатации, руководства по администрированию и т. п.);

4) документы 4-го уровня, содержащие свидетельства выполненной деятельности по ОИБ и отражающие достигнутые результаты (промежуточные и окончательные), относящиеся к ОИБ организации.

Рис. 3.2. Иерархия документов в области ОИБ для организаций БС РФ

Согласно ГОСТ Р ИСО/МЭК 17799–2005 на верхнем уровне ПолИБ должны быть оформлены следующие документы: «Концепция обеспечения ИБ» (или просто «Концепция ИБ»), «Правила допустимого использования ресурсов информационной системы», «План обеспечения непрерывности бизнеса» [13]. На практике можно встретить и документы с такими названиями: «Регламент управления ИБ», «Технический стандарт ИБ» и т. п. Данные документы могут выпускаться в двух редакциях – для внешнего и внутреннего использования.

По аналогии с определением Концепция ИБ РФ Межведомственной комиссии по ИБ Совета Безопасности РФ (1995 г.) *концепция ИБ организации* – это официально принятая руководством организации система взглядов на проблему ОИБ, методы и средства защиты жизненно важных интересов организации в информационной сфере. Эта система взглядов взаимоувязывает правовые, организационные и программно-аппаратные меры защиты и основана на анализе защищенности ИС в разрезе видов угроз и динамики их развития. Концепция ИБ отражает стратегию и тактику ОИБ организации и отвечает на три основных вопроса: что защищать, от чего защищать и как защищать. Таким образом,

концепция ИБ организации во многом схожа с корпоративной ПолИБ, хотя второй документ содержит более конкретное наполнение стратегии и тактики правилами, процедурами, практическими приемами и руководящими принципами в области ОИБ, которыми руководствуется организация в своей деятельности.

Еще один подход разделяет ПолИБ на две категории: административные, выполняемые людьми, и технические, реализуемые с помощью оборудования и программ.

Организационная или *административная ПолИБ* (англ. *organizational security policy*) и есть ПолИБ в выше определенном понимании. Она обычно излагается в документах трех уровней. Документы верхнего уровня носят общий характер и определяют ПолИБ для организации в целом. Второй уровень выделяют в случае структурной сложности организации или при необходимости обозначить специфичные области деятельности, подразделения, технологии, подсистемы и т. п. Третий уровень относится к конкретным службам или подразделениям организации и детализирует верхние уровни ПолИБ. На данном уровне определяются конкретные цели, частные критерии и показатели ИБ, задаются права групп пользователей, формулируются условия доступа к информации, выводятся правила ОИБ и т. п.

Техническая ПолИБ (англ. *technical security policy*) – это совокупность законов, правил и практических методов, регулирующих обработку чувствительной информации и использование ресурсов ПО и аппаратным обеспечением (АО) ИС [www.finam.ru/dictionary]. Техническая ПолИБ базируется на правилах двух видов. Первая группа связана с заданием правил разграничения доступа ко всем информационным ресурсам организации, вторая – основана на правилах анализа сетевого трафика как внутри интранета, так и при его выходе или входе из интранета. В основе этих правил лежит принцип доверия – пользователям, приложениям, процессам, базам данных (БД), файлам и т. п. Поэтому определяя техническую ПолИБ, нужно установить, насколько можно доверять людям и информационным ресурсам, поскольку возможны атаки с подменой («маскарадом») ресурсов (англ. *spoofing*).

Кроме этого, *ПолИБ могут создаваться для отдельных пользователей или для группы пользователей* – для отдельного департамента, роли/должности, внутри организации или за ее пределами (для партнеров, клиентов, аудиторов и т. п.).

Итак, поскольку в контексте данного учебного пособия наиболее важным понятием является ***ПолИБ организации***, определим ее как ***документацию, определяющую высокоуровневые цели, содержание и основные направления и устанавливающую правила, процедуры, практические приемы и руководящие принципы ОИБ активов организации, которыми она руководствуется в своей деятельности.***

3.2. Причины выработки политики ИБ

Предположим, что администратор ИБ интранета крупной организации наблюдает за ней поздно вечером и видит, что развивается атака [85]. Что ему делать? Позволить атаке и дальше продолжаться и собирать регистрируемые соответствующими системами данные для дальнейшего расследования или отключить интранет от экстранета (от сетей бизнес-партнеров данной организации и каналов Интернета, соединяющих интранет и эти сети)? Если так, отключить ли основное средство фильтрации трафика – МЭ – между интранетом и экстранетом? Или отключить соединение с Интернетом, например, препятствуя доступу пользователей на веб-сервер организации? Имеет ли он полномочия это сделать? Руководству организации до наступления такого события необходимо четко расставить приоритеты и определить все необходимые действия.

Рассмотрим сценарий, когда администратор ИБ думает, что интранет действительно атакуют, поэтому и отключает соединение с экстранетом. Пользователи выражают свое недовольство из-за невозможности выполнения своих привычных операций в интранете. А потом оказывается, что администратор ИБ ошибся и, например, принял работу только что принятого в организацию нового сотрудника за злоумышленника. Кража данных является понятием теоретически возможным, а недовольные пользователи вполне реальны. Таким образом, необходима политика, которая определяет важность всех защитных мер и четко устанавливает процедуры, необходимые для выполнения, когда кажется, что имеет место атака. Как только точно определены приоритеты, нужно понять технологию реализации установленной политики.

Наиболее правильный и эффективный способ добиться минимизации рисков нарушения ИБ организации еще до того, как появится первая проблема с безопасностью, – разработать ПолИБ и в соответствии с ней реализовать, эксплуатировать и совершенствовать СОИБ организации [11].

Можно выделить несколько основных аргументов в пользу того, что ПолИБ обязательно должна быть выработана для организации любого масштаба и вида деятельности. Во-первых, ПолИБ составляет общую основу для защиты всех влияющих на ОИБ активов организации, в рамках которой определяются правила разграничения доступа к этим активам. Она определяет, какое поведение по отношению к активам разрешено, т. е. является санкционированным, а какое запрещено, является несанкционированным и свидетельствует о незаконном их использовании. Во-вторых, ПолИБ определяет «правила игры» для всех сотрудников организации и третьих лиц, что позволяет достичь согласия по вопросам ОИБ как внутри самой организации (включая ее руководство), так и вовне. В-третьих, ПолИБ часто помогает сделать правильный вы-

бор самой платформы для работы с активами, учитывая, какие инструментальные средства и процедуры будут использованы.

Первостепенной целью разработки ПолИБ организации является обеспечение решения вопросов ОИБ в пределах организации и вовлечение ее высшего руководства в данный процесс. Для этого в первую очередь она определяет правильный (с точки зрения организации) способ использования ее активов, а также процедуры, предотвращающие или реагирующие на нарушения ИБ. Важно также подчеркнуть, что в основе любой политики лежат *модели доверия, или трастовые модели* (англ. *trusted models*). Для ИС наиболее точно смысл понятия «доверие» передает следующая формулировка: можно сказать, что один субъект «доверяет» другому, когда предполагает, что второй субъект будет вести себя точно так, как ожидает от него первый на основе их взаимодействия [86, 87]. Таким образом, доверие имеет дело с предположениями, ожиданиями и поведением. Оно не может быть измерено количественно. Существует риск, связанный с доверием. Следовательно, при разработке ПолИБ необходимо определить, кто, к чему и каким образом может получать доступ. Здесь можно провести следующую аналогию – при первой установке программно-аппаратных систем чаще всего производителем предусмотрена защита по принципу наименьшего доступа для всех. Далее для каждой группы пользователей и входящих в нее отдельных представителей определяются виды доверия (например, для файла чтение, копирование, модификация, удаление, создание). Это дело достаточное сложное и даже деликатное. Если доверие ко всем слишком велико, то им могут злоупотреблять. Если доверия заслуживает лишь очень небольшая группа пользователей, то и в этом случае возникнут ситуации, когда выполнение обычных обязанностей сотрудниками организации будет затруднено, например постоянными процедурами аутентификации, что вызовет с их стороны только раздражение, полное неприятие ПолИБ и нежелание ее поддерживать и осуществлять ее основные положения на практике. Компромиссное решение в данном случае и будет самым подходящим – всего должно быть в меру, в том числе доверия и недоверия.

Существует три основные трастовые модели.

Либеральная – доверять всем и всегда. Модель самая простая, но непрактичная, поскольку любые пользователь и процесс в системе имеют доступ к любым ресурсам, независимо от их конфиденциальности. Один проникший в систему злоумышленник, внешний или внутренний, может получить несанкционированный доступ к информации, которая определяет успешность всего бизнеса организации.

Запретительная – не доверять никому и никогда. Модель также малоприменима на практике, поскольку существенно ограничивает или даже затрудняет выполнение основных функций практически всех слу-

жащих организации, и тогда просто невозможно найти тех, которые согласятся работать в таких условиях.

Компромиссная – доверять иногда некоторым людям и степень доверия периодически пересматривать. Модель определяет доступ ко всем ресурсам по мере необходимости, например по запросам от пользователей или руководства организации. Далее использование предоставленного доступа контролируется с помощью специальных систем, позволяющих регистрировать доступ пользователей и процессов ко всем ресурсам и обнаруживать факты злоупотребления. Эти системы позволяют гарантировать, что доверие не нарушалось. Данная модель, как и все предыдущие, предполагает, что при начале работы в системе все пользователи уведомляются об их правах доступа, а примеры нарушения этих прав становятся общеизвестны всем сотрудникам организации. Из представленных это самая разумная модель.

Выбор конкретной модели доверия, с учетом которой разрабатывается ПолИБ, определяется руководством организации.

Среди других причин, побуждающих организацию разрабатывать ПолИБ, выделим такие [83]:

Требование руководства, обнаружившего недостаток внимания к проблемам ИБ, которые привели к снижению эффективности бизнеса. Нескольких серьезных инцидентов, повлекших за собой остановку или замедление работы компании в результате различных локальных и удаленных атак, разглашение конфиденциальной информации или кража компьютеров существенно стимулируют появление таких требований.

Требования законодательства и отраслевых стандартов. ПолИБ позволяет определить правила, в соответствии с которыми часть информации организации будет отнесена к категории коммерческой или служебной тайны, что позволит защитить ее юридически (статья 139 Гражданского кодекса РФ [88]). В зависимости от сферы деятельности организация должна выполнять требования существующего законодательства ее отрасли. Например, в соответствии со статьей 857 Гражданского кодекса РФ банки должны гарантировать тайну банковского счета и банковского вклада, операций по счету и сведений о клиенте. Страховщики должны защищать тайну страхования (статья 946 ГК РФ) и т. п. Также в соответствии с Указом Президента РФ № 188 от 06.03.97 (с изменениями от 23.09.2005 г.) «Об утверждении перечня сведений конфиденциального характера» организации должны обеспечивать защиту персональных данных сотрудников.

Требования клиентов и партнеров о подтверждении необходимого уровня ОИБ для гарантии того, что их конфиденциальная информация защищена надлежащим образом. Они могут потребовать юридического подтверждения данного факта в контрактах. Именно в ПолИБ есть четкое доказательство намерений организации относительно ИБ.

Необходимость сертификации по стандартам (например, ISO/IEC 9001 [89, 90], 27002, 15408 и т. п.), подтверждающей необходимый уровень ОИБ для защиты информации и бизнес-процессов.

Устранение замечаний аудиторов и выполнение их рекомендаций. Любая внешняя аудиторская проверка обращает внимание на необходимость формализации всех бизнес-процесов, в том числе особое внимание уделяется наличию ПолИБ, на соответствие которой может проводиться аудит.

Обеспечение конкурентоспособности за счет оптимизации бизнес-процессов и увеличения результативности. Правильно разработанная и реализованная ПолИБ позволяет уменьшить время недоступности сервисов, вызванных инцидентами ИБ, таким образом, увеличивая показатель живучести организации.

Демонстрация заинтересованности руководства в ОИБ, что значительно увеличивает приоритет безопасности в глазах сотрудников организации. Без этого они могут не воспринимать ПолИБ всерьез.

Создание корпоративной культуры ИБ и широкое вовлечение сотрудников в процесс ОИБ. Необходимо убедить сотрудников в том, что ОИБ – их прямая обязанность. Это достигается путем введения процедуры обязательного ознакомления с требованиями ПолИБ и подписания соответствующего документа о том, что сотрудник ознакомлен, ему понятны все требования политики и он обязуется их выполнять. ПолИБ позволяет ввести требования по поддержанию необходимого уровня ИБ в перечень обязанностей каждого сотрудника. Также важным условием успеха в области ОИБ становится создание в организации атмосферы, благоприятной для пропаганды и поддержания высокого приоритета ИБ.

Уменьшение стоимости страхования. Страхование – важная составляющая управления информационными рисками. Это метод защиты информации в рамках финансово-экономического обеспечения системы защиты информации, основанный на выдаче страховыми обществами гарантий субъектам информационных отношений по восполнению материального ущерба в случае реализации угроз ИБ. Наличие ПолИБ является необходимым и обязательным условием страхования. В России есть фирмы, предлагающие страховать информационные риски (например, РОСНО, Ингосстрах, РОСТРА и другие). Стоимость страхования определяет путем проведения аудита ИБ независимой организацией, специализирующейся в этой области.

Экономическая целесообразность. ПолИБ является самым дешевым и одновременно самым эффективным средством ОИБ за счет ее последовательного воплощения и дальнейшего соблюдения в каждодневной жизни организации.

Хорошая практика. Наличие ПолИБ сегодня является правилом хорошего тона. Еще в 2002 г. в опросе, проведенном компанией PriceWater HouseCoopers в Великобритании, 67 % компаний выделили именно эту причину создания ПолИБ.

После принятия и утверждения ПолИБ касается каждого сотрудника организации. Большинство людей вполне оправданно могут сопротивляться любым мерам, которые, по их мнению, будут сказываться на результативности их работы. Например, многочисленные процедуры идентификации перед доступом к данным, находящимся в конфиденциальных БД, увеличат время эффективной работы за компьютером. Некоторые люди в силу своего характера могут сопротивляться любым нововведениям и переменам в работе. Часть пользователей может не признавать никаких запретов, ограничивающих свободу их действий, и рассматривать ПолИБ лишь как меру контроля за их поведением (такой контроль в зарубежных научных публикациях имеет свой термин – «синдром старшего брата»). Кроме того, люди боятся, что ПолИБ будет трудно придерживаться и ее будет трудно осуществлять.

Каждый человек имеет свои представления относительно потребности в контроле за безопасностью. Они не всегда совпадают с теми, которые приняты в организации, куда он пришел работать. Если изначально потенциальный сотрудник не разделяет ПолИБ организации, стоит принципиально решать вопрос о его приеме на работу.

Доступ к активам организации предоставляется ее сотрудникам, а также клиентам, подрядчикам, бизнес-партнерам и другим заинтересованным посторонним лицам. Следовательно, пользователями ПолИБ являются все те, кто имеют доступ к активам организации и от деятельности кого зависит обеспечение ее ИБ.

Так кто же должен быть заинтересован в ПолИБ? В первую очередь это сами пользователи – их ПолИБ касается в наибольшей степени, поскольку регламентирует их каждодневную работу. Это вспомогательный персонал систем (системный администратор, администратор ИБ, технический персонал и т. д.) – от них требуется реализовывать на практике и следить за выполнением ПолИБ. И наконец, это руководство организации – именно оно в первую очередь ответственно перед своими сотрудниками, клиентами и заказчиками, обеспокоено относительно репутации организации, заинтересовано в ее процветании в условиях рыночной конкуренции и в защите определяющих это процветание активов. Кроме этого, ПолИБ устанавливает средства управления ИБ в соответствии с ее основными положениями и требованиями, что необходимо для использования в работе различных регулирующих органов, аудиторов ИБ и т. п.

3.3. Основные требования и принципы, учитываемые при разработке и внедрении политики ИБ

ПолИБ как высокоуровневый основополагающий документ определяет систему приоритетов, принципов и методов достижения целей защищенности различных активов организации в условиях наличия для них угроз ИБ. Она содержит основные методологические подходы, позволяющие специалистам в области ИБ и информатизации, а также другим специалистам организации, определить наиболее важные объекты защиты, формулировать принципы и направления работ, разрабатывать необходимые защитные меры. Поэтому формулировать ПолИБ путем выработки четкой позиции в решении вопросов ИБ должно высшее руководство – президент, председатель, директор, совет директоров или иной уполномоченный. Цель ОИБ не может быть достигнута, пока на самом высоком уровне не определено, чего следует добиваться, и не выделены ресурсы, позволяющие должным образом защитить информационную инфраструктуру организации и обеспечить управление ею.

ПолИБ организации разрабатывается на основе накопленного в организации опыта в области ОИБ, результатов идентификации активов, подлежащих защите, оценки рисков ИБ, с учетом особенностей бизнеса и технологий, требований законодательства Российской Федерации, отраслевых нормативных актов, а также интересов и бизнес-целей конкретной организации [11].

Согласно [13, 14, 21, 22] основными требованиями, предъявляемыми к ПолИБ, являются такие:

- ПолИБ должна быть утверждена высшим руководством организации и издана.
- ПолИБ должна быть реализуема (т. е. содержать только те положения, которые могут быть реализованы на практике), а ее реализация контролируема.
- ПолИБ должна быть краткой (лучшие практики указывают на объем не более 10 страниц), простой для понимания и не допускать двойного толкования ее положений.
- ПолИБ должна обеспечивать защиту и при этом не влиять на эффективность работы сотрудников организации, т. е. не снижать результативность их работы.
- ПолИБ должна устанавливать ответственность руководства и излагать подход организации к управлению ИБ.
- ПолИБ должна регулярно (через запланированные промежутки времени, по графику) анализироваться. Анализ должен включать в себя оценивание возможностей для улучшения ПолИБ и подход к управлению ИБ в ответ на изменения в организационном окружении, деловых обстоятельствах, юридических условиях или в технической

среде. Анализ ПолИБ должен учитывать результаты ее анализа со стороны руководства.

- В случае возникновения значительных изменений в текущем развитии организации с целью обеспечить соответствие, адекватность и результативность ПолИБ, она должна пересматриваться и модифицироваться согласно разработанной заранее процедуре. Периодические пересмотры должны включать проверку соответствия ПолИБ актуальной законодательной базе, оценку ее эффективности, исходя из характера, числа и последствий зарегистрированных инцидентов ИБ, определение стоимости мероприятий по управлению ИБ и их влияние на бизнес, анализ влияния изменений в технологиях на деятельность организации. Такая процедура должна обеспечивать осуществление пересмотра ПолИБ в соответствии с изменениями, затрагивающими первоначальную оценку рисков ИБ, например, путем выявления существенных инцидентов ИБ, появления новых уязвимостей или изменения организационной или технологической инфраструктуры организации.
- Должно быть назначено ответственное за ПолИБ должностное лицо, которое отвечает за ее реализацию и пересмотр в соответствии с установленной процедурой.
- ПолИБ должна быть надлежащим образом доведена в доступной и понятной форме до сведения всех сотрудников организации, с которой они должны ознакомиться чаще всего под расписку. Программа обучения в области ИБ и контрольные проверки действий в тех или иных ситуациях могут достаточно эффективно демонстрировать всем пользователям действенность соблюдения ПолИБ.
- Чтобы быть эффективной, ПолИБ должна быть наглядной. Это способствует реализации политики, помогая гарантировать ее знание и понимание всеми сотрудниками организации. Видеофильмы, семинары, статьи во внутренних изданиях организации или на ее внутреннем веб-узле увеличивают такую наглядность.
- ПолИБ должна быть обязательно согласована с общепризнанными основами теории ИБ, со всеми существующими нормативно-правовыми документами, соблюдение которых требуется от организации в стране ее функционирования, а также директивами, законами, приказами и общими задачами самой организации. Она должна быть интегрирована в общую политику организации и согласована с другими политиками (например, политикой приема/найма на работу).
- При распространении ПолИБ за пределы организации следует позаботиться о том, чтобы не раскрыть важную (конфиденциальную, критичную) информацию (англ. *sensitive information*), потеря, раскрытие или уничтожение которой по тем или иным причинам нежелательны для бизнеса или её владельца.

- Пересмотренная ПолИБ также должна быть утверждена руководством.

Выполняя перечисленные требования, можно разработать действительно эффективную ПолИБ, которая обладает следующими свойствами:

- определяет необходимый и достаточный набор требований по ОИБ, позволяющих уменьшить риски ИБ до приемлемой величины;
- основывается на первоначально проведенном анализе рисков ИБ, определенном оптимальном уровне риска для организации на основе заданного критерия;
- оказывает минимальное влияние на производительность труда;
- учитывает особенности бизнес-процессов организации;
- поддерживается руководством;
- позитивно воспринимается и исполняется сотрудниками.

Разрабатываемая ПолИБ обязательно отражает следующие принципы, которыми целесообразно руководствоваться при ее использовании и поддержании ИБ в организации на требуемом уровне [80, 85, 91]:

Законность, то есть осуществление защитных мер в соответствии с действующим законодательством в области ИБ, другими нормативными актами по ОИБ, утвержденными органами государственной власти, с применением всех дозволенных методов обнаружения и пресечения правонарушений.

Определенность целей, сформулированных в ПолИБ.

Системность, позволяющая учесть все взаимосвязанные и изменяющиеся во времени элементы, условия и факторы, значимые для поддержания ИБ в организации, включая все объекты защиты и направления нарушений ИБ, уязвимости используемых систем, высокую квалификацию злоумышленника и т. п.

Комплексный (мультидисциплинарный) подход к разработке ПолИБ, позволяющий учитывать правовые, технические, административные, организационные, учебные, коммерческие и функциональные вопросы;

Научная обоснованность и техническая реализуемость защитных мер, что позволяет реализовать их на современном уровне развития науки и техники для достижения заданного уровня ИБ, соответствующего установленным нормам и требованиям по ОИБ.

Эшелонированность (многоуровневость) обороны (англ. *defence in depth*) и *разнообразие защитных средств* (нельзя полагаться на один защитный рубеж, каким бы надежным он ни казался: в интранете за средствами физической защиты должны следовать программно-технические средства, за идентификацией и аутентификацией – управление доступом, и как последний рубеж – протоколирование и аудит); тогда злоумышленник для взлома системы должен владеть разнообразными знаниями и навыками.

Способность защитных мер к интеграции для наиболее эффективного выполнения требования ПолИБ и *согласованность (скоординированное функционирование) применения различных защитных мер* при построении целостной системы защиты организации, отсутствие слабых мест при стыковке различных защитных мер, покрытие ими всех объектов защиты, в случае наступления инцидента ИБ.

Эффективность и непрерывность защиты, предполагающая целенаправленный непрерывный процесс принятия соответствующих мер на всех этапах жизненного цикла организации.

Разумная достаточность, позволяющая выбрать золотую середину между стойкостью защиты и ее стоимостью, потреблением вычислительных ресурсов, удобством работы пользователей и другими характеристиками защитных мер.

Своевременность, адекватность и пропорциональность защитных мер, определенных в ПолИБ, реальным угрозам и рискам ИБ.

Риск-ориентированный подход при разработке ПолИБ.

Гибкость управления и применения защитных мер, позволяющая варьировать уровень защищенности в зависимости от текущей ситуации и потребности организации в ИБ в данный период времени; гибкость также важна, когда установку средств защиты необходимо осуществлять на уже работающую систему, не нарушая процесса ее нормального функционирования.

Невозможность миновать защитные средства (применительно к интранет это означает, что все информационные потоки в защищаемый интранет и из него должны проходить через средство фильтрации – МЭ; не должно быть «тайных» модемных входов или тестовых линий, идущих в обход него).

Усиление самого слабого звена, выявляемого при регулярном обследовании защищаемых активов организации (злоумышленник предпочитает легкую победу; часто самым слабым звеном оказывается не компьютер или ПО, а человек; тогда проблема ОИБ приобретает нетехнический характер).

Простота и управляемость защитных средств (защитные средства должны быть интуитивно понятны и просты в использовании; только для простого защитного средства можно доказать его корректность; только в простой и управляемой системе можно проверить согласованность конфигурации различных компонентов и осуществить централизованное администрирование).

Невозможность перехода защитных средств в небезопасное состояние, т. е. при любых обстоятельствах, в том числе нештатных, они либо полностью выполняют свои функции, либо полностью блокируют доступ к особо важным активам организации.

Наблюдаемость и контролируемость защитных мер (любые предлагаемые защитные меры должны быть устроены так, чтобы результат их применения был явно наблюдаем (прозрачен) и мог быть оценен подразделением организации, имеющим соответствующие полномочия).

Обязательность контроля (мониторинга и аудита) защитных мер и соблюдения ПолИБ, позволяющая своевременно выявлять и пресекать попытки ее нарушения на основе используемых защитных мер при совершенствовании критериев и методов оценки их эффективности с учетом влияния защитных мер на бизнес-цели организации.

Совершенствование защиты за счет периодической переоценки защитных мер и потребности в них.

Разделение полномочий (обязанностей) – распределение ролей и ответственности, при котором ни один человек не имеет полномочий, позволяющих ему единолично осуществлять выполнение критичных операций, и не может нарушить критически важный для организации процесс или создать уязвимость в защите по заказу злоумышленников (важно, например, для предотвращения злонамеренных или неквалифицированных действий системного администратора, сговора между сотрудниками).

Минимизация полномочий и привилегий, предписывающая выделять пользователям и администраторам систем и ИБ только те права доступа, которые необходимы им для выполнения служебных обязанностей (цель – уменьшить ущерб от случайных или умышленных некорректных действий).

Рассмотрение как *персональной* (для каждого сотрудника в пределах его полномочий), *так и групповой ответственности* в случаях инцидентов ИБ, когда распределение прав и обязанностей сотрудников строится таким образом, чтобы в случае любого нарушения круг виновников был четко известен или сведен к минимуму.

Обеспечение всеобщей поддержки защитных мер, предусматривающее комплекс мер, направленный на обеспечение лояльности персонала и его постоянное теоретическое и практическое обучение (если сотрудники организации считают ИБ чем-то излишним или даже враждебным, то режим безопасности сформировать не удастся).

Информированность, т. е. каждый должен иметь возможность ознакомиться с положениями ПолИБ, знать о тех мерах, практиках и процедурах, на которые она ссылается.

Соблюдение этики и учет различных прав и законных интересов сотрудников организации, включая право на частную жизнь.

Этот список достаточно полон, но при необходимости он может быть расширен с учетом особенностей организации и сферы ее деятельности.

3.4. Содержание политики ИБ

ПолИБ только определяет, *что* должно быть защищено и какова ответственность в случае несоблюдения ее положений. Защитные меры определяют, *как* конкретно защитить активы организации. Они являются механизмами реализации ПолИБ на практике и представляют собой полный перечень всех рекомендаций и действий, которые должны предприниматься в определенных обстоятельствах и при определенных условиях. Защитные меры выбираются таким образом, чтобы устранить так называемую проблему *одной точки провала* (например, служащий внезапно уволился и его функции по реализации ПолИБ никому не передали, или вышло из строя и не подлежит восстановлению какое-то средство защиты).

ПолИБ содержит общие требования по ОИБ организации в целом. При этом обязательно учитываются особенности организации и ее деятельности, а также выделяются основные направления, связанные с ОИБ организации, и формулируются общие (основные) требования по каждому из этих направлений.

Еще один важный момент – каков будет вид представления и состав документации, определяющей ПолИБ. ПолИБ может быть описана в одном большом или нескольких небольших документах. Несколько не очень объемных документов чаще предпочтительнее, так как их проще при необходимости обновлять. Для организаций небольшого размера, конечно же, легче изложить всю ПолИБ в одном документе.

В тексте ПолИБ обязательно в явном виде присутствуют ответы на следующие вопросы: что (цель политики), кто (на кого она распространется), где (ее область действия), как (факторы соблюдения и оценка соблюдения политики), когда (когда политика вступает в действие), почему (необходимость внедрения политики).

Основное содержание ПолИБ наглядно представлено рис. 3.3 [17].

Рис. 3.3. Содержание ПолИБ организации

Выработка набора конкретных ПолИБ зависит от размера и целей организации, их принимающей. Они должны по возможности носить не рекомендательный, а обязательный характер. Ответственность за их нарушение должна быть четко определена.

Для автоматизации процесса создания ПолИБ и их проверки на соответствие некоторым наиболее популярным международным стандартам предназначены, например, британская система Cobra компании

C&A Systems Security Ltd [www.riskworld.net] и российская система КОНДОР 2006 компании Digital Security [www.dsec.ru].

Далее, систематизируя рассмотренные в первой главе международные и национальные стандарты в области ИБ и имеющийся многолетний мировой опыт разработки действительно «работоспособных» ПолИБ, определим содержание корпоративной ПолИБ и двух видов частных ПолИБ – по конкретным вопросам и для конкретных систем.

3.4.1. Содержание корпоративной политики ИБ

По своему назначению корпоративная ПолИБ является каркасом, объединяющим все остальные документы, регламентирующие обеспечение и управление ИБ в организации. В нее рекомендуется включать следующие положения [75]:

1. Определение ИБ в терминах деятельности данной организации, области действия политики, целей, задач и принципов ОИБ организации.

2. Изложение намерения ОИБ, направленного на достижение указанных целей и на реализацию принципов ОИБ.

3. Общие сведения об активах, подлежащих защите, их классификацию.

4. Модели угроз и нарушителей (внутреннего и внешнего) ИБ, на противодействие которым ориентирована корпоративная ПолИБ.

5. Высокоуровневое изложение правил и требований по ОИБ, представляющих особую важность для организации (например, обеспечение соответствия законодательным актам, нормативным документам РФ в области ОИБ и нормативным актам организации; требования к управлению ИБ; требования по предотвращению и обнаружению компьютерных вирусов и другого вредоносного ПО; требования по УНБ).

6. Санкции и последствия нарушений корпоративной ПолИБ.

7. Определение общих ролей и обязанностей, связанных с ОИБ, включая информирование об инцидентах ИБ.

8. Перечень частных ПолИБ, развивающих и детализирующих положения корпоративной Пол ИБ, а также указание подразделений организации, ответственных за их соблюдение и/или реализацию.

9. Положения по контролю реализации корпоративной ПолИБ организации.

10. Ответственность за реализацию и поддержку документа.

11. Условия пересмотра (выпуска новой редакции) документа.

К разработке и согласованию корпоративной ПолИБ рекомендуется привлекать представителей следующих служб организации, связанных с ее информационной сферой: руководство организации; профильные подразделения; служба информатизации; служба безопасности (ИБ).

Корпоративная ПолИБ обязательно утверждается руководителем организации (например, председателем, генеральным директором, президентом) и в ее названии указывается название организации, которой она

принадлежит. Она может быть представлена как комплектом документов, так и единым обобщающим документом.

Согласно представленному в справочнике по компьютерной безопасности Национальным институтом стандартов и технологий еще в 1995 г. описанию, *корпоративная ПолИБ как политика верхнего уровня должна включать в себя следующие разделы* [84].

Цель (назначение). Корпоративная ПолИБ обычно содержит утверждение, поясняющее, зачем она была разработана. Всегда полезно явно указать цель или причины ее написания. Например, если организация предоставляет услуги по поддержке больших БД, тогда ее основными целями могут быть снижение числа ошибок, потери и искажения данных, а также быстрота восстановления после нештатных ситуаций. Для организации, обрабатывающей персональные данные, первостепенной задачей может быть усиленная защита от несанкционированного раскрытия информации о клиентах [78, 79]. Поэтому типовыми являются следующие цели:

- обеспечение устойчивого функционирования организации за счет предотвращения реализации угроз ИБ ее активам, защита законных интересов владельца информации от противоправных посягательств, обеспечении нормальной производственной деятельности всех подразделений организации;
- обеспечение уровня ИБ в конкретных функциональных областях, соответствующего нормативным документам организации и рассчитанного на основе риск-ориентированного подхода (с учетом результатов оценки рисков ИБ);
- выработка планов восстановления после критических ситуаций и ОНБ организации и другие;
- достижение экономической целесообразности в выборе защитных мер;
- реализация подотчетности анализа регистрационной информации и всех действий пользователей с информационными ресурсами и т. п.

Задачами ОИБ являются все действия, которые необходимо выполнить для достижения поставленных целей. В частности, необходимо решать такие задачи, как анализ и управление рисками ИБ, расследование инцидентов ИБ, разработка и внедрение планов ОНБ, повышение квалификации и осведомленности сотрудников в области ИБ и т. д.

Область действия. Перед изложением самой ПолИБ определяется область ее действия с помощью ограничений и условий в понятных всем терминах, которые вводятся в явном виде. Надо уточнить, где, как, когда, кем и к чему применяется данная ПолИБ. Если, например, говорить о ПолИБ при подключении организации к Интернету, то может понадобиться уточнение, какие соединения, через которые ведется работа с Интернетом (напрямую или опосредованно), охватывает эта политика. ПолИБ также может определять, учитываются ли другие аспек-

ты работы в Интернете, такие как соединение с Интернетом с домашнего компьютера.

ПолИБ точно определяет, какие активы организации она затрагивает – персонал, информацию, ПО и АО, устройства, технологии и т. п. Например, защищаемые в рамках ПолИБ активы организации можно описать так: «Положения настоящей ПолИБ распространяются на все виды информации, хранящиеся или передающиеся в организации. В том числе на информацию, зафиксированную на материальных носителях или передающуюся в устной или визуальной форме». Но во многих случаях корпоративная ПолИБ имеет отношение ко всем системам и всем сотрудникам организации без исключения.

Основные положения ПолИБ. В явной форме описывается позиция организации (то есть решение ее руководства) по данному вопросу. Позиция может быть сформулирована как в наиболее общем виде как набор целей, которые преследует организация в данном аспекте, так и конкретизирована.

В ПолИБ требуется кратко описать все процессы и процедуры СУИБ. В частности, выделяются такие процедуры, как контроль доступа к активам организации, внесение изменений в ее ИС, взаимодействие с третьими лицами, повышение квалификации сотрудников в области ИБ, расследование инцидентов ИБ, аудит ИБ. В описании каждой процедуры необходимо четко определить цели и задачи процедуры, основные правила ее выполнения, регулярность или сроки выполнения.

Перечисляются конкретные меры, реализующие ПолИБ в организации, дается обоснование выбора именно такого перечня мер и указывается, какие угрозы ИБ для активов наиболее эффективно предотвращаются данными защитными мерами.

С целью формализации процесса управления ИБ в соответствии с ПолИБ требуется создание организационной структуры, которую также требуется описать.

Необходимо предусмотреть период пересмотра ПолИБ, что может быть изложено, например, следующим образом: «Положения Политики ИБ требуют регулярного пересмотра и корректировки не реже одного раза в полгода. Внеплановый пересмотр Политики ИБ проводится в случаях:

- существенных изменений в национальной законодательной базе в области ИБ;
- внесения существенных изменений в интранет организации;
- возникновения инцидентов ИБ.

При внесении изменений в положения Политики ИБ организации учитываются:

- результаты анализа функционирования СУИБ со стороны руководства организации;
- результаты аудита ИБ (внешнего и внутреннего);
- рекомендации независимых экспертов по ИБ».

Ответственность (*роли и обязанности*). В этом разделе ПолИБ точно устанавливается, кто и за что отвечает. Фраза «За ОИБ несут ответственность все сотрудники организации» на практике мало что означает. Указывается, на кого конкретно возлагается ответственность за соблюдение ПолИБ (например, менеджеров, владельцев активов, пользователей, администраторов систем и т. д.). Если для использования ПО сотрудникам требуется разрешение руководства, должно быть известно, у кого и как его можно получить.

Для ПолИБ уместно описание (с краткой детализацией) нарушений, которые неприемлемы, и последствий такого поведения. Могут быть явно перечислены наказания, применяемые к нарушителям ПолИБ (предварительно их нужно согласовывать с соответствующими должностными лицами и отделами и законодательными актами).

За нарушение ПолИБ должны быть предусмотрены конкретные дисциплинарные, административные взыскания и материальная ответственность. Но при этом нельзя забывать, что нарушения ПолИБ бывают и непреднамеренными со стороны сотрудников – они могут быть связаны, например, с отсутствием соответствующих знаний.

Устанавливаются как организационные, так и технические меры реагирования на нарушение ПолИБ. Эти меры предусматривают оповещение об инциденте ИБ, соответствующую реакцию, процедуры восстановления, сбор доказательств, проведение расследования и привлечение нарушителя к ответственности. Система мер по реагированию на инциденты ИБ должна быть скоординирована между ИТ-департаментом, службой безопасности и службой персонала.

Также полезно поставить задачу конкретному подразделению организации следить за соблюдением ПолИБ. Кроме этого, приводится информация о должностных лицах, ответственных за реализацию ПолИБ, и четко устанавливаются их обязанности в отношении разработки и внедрения различных аспектов ПолИБ, а также в случае нарушения политики. Обязанность за общее управление ИБ возлагается на руководство организации. Ответственность сторонних пользователей обязательно оговаривается в соответствующих договорах. Отдельно описывается ответственность за контроль соблюдения ПолИБ.

Соблюдение ПолИБ. Это выражается в соблюдении двух видов соответствий:

1. Общее соответствие, обеспечивающее выполнение требований по разработке ПолИБ и определению ответственности, возложенной на различные организационные структуры поддержания ИБ. Часто на отдел надзора возлагается ответственность за контроль за соблюдением такого соответствия, в том числе, насколько хорошо организация реализует приоритеты руководства, установленные в ПолИБ.

2. Использование только установленных наказаний и дисциплинарных мер. Поскольку ПолИБ – это высокоуровневый документ, то кон-

кретные меры наказания за различные нарушения, как правило, не детализированы в корпоративной ПолИБ. Поэтому политика может разрешить создание соответствующих структур, которые будут заниматься нарушениями и реализацией конкретных дисциплинарных мер.

Ответственные (консультанты) по вопросам ИБ и справочная информация. Для любой ПолИБ нужны консультанты, с кем можно связаться в случае необходимости и получить квалифицированную помощь, разъяснения и дополнительную информацию по вопросам ОИБ. Можно назначить сотрудника, занимающего конкретную должность консультанта. Например, по некоторым вопросам консультантом может быть один из менеджеров, по другим – начальник отдела, сотрудник технического отдела, системный администратор или сотрудник службы ИБ. Они должны уметь разъяснять положения ПолИБ и правила работы с конкретной системой. В их обязанности входит ознакомление всех новых служащих организации с ПолИБ при поступлении на работу и сообщение об изменениях в политике по мере их внесения. Также должно вестись обучение всех сотрудников основным вопросам ОИБ, а администратор и сотрудники отдела ИБ организации должны регулярно проходить переподготовку с целью повышения квалификации в специализирующихся в этих вопросах учебных заведениях.

Более современными общепризнанными стандартами, описывающими общее содержание комплексной ПолИБ организации (в контексте данного учебного пособия – корпоративной ПолИБ) являются ISO/IEC 27002:2005 [22] и ГОСТ Р ИСО/МЭК 17799–2005 [13]. В этих документах отмечается, что ПолИБ как неотъемлемая часть общей политики организации включает, как минимум, следующее:

1) определение ИБ, ее общих целей и области действия, а также раскрытие значимости безопасности как инструмента, обеспечивающего возможность совместного использования информации;

2) изложение целей и принципов ИБ, сформулированных руководством, и соответствующих бизнес-стратегии и целям организации, включая вопросы оценки и управления рисками ИБ;

3) краткое изложение и разъяснение наиболее существенных для организации политик, принципов, правил и требований, например: соответствие законодательным требованиям и договорным обязательствам; требования в отношении обучения вопросам ИБ; предотвращение появления и обнаружение вирусов и другого вредоносного ПО; УНБ; последствия нарушений и ответственность за нарушения ПолИБ;

4) определение общих и конкретных обязанностей сотрудников в рамках управления ИБ, включая информирование об инцидентах ИБ;

5) ссылки на документы, дополняющие ПолИБ, например, более детальные политики и процедуры безопасности для конкретных ИС, а также правила безопасности, которым должны следовать пользователи.

3.4.2. Содержание частных политик ИБ

Содержания частных ПолИБ по перечню разделов не отличаются от таковых для корпоративной ПолИБ [84]. Все их положения ни в коем случае не должны вступать в противоречия с корпоративной ПолИБ и формируются на основании принципов, требований и задач, определенных в корпоративной ПолИБ, с учетом:

- детализации, уточнения и дополнительной классификации активов и угроз ИБ;
- определения владельцев защищаемых активов;
- оценки рисков ИБ и возможных последствий реализаций угроз ИБ в границах области действия регламентируемой политикой области, системы, технологии, подразделения и т. п.

Не рекомендуется повторение одинаковых правил в различных частных политиках. Включение в частную ПолИБ правила, содержащегося в другой существующей политике, целесообразно осуществлять посредством соответствующей ссылки.

Согласно [75] частные ПолИБ определяют следующее:

- цели и задачи ОИБ, на обеспечение которых направлена частная ПолИБ;
- область действия, определение объектов защиты, уязвимостей, угроз ИБ и оценка рисков ИБ, связанных с объектами защиты;
- сведения о виде деятельности, на ОИБ которой направленно действие положений частной ПолИБ, совокупности банковских технологий, применяемых в рамках выполнение данного вида деятельности, и основных технологических процессов, реализующих указанные технологии;
- определение субъектов (ролей), на которых распространяется действие политики (как структурных подразделений организации, так и отдельных исполнителей);
- содержательную часть (требования и правила);
- обязанности по ОИБ в рамках области действия частной ПолИБ, описание функций субъектов (ролей) над управляемыми объектами в рамках регламентируемых технологических процессов;
- состав ссылочных документов (документы, ознакомление с которыми обязательно для адекватного понимания текста политики);
- положения по контролю реализации политики;
- ответственность за реализацию и поддержку политики;
- условия пересмотра политики.

Обобщая лучшие мировые практики написания частных ПолИБ, более подробно рассмотрим ***ПолИБ по конкретному вопросу (проблеме, области)***. Также как и корпоративная, данная ПолИБ обычно распространяется на организацию в целом.

Описание вопроса. Чтобы сформулировать такую ПолИБ, сначала необходимо описать проблему с учетом принятой терминологии, её особенностей и условий успешного разрешения. Кроме того, часто бывает полезно указать цели или обоснование политики, которые могут быть полезны при ее реализации. Например, организации нужно разработать политику использования «неофициального» ПО, под которым понимается любое ПО, не одобренное официально, не переданное, не администрируемое и не находящееся в собственности организации. Кроме того, должны быть оговорены некоторые условия, например, для ПО, находящегося в собственности сотрудников, но одобренного для использования в их работе, и для ПО бизнес-партнеров организации.

Описание позиции организации. Четко излагается позиция организации (т. е. решение руководства) по данному вопросу. Продолжая предыдущий пример, это будет означать заявление, когда использование неофициального ПО запрещено – во всех или отдельных случаях, есть ли дополнительные руководящие указания по его возможному утверждению и использованию, возможны ли некоторые исключения из правил, когда, как и на какой основе их получить.

Применимость. Здесь уточняется, где, как, когда, к кому и какая конкретно политика применяется. Например, это может означать, что упомянутая политика использования неофициального ПО предназначена для применения только в основном офисе организации его сотрудниками и не применима к сотрудникам офисов, расположенных в других регионах. Кроме того, необходимо уточнение применения политики к сотрудникам, работающим в нескольких офисах и/или на дому.

Роли и ответственность. Например, если политика позволяет после соответствующего согласования использовать в работе неофициальное ПО, находящееся в собственности работников, то должно быть указано, как и где официально получить такое разрешение. Также необходимо уточнить, кто будет нести ответственность за обеспечение того, чтобы только рекомендованное ПО используется на компьютерах организации и, возможно, осуществлять мониторинг компьютеров с целью обнаружения неофициального ПО.

Вопросы соответствия. Для некоторых типов политики может быть целесообразно описать, с некоторыми деталями, неприемлемые нарушения и последствий такого поведения. Наказания могут быть сформулированы вполне конкретно и должны быть согласованы с кадровой политикой организации, соответствующими должностными лицами и ведомствами и, возможно, общественными организациями (например, профсоюзами). Желательно, чтобы какое-либо подразделение организации осуществляло контроль за таким соответствием.

Контактные лица и дополнительная информация. Конкретные фамилии в данном разделе не указываются, а пишутся только должности

лиц, к которым следует обращаться за дополнительной информацией и разъяснениями.

В поддержку рассмотренной политики обычно создаются руководства и описываются процедуры. Для рассмотренного примера может быть создано руководство по проверке дисков и других мобильных устройств, приносимых сотрудниками из дома или привозимых из командировки в другой офис.

ПолИБ для конкретной системы особенно важна для использования и обеспечения ИБ этой системы. В разных подразделениях организации могут использоваться различные системы (например, информационные), поэтому данная политика чаще всего имеет более узкую направленность, чем корпоративная. Она обязательно должна учитывать позицию тех, кто с этими системами непосредственно работает.

Разработать последовательную ПолИБ для конкретной системы можно, только выводя правила из целей ОИБ в поддержку основного назначения самой системы. Поэтому для такой ПолИБ полезно рассмотреть двухуровневую модель: цели ОИБ и функциональные правила ОИБ, которые тесно взаимосвязаны и часто трудно различимы с технической точки зрения их осуществления.

Цели ОИБ системы. Процесс их определения начинается с анализа потребности в обеспечение конфиденциальности, целостности и доступности для достижения основных целей использования системы. Но только такой формулировки не достаточно – цели должны быть указаны более конкретно. Они должны быть достижимы на практике и согласованы с целями других политик организации. Цели формулируются в виде ряда утверждений в отношении защищаемых ресурсов, с которыми работает система. Они должны учитывать допустимые в организации затраты на их достижение, а также функциональные, технические и другие ограничения.

Роли по ОИБ системы. Детализируются и формализуются правила назначения ответственности за ОИБ, правила использования системы и последствия их несоблюдения. Выделяются правила функционирования системы. Например, определяется санкционированное и несанкционированное изменение ее настроек, кто (по должности, рабочему положению и т. п.) может вносить санкционированные изменения (например, модифицировать, уничтожать и т. д.), в какие типы данных и при каких условиях. Степень детализации этих положений может быть различна. Чем более точно установлены правила, тем проще выявить, когда и кем они были нарушены, и автоматизировать обнаружение таких событий. Это создает определенные вычислительные сложности, поэтому при установлении, например, прав доступа лучше всего пользоваться принципом разумной достаточности.

Любые обоснованные отклонения от соблюдения корпоративной ПолИБ или общей практики при работе с рассматриваемой системой должны быть оговорены.

Реализация политики. Описываются все аспекты ОИБ системы, включая организационные, технические и другие. Ограничение физического доступа в помещения, контроль логического доступа, системы обнаружения вторжений (СОВ), защита компьютеров от загрузки с дискет, контроль за работой ПО, регулярный внутренний аудит – лишь некоторые из средств, которые могут участвовать в реализации политики на практике.

Для большей наглядности изложенного в Приложении приведены примеры некоторых частных ПолИБ, разработанные на основе англоязычного материала сайта организации SANS [www.sans.org/ security-resources/policies/].

3.5. Жизненный цикл политики ИБ

Опыт разработки ПолИБ показывает, что жизненный цикл любой из них начинается с определения состава группы разработки и функций каждого сотрудника, входящего в нее. Сразу же решается, кто в дальнейшем будет знакомить с ней сотрудников организации и следить за ее реализацией, какие меры будут применяться к тем, кто ее нарушает, а также какова периодичность и каков порядок пересмотра ПолИБ в зависимости от изменяющихся условий ведения бизнеса организации (это связано с тем, что соблюдение адекватной ПолИБ в течение длительного времени является практически невыполнимой задачей, так как меняется как окружающая среда, так и сама организация: модифицируются ее активы, информационная инфраструктура и т. п.).

Следующий шаг – это способ выработки ПолИБ, то есть на основе какой информации будет определяться политика, кем эта информация предоставляется и какова степень доверия к ней. Как показывает практика, нельзя включать в рассмотрение те факторы, которые часто меняются. И нельзя сводить ПолИБ лишь к детальному плану реализации основных мер по защите всех активов организации (например, недопустима ориентация на конкретные средства защиты и указание конкретных версий продуктов конкретных производителей, иначе при появлении новых версий и выпуске средств новых производителей придется пересматривать всю ПолИБ).

На этом этапе создания ПолИБ необходимо получить ответы руководства, клиентов и пользователей отдельных сервисов организации и всех заинтересованных лиц на следующие вопросы. Какие ожидания пользователи и клиенты возлагают на ОИБ организации? Потеряет ли организация клиентов, если ее ИБ будет обеспечена недостаточно серьезно или если она будет обеспечена настолько серьезно, что это затруд-

нит выполнение ими их обычных обязанностей? Сколько времени простоя или какие материальные потери уже принесли нарушения ИБ организации в прошлом? Обеспокоена ли организация угрозами ИБ, исходящими от внутренних пользователей? Может ли она доверять своим пользователям? Сколько конфиденциальной информации находится в интерактивном режиме доступа (on-line) в сети организации? Каковы предполагаемые потери организации, если эта информация будет скомпрометирована или украдена? Нужны ли организации различные уровни ИБ для разных подразделений и категорий пользователей? Существуют ли в организации руководящие принципы, регламентирующие ОИБ, инструкции или законы, которые требуется выполнять? Если да, то следуют ли этим руководящим принципам и правилам в организации? Имеют ли требования основного бизнеса организации приоритет над требованиями по ОИБ при их несоответствии? Если да, то поощряется ли такой подход в организации? Насколько важны конфиденциальность, целостность и доступность информации для полноценной работы организации? Являются ли решения, которые принимаются в организации, соответствующими потребностям ее бизнеса и ее экономическому положению?

После ответа на все эти и, несомненно, другие важные вопросы определяется содержание самой ПолИБ и начинается ее написание.

Упрощенный взгляд на разработку и реализацию ПолИБ представлен на рис. 3.4.

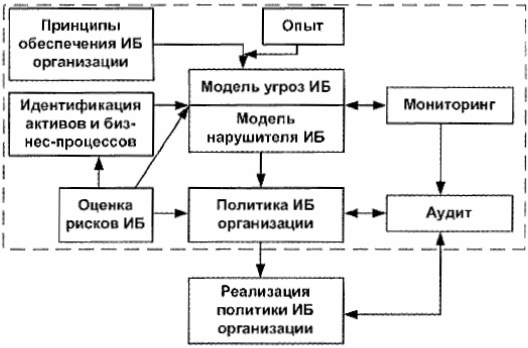

Рис. 3.4. Разработка и реализация ПолИБ

Руководствуясь признанными в организации принципами ОИБ, проведя идентификацию активов и бизнес-процессов, оценив риски ИБ, учитывая собственный опыт и лучшие мировые практики, извлекая уроки по результатам постоянного мониторинга ИБ, разрабатываются две модели ИБ – угроз ИБ и нарушителей ИБ. Все это вместе является осно-

вой ПолИБ. После соответствующих процедур согласования и утверждения ПолИБ вступает в силу, реализуется силами всех определенных заранее должностных лиц и соблюдается всеми, к кому она применима. ПолИБ является основным документом, выполнение которого на практике оценивается при проведении аудита ИБ (как внешнего, так и внутреннего) и каждодневного мониторинга событий, влияющих на ИБ.

При более детальном рассмотрении в жизненном цикле ПолИБ можно выделить четыре основных стадии: разработка, внедрение, применение и аннулирование и соответствующие им одиннадцать шагов, которые нужно выполнить при работе с ПолИБ – начиная с написания и заканчивая изъятием из обращения (рис. 3.5) [80].

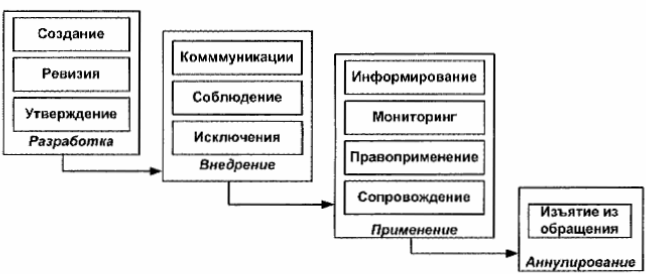

Рис. 3.5. Стадии жизненного цикла ПолИБ

На стадии разработки ПолИБ пишется, в нее вносятся одобренные после обсуждения в коллективе и с руководством коррективы и в соответствии с определенной заранее процедурой ПолИБ утверждается. Затем на стадии внедрения ПолИБ доводится до сведения всех заинтересованных лиц (сотрудников, бизнес-партнеров, клиентов), обеспечивается ее соответствие всем необходимым стандартам, нормам и требованиям и непосредственное соблюдение, а также определяются исключительные случаи (исключения), когда она не выполнима. На стадии применения ПолИБ поддерживается в актуальном состоянии (в нее вносятся соответствующие текущему уровню развития организации изменения), ее основные положения с изменениями доводятся до сведения всех заинтересованных лиц, а также постоянно проверяется ее соответствие всем установленным требованиям. Также должным образом контролируется исполнение ПолИБ всеми, на кого она распространяется. И, наконец, на стадии аннулирования, чаще всего после ее замены новой редакцией или совершенно новым по содержанию документом, ПолИБ изымается из обращения в связи с ненадобностью.

Все шаги жизненного цикла ПолИБ должны быть выполнены обязательно, а некоторые из них, такие как сопровождение, информирование,

мониторинг соблюдения и правоприменение, выполняются итерационно во время всего жизненного цикла.

Анализируя стандарты и лучшие практики применения ПолИБ, опишем в виде подробных практических рекомендаций с необходимыми обоснованиями выделенные выше стадии и входящие в них шаги.

3.5.1. Разработка политики ИБ

Разработка ПолИБ – длительный и трудоемкий процесс, требующий высокого профессионализма, отличного знания нормативной базы в области ИБ и, помимо всего прочего, писательского таланта. Не всегда создание ПолИБ нужно начинать с нуля. Во многих случаях можно воспользоваться существующими наработками, ограничившись адаптацией типового комплекта ПолИБ к специфическим условиям конкретной организации. Этот путь часто позволяет сэкономить многие месяцы работы и повысить качество разрабатываемых документов. Кроме того, он является единственно приемлемым в случае отсутствия в организации собственных ресурсов для квалифицированной разработки ПолИБ.

Сначала разрабатывается корпоративная ПолИБ, затем частные политики.

Как было отмечено выше, в стадию разработки ПолИБ входят ее создание и согласование (включая коррекцию), ревизия и утверждение.

Создание, или написание ПолИБ. Это самый четко формализованный шаг жизненного цикла ПолИБ, который включает в себя деятельность по планированию, проведению различных исследований, документированию необходимой информации и написанию самой ПолИБ. На данном шаге обязательно осуществляются следующие мероприятия:

- определяется, зачем ПолИБ нужна в организации (например, в соответствии с правовыми требованиями или требованиями регулирующих органов);
- устанавливаются границы и область действия;
- выделяются роли и ответственность, связанные с реализацией и внедрением ПолИБ;
- назначается группа конкретных людей, которые будут участвовать во всех процессах создания политики;
- оценивается осуществимость реализации ПолИБ.

Также выявляется применимость различных требований к разработке ПолИБ конкретной организации (требования утверждающих политику, требования по ее согласованию, формат и т. д.) и проводятся исследования в соответствии со стандартизованными для различных отраслей лучшими практиками.

По мере необходимости осуществляется координация деятельности между всеми участвующими в процессе создания ПолИБ сторонами как внутри, так и вне организации. Буклет SAGE «A Guide to Developing

Computing Policy Documents» рекомендует следующий состав рабочей группы по разработке ПолИБ [92]:

- член совета директоров;
- представитель руководства организации (президент, директор, финансовый директор, директор по развитию и т. п.);
- директор департамента информатизации (автоматизации);
- директор департамента ИБ;
- представитель юридического отдела;
- аналитик ИТ-службы;
- аналитик службы безопасности;
- представитель пользователей;
- технический писатель.

Результатом данного шага является написанная политика, соответствующая стандартам и процедурам, принятым в организации.

Ревизия, или независимая оценка, ПолИБ. Как показывает практика, желательно, чтобы до начала ее использования в организации ПолИБ подверглась критической оценке. На этом шаге осуществляется независимая оценка отдельными лицами (группами лиц) ПолИБ, предшествующая окончательному ее утверждению. В процессе оценки должны рассматриваться не только технические, но и юридические аспекты ОИБ, поскольку политика имеет непосредственное отношение к практической деятельности организации и напрямую затрагивает работу ее персонала.

Обычно назначается специальная комиссия по оценке ПолИБ, которая анализирует и оценивает ее жизнеспособность. Эта комиссия состоит из группы заинтересованных лиц, работающих в организации, которые несут ответственность за то, что ПолИБ хорошо написана и понятна, полностью согласована и выполнима с точки зрения людей, процессов и технологий, которых она затрагивает. Из-за большого объема ПолИБ комиссия не имеет возможности оценить в короткие сроки все описанные процедуры ОИБ, но к этому нужно стремиться. Особо важные процедуры должны быть оценены обязательно.

Достоинства такой оценки не подлежат сомнению: ПолИБ получается более жизнеспособной, поскольку ее проверяют те, кто может иметь несколько отличные или более широкие взгляды, чем взгляды создателей политики; более широкая поддержка ПолИБ за счет увеличения числа заинтересованных лиц; доверие к ПолИБ возрастает из-за привлечения к ее оценке специалистов различных профилей.

На этом шаге разработки ПолИБ осуществляются следующие действия:

- ПолИБ формально или неформально представляется оценщикам;
- решаются все вопросы, которые могут возникнуть во время оценки;
- обосновывается, почему ПолИБ необходима организации, и объясняются цели, содержание и потенциальная польза от ПолИБ.

Разработчики политики дают свои комментарии оценщикам, вырабатывают рекомендации по ее изменению, учитывают важные замечания и вносят изменения в окончательную редакцию, которая после этого готова к утверждению.

Также проводится оценка ПолИБ со стороны самого руководства организации. Входными данными для этого являются следующие сведения [13, 22]:

1) обратная реакция заинтересованных сторон;
2) результаты независимых анализов;
3) статус предупреждающих и корректирующих действий;
4) результаты предыдущего анализа со стороны руководства;
5) выполнение процессов и соблюдение ПолИБ;
6) изменения, которые могут повлиять на подход организации к управлению ИБ, включая изменения в окружении организации, направленности ее бизнеса, доступности ресурсов, договорных, нормативных и юридических условиях или в технической среде;
7) тенденции, связанные с угрозами ИБ и уязвимостями;
8) инциденты ИБ;
9) рекомендации, предоставленные соответствующими органами.

Отчет с результатами анализа ПолИБ со стороны руководства включает любые решения и действия, касающиеся улучшения подхода организации к управлению ИБ и ее процессами, целей и средств управления и распределения ресурсов и/или обязанностей.

Утверждение ПолИБ. Процесс утверждения ПолИБ представляет собой простое одобрение руководством окончательной редакции документа. На бумажном документе с ПолИБ ставится подпись соответствующего уполномоченного должностного лица организации, после чего ПолИБ готова к непосредственному использованию.

Утверждение требует от разработчиков ПолИБ следующих действий:

- дать обоснованные разъяснения официальному лицу, имеющему полномочия утвердить ПолИБ;
- координировать все действия по утверждению ПолИБ с этим официальным лицом;
- представить рекомендации, появившиеся после ревизии ПолИБ;
- предпринимать должные усилия по расширению поддержки ПолИБ со стороны руководства организации.

Если уполномоченное лицо колеблется демонстрировать полное одобрение ПолИБ и сразу подписывать ее, разработчики политики должны решить вопросы временного утверждения ПолИБ.

3.5.2. Внедрение политики ИБ

После официального утверждения ПолИБ начинает претворяться в жизнь. Опыт показывает, что с наибольшими трудностями организациям приходится сталкиваться именно на этом этапе, который, как правило, связан с необходимостью решения технических, организационных

и иных проблем. Часть пользователей может сознательно либо бессознательно сопротивляться введению новых правил поведения, которым теперь необходимо следовать, а также программно-технических механизмов защиты информации, в той или иной степени неизбежно ограничивающих свободный доступ к информации. Администраторов интранета может раздражать необходимость выполнения требований ПолИБ, усложняющих задачи администрирования. Помимо этого, могут возникать и чисто технические проблемы, связанные, например, с отсутствием в используемом ПО функциональности, необходимой для реализации отдельных положений ПолИБ.

Чтобы внедрение завершилось успешно, должна быть создана группа по внедрению ПолИБ, действующая по согласованному плану в соответствии с установленными сроками выполнения работ.

В стадию внедрения ПолИБ входят три основных шага: коммуникации по ее распространению, собственно соблюдение ПолИБ теми, на кого она распространяется, и обработка исключительных ситуаций.

Коммуникации. Основной целью данного шага является распространение ПолИБ внутри организации и среди тех, на кого она распространяется – партнеров, клиентов и т. д. При этом обязательно осуществляются следующие мероприятия:

- определяются степень и метод начального распространения политики;
- решаются вопросы ее доставки в другие географические регионы, а также языковые проблемы;
- предотвращается несанкционированное распространение;
- устанавливается система надзора за распространением.

Для повышения эффективности перечисленных мероприятий разрабатывается и реализуется план, в котором рассматриваются все эти вопросы, а также выделяются ресурсы для данного шага, определяются их зависимости, документируется ознакомление сотрудников с ПолИБ и вырабатываются способы повышения ее наглядности.

Распространением ПолИБ обычно занимается отдел коммуникаций организации.

Соблюдение ПолИБ. Этот шаг заключается в непосредственном выполнении ПолИБ и всех ее требований на практике, для чего осуществляются следующие мероприятия:

- проводится работа с сотрудниками организации, разъясняющая, как им наилучшим образом исполнять ПолИБ в различных ситуациях и организационных моментах;
- обеспечивается понимание политики теми, от кого требуется ее реализация, контроль и поддержка соблюдения;
- осуществляется мониторинг, отслеживание и составление отчетности по темпам, масштабам и эффективности деятельности по осуществлению ПолИБ;

- измеряется непосредственное влияние политики на деятельность организации;
- проводится информирование руководства о ходе осуществления ПолИБ.

Систематизируя лучшие практики по эффективному внедрению ПолИБ, можно сделать вывод, что соблюдение ПолИБ в значительной степени является элементом корпоративной этики. Поэтому на уровень ИБ организации серьезное влияние оказывают отношения как в коллективе, так и между коллективом и собственником или руководством, представляющим интересы собственника. Следовательно, этими отношениями необходимо грамотно и своевременно управлять. Понимая, что наиболее критичным элементом ОИБ организации является ее персонал, собственник должен всемерно поощрять заинтересованность и осведомленность персонала в решении проблем ИБ и строгом соблюдении ПолИБ [11].

Исключения из ПолИБ. Основная деятельность на этом шаге – разрешение ситуаций, когда исполнение ПолИБ невозможно либо частично, либо полностью. Из-за нехватки времени и персонала и других эксплуатационных требований не все политики могут быть выполнены так, как это первоначально предполагалось. Таким образом, исключения из политики, в полной мере не отвечающие ее требованиям, рассматриваются и согласуются с соответствующими лицами, возможно даже с руководством организации. Определяется процедура фиксации запросов в соответствующие службы на признание, отслеживание, оценку и одобрение/неодобрение исключений. После этого такие исключения документируются и контролируются на протяжении утвержденного срока признания исключения. Все наиболее часто повторяющиеся исключения из политики, а также временные отказы от выполнения требований из-за краткосрочных обстоятельств фиксируются. Данной деятельностью может заниматься упомянутая выше комиссия, проводящая оценку ПолИБ.

3.5.3. Применение политики ИБ

За внедрением ПолИБ логически последовательно следует этап ее применения. В него входят информирование, мониторинг, правоприменение и сопровождение.

Информирование о ПолИБ. Этот шаг включает в себя постоянную деятельность по ознакомлению сотрудников организации и всех заинтересованных лиц и лиц, на которых она распространяется, с содержанием ПолИБ с целью выполнения ими ее требований. Для этого осуществляются следующие действия:

- определяются потребности в информировании различных целевых групп в рамках организации (исполнителей, руководителей, пользователей и т. д.);

- устанавливаются наиболее эффективные методы информирования для каждой из групп (например, брифинги, обучение, рассылка сообщений и т. п.);
- разрабатываются и распространяются различные информационные материалы (видеоролики, презентации, плакаты, почтовые рассылки и т. д.) о необходимости соблюдения ПолИБ;
- измеряется уровень информированности сотрудников о ПолИБ (например, посредством тестирования) и по полученным результатам данная деятельность корректируется.

Информирование также включает в себя освещение вопросов соответствия ПолИБ текущему бизнесу организации и правоприменения политики (с разъяснением наказаний за ее нарушение), а также рассмотрение текущих угроз ИБ, что свидетельствует об актуальности и реальности проблем ОИБ в организации.

В различных стандартах и рекомендациях в области ИБ особо отмечается, что необходимо не просто довести содержание ПолИБ до сведения всех целевых групп, но также провести обучение и дать необходимые разъяснения сомневающимся, которые пытаются обойти новые правила и продолжать работать по-старому.

За осуществление информирования назначаются ответственные (в пределах всей организации, если рассматривать, например, корпоративную ПолИБ, или в пределах подразделений, если рассматривать частные ПолИБ, касающиеся только этих подразделений). Обычно они работают совместно с департаментом персонала или департаментом, отвечающим за обучение персонала, что обеспечивает общность их совместных действий и оптимизирует использование задействованных в процессе информирования ресурсов. Такими ответственными чаще всего становятся сотрудники департамента ИБ.

Мониторинг ПолИБ. Соблюдение положений и требований ПолИБ является обязательным для всех сотрудников организации и должно непрерывно контролироваться. Информация для отслеживания и написания отчетов по эффективности соблюдения ПолИБ собирается из разных источников – наблюдений сотрудников и руководителей, отчетов с результатами различных плановых проверок (внешнего и внутреннего аудитов ИБ, различных оценок, анализов и т. п.) и постоянного мониторинга в ИС (в первую очередь на основе журналов регистрации событий, влияющих ни ИБ этих систем), а также отчетов и действий при реагировании на инциденты ИБ.

В данном контексте мониторинг заключается в постоянной деятельности по контролю за соблюдением или несоблюдением ПолИБ с использованием формальных и неформальных методов и подготовке отчетов для соответствующих лиц с целью принятия определенных мер.

Проведение систематически повторяемого (по заранее составленному графику) планового внешнего или внутреннего аудита ИБ является

одним из основных методов контроля жизнеспособности ПолИБ, позволяющего оценить эффективность ее использования. Результаты аудита ИБ могут служить основанием для пересмотра некоторых положений ПолИБ и внесения в нее необходимых корректировок.

Ответственность за осуществление деятельности в рамках шага «мониторинг» обычно распределяется между всеми сотрудниками и руководителями организации, внутренними аудиторами, сотрудниками, отвечающими за ИБ, и т. д.

Каждый сотрудник, на которого распространяются определенные требования по ОИБ в соответствии с ПолИБ, должен помогать в проведении мониторинга ПолИБ, сообщая обо всех замеченных им отклонениях как в самой политике, так и защитных мерах, реализующих ее.

Правоприменение ПолИБ. Правоприменение включает в себя ответную реакцию со стороны руководства на действия или бездействие, результатом которых стали нарушения ПолИБ. Это означает, что как только нарушение выявлено, определяются соответствующие корректирующие действия, которые применяются к нарушителям (в виде дисциплинарных мер), а также к процессам (их переработка) и технологиям (их обновление), пострадавшим от нарушений, что в дальнейшем предотвращает или затрудняет повторение подобных нарушений в будущем. Как уже отмечалось выше, включение информации о таких корректирующих действиях в информирование целевых групп является достаточно эффективным средством.

Основная ответственность за осуществление данной деятельности возлагается на руководителей сотрудников, на которых распространяется ПолИБ.

Сопровождение ПолИБ. Данный шаг означает обеспечение широкого применения и поддержания целостности ПолИБ. Он включает следующие действия:

- отслеживаются основные побудительные мотивы и события для внесения изменений в нее (например, изменения в технологиях, процессах, людях, самой организации, направленности бизнеса и т. д.), которые могут влиять на политику;
- вырабатываются рекомендации и согласуются коррективы, которые требуется внести в ПолИБ в соответствии с вышеперечисленными изменениями;
- осуществляется документирование изменений в ПолИБ и регистрируется деятельность по ее корректировке.

Все это обеспечивает как постоянную доступность ПолИБ для всех сторон, на которых она распространяется, так и поддержание целостности политики посредством эффективного контроля ее редакций. Если в ПолИБ требуется внести изменения, то должны быть обязательно повторно выполнены шаги по пересмотру, утверждению, информированию, коммуникациям и соблюдению.

Ответственность за выполнение данного шага применительно к различным политикам осуществляют все, на кого они распространяются – от руководства организации до ответственных за ИБ в подразделениях и рядовых сотрудников.

3.5.4. Аннулирование политики ИБ

Аннулирование является заключительной стадией жизненного цикла ПолИБ, а изъятие из обращения – последним его шагом. Чтобы избежать путаницы, отслужившая свой срок «лишняя» политика удаляется из перечня действующих, архивируется для дальнейших ссылок на нее, а решение об отмене ПолИБ (включая обоснование, дату и т. д.) документируется.

Изъятие из обращения устаревшей редакции ПолИБ, которая уже послужила своей полезной цели, производится по различным причинам.

Первая из причин – ПолИБ не в полной мере отвечает всем потребностям организации, не всегда охватываются все области, которые должны быть регламентированы сформулированными в политике требованиями, однако понимание этого приходит с опытом. На стадии разработки организации часто пытаются написать ПолИБ без проведения ее независимой оценки – в результате политики не очень хорошо продуманы и должным образом одобрены. Недальновидные руководители часто не уделяют должного внимания рассмотрению исключений (стадия внедрения ПолИБ), ошибочно думая, что не может быть таких обстоятельств, при которых соблюдение политики невозможно. Многие организации не в состоянии постоянно оценивать потребность в установленной ПолИБ на стадии ее применения, принижают важность обеспечения целостности и доступности политики. Скорее всего после наблюдения за процессом применения ПолИБ и оценки эффективности ее использования потребуется осуществить ряд существенных доработок. Тогда появится потребность во второй редакции той же ПолИБ.

Вторая причина – организация больше не использует технологию, для которой разрабатывалась ПолИБ, или используемые технологии и организация бизнес-процессов существенно изменились, что приводит к необходимости корректировать существующие подходы к ОИБ и отказаться от данной ПолИБ как таковой.

Ответственностью за аннулирование ПолИБ наделяется соответствующее официальное лицо в организации.

3.6. Ответственность за исполнение политики ИБ

Согласно основным стандартам в области ИБ [13, 14, 21, 22] для полноценной реализации всех стадий и шагов жизненного цикла ПолИБ и адекватного назначения ответственности за их осуществление в организации создается соответствующая инфраструктура, обеспечивающая

правильное понимание и постоянное исполнение политики, устанавливающая иерархические связи взаимоподдерживающих друг друга уровней и эффективно подстраивающаяся под частые изменения технологического и организационного характера. Обязательно определяются специалисты, непосредственно осуществляющие деятельность по управлению ИБ и таким образом внедряющие основные положения ПолИБ, например, обучающие сотрудников, разрабатывающие критерии для оценки эффективности, планирующие мероприятия по управлению ИБ и т. д. Обычно создается рабочая группа по управлению ИБ, в которую, как правило, входят руководители различных подразделений организации. В обязанности группы входит утверждение документов по ОИБ, разработка и утверждение стратегии управления рисками ИБ, контроль выполнение процедур СУИБ, оценка эффективности функционирования СУИБ и др.

Также определяются назначаемые сотрудникам связанные со всеми стадиями жизненного цикла ПолИБ роли. Под ролью обычно понимается заранее определенная совокупность правил, устанавливающая допустимое взаимодействие между субъектом и объектом [11]. К субъектам могут относиться сотрудники, клиенты, партнеры и иные лица и инициируемые от их имени процессы по выполнению действий над объектами. Объектами, в свою очередь, могут быть программные и аппаратные средства, информационные ресурсы, сервисы, процесс, системы, над которыми выполняются действия. При этом необходимо учитывать следующее:

- бизнес-цели организации и цели ОИБ, а также необходимые и достаточные ресурсы для реализации этих целей;
- функциональные и процедурные требования;
- разделение бизнес-процесса на подпроцессы для присвоения ролей, руководствуясь принципом «один процесс – несколько ролей»;
- возможность группировки и взаимодействия ролей;
- наличие контроля своевременности и качества выполнения ролей, для чего определяются дополнительные роли по ОИБ и критерии оценки эффективности выполнения правил для каждой роли, иначе может возникнуть новая уязвимость;
- установление ответственности за выполнение каждой роли.

Практика использования ПолИБ в различных организациях показывает, что наиболее часто используемыми типовыми ролями участников процессов ОИБ, выделяемыми в ПолИБ, являются следующие:

Создатель ресурса – сотрудник, непосредственно создавший ресурс.

Владелец ресурса – сотрудник, несущий конечную ответственность за ИБ ресурса и определяющий правила использования ресурса. Он организует ОИБ своего ресурса в виде формализованных правил, технических политик, настроек конфигурации, организационных мероприятий и регламентов.

Пользователь ресурса – сотрудник, привлеченный работник, использующий ресурс для своих производственных задач и несущий ответственность в соответствии с корпоративными стандартами в рамках правил, определенных владельцем.

Администратор ресурса – сотрудник, ответственный за применение правил использования ресурса, определенного владельцем. Администратор обязан осуществить и поддерживать настройку среды работы ресурса для применения технических средств, обеспечивающих поддержку правил использования ресурса. Он должен сообщать контролеру и/или владельцу о нарушениях, недостатках и ошибках, выявленных при работе с ресурсом.

Контролер ресурса – сотрудник, ответственный за соответствие ресурса правилам, которые установлены владельцем. Контролер обязан имеющимися средствами мониторинга и аудита обеспечить уверенность в соблюдении пользователями и администраторами правил использования ресурса либо выявлять факты нарушения таких правил. Он обязан принять меры для прекращения и предотвращения нарушений.

Подобное распределение ролей хорошо тем, что позволяет правильно планировать процессы и обязанности отдельных субъектов. Если при разработке ПолИБ обнаруживается, что роли пересекаются, это дает повод усомниться в правильности планирования данного процесса либо распределения обязанностей его субъектов.

Ответственность за исполнение ПолИБ имеет непосредственное отношение к управлению ИБ в организации. Все вопросы, которые так или иначе относятся к человеческому фактору, эффективнее всего решаются при участии департамента персонала в центральном офисе или соответствующем подразделении в филиале организации. Ответственность, связанная с непосредственным выполнением процедур ОИБ, существенно зависит от технического аспекта и, следовательно, определяется совместно с представителями департаментов, сопровождающих работу программных и аппаратных средств. Эти процедуры часто выполняются децентрализовано (в разное время, «на местах» – в географически удаленных друг от друга офисах одной организации), но они должны обязательно быть согласованы с общей корпоративной ПолИБ и должны быть проверены для установления возможности их выполнения при оценке политики.

Конкретное распределение обязанностей указано выше в конце каждого шага жизненного цикла ПолИБ. Из этого видно, что ответственность на различных стадиях жизненного цикла ПолИБ во многом похожа (особенно это касается написания, информирования, сопровождения и аннулирования), но имеется и ряд различий. Они прежде всего связаны с тем, в рамках какой ПолИБ – корпоративной или частной – описывается ответственность.

Рассмотрение ответственности, связанной с ПолИБ, возможно и с других точек зрения. Ответственность по ОИБ активов организации может быть долгосрочной, возлагаемой на весь период жизненного цикла политики, или краткосрочной, предполагающей выполнение обязанностей в повседневной деятельности. Ответственность может возлагаться на всех сотрудников организаций, что относится к корпоративной ПолИБ или частной ПолИБ для одной технологии или одной системы, эксплуатируемой во всех подразделениях организации, или на часть сотрудников, работающих в одном или нескольких подразделениях с только там используемой системой или технологией. Контроль выполнения обязанностей в отношении ПолИБ может осуществляться централизованно или децентрализовано (чаще в отношении соблюдения частных ПолИБ) силами самой организации и ее подразделений. При вовлечении в соблюдение ПолИБ сторонних лиц, не работающих в данной организации на постоянной основе, возлагаемая на них ответственность может контролироваться из самой организации лишь в ограниченном объеме.

Выделяют несколько основных принципов, которыми руководствуются, устанавливая ответственность и распределяя роли и обязанности, связанные с ПолИБ [80].

Принцип разделения полномочий (обязанностей). Он предполагает такое распределение ролей и ответственности, при котором один человек не может нарушить критически важный для организации процесс. Данный принцип должен применяться при определении ответственности за конкретную функцию ОИБ в соответствии с требованиями ПолИБ, что обеспечивает выполнение необходимых проверок и баланса между обязанностями. При этом нельзя допускать конфликта интересов. Так, например, не следует совмещать обязанности по разработке, сопровождению, исполнению, администрированию или контролю систем, обязанности исполнителя и администратора, администратора и аудитора, разработчика и аудитора [11].

Руководствуясь соображениями эффективности, *ответственность за определенные функции в отношении ПолИБ может потребоваться возложить не только на главного ответственного за ПолИБ, но и на других сотрудников организации.* Например, распространение политики и коммуникации по вопросам ПолИБ лучше всего могут осуществить подразделения, обычно исполняющие подобные функции (например, департамент коммуникаций и т. п.). С другой стороны, деятельность по информированию эффективнее всего реализуется подразделением, занимающимся вопросами обучения сотрудников организации (например, учебным департаментом). Учебный департамент может оказать неоценимую поддержку при начальном распространении политики и в оценке эффективности деятельности по информированию сотрудников. Такая деятельность должна осуществляться на постоянной основе, поскольку

она хорошо контролирует соблюдение ПолИБ и правоприменение ее положений, и должна определять требования по обновлению программ информирования, каждая из которых является важным элементом эффективного повышения осведомленности сотрудников организации в вопросах, относящихся к политике.

Границы и время средств управления в отношении ПолИБ влияют на установление ответственности за выполнение конкретных требований политики. Как правило, ответственный за ПолИБ играет лишь ограниченную роль в мониторинге ее соблюдения, поскольку он должен одновременно участвовать во всех процессах реализации политики. Руководители среднего звена из-за их близости к обычным сотрудникам, подпадающим под действие ПолИБ, могут наиболее эффективно контролировать и обеспечивать соблюдение политики и поэтому должны нести ответственность за эти функции. Именно они могут гарантировать, что ПолИБ в настоящее время соблюдается, а все ее нарушения своевременно и эффективно рассматриваются.

Ограничения на полномочия соответствующего органа или лица также могут повлиять на успешное исполнение требований ПолИБ. Эффективность политики часто оценивается ее наглядностью и важностью, придаваемой ей руководством организации. Во многих случаях эффективность ПолИБ зависит от уполномоченных органов и лиц, на которых возлагается ответственность за ее внедрение и контроль за соблюдением. Чтобы политика имела широкую поддержку, утверждающее ее должностное лицо должно иметь в пределах организации признанные всеми полномочия. Как правило, функции по ОИБ в соответствии ПолИБ распределяются между различными подразделениями и требуют поддержки при их исполнении со стороны руководства верхнего уровня. Следовательно, ответственность за внедрение и соблюдение ПолИБ лучше всего возлагать на исполнительную дирекцию организации.

Привлечение комиссии по оценке ПолИБ может обеспечить более широкое понимание деятельности, на которую распространяется политика. Ее компетентная оценка поможет правильно написать ПолИБ, что будет способствовать ее принятию и успешной реализации. Эта оценка может быть также использована для прогнозирования потенциальных проблем с реализацией ПолИБ и эффективной оценке ситуаций, когда оправданы исключения из политики.

Должна быть *ответственность за осуществление ПолИБ на всех стадиях ее жизненного цикла и отдельных его шагов*. На какую часть организации распространяется ПолИБ? Или она применима только к одному подразделению, пользователям отдельной технологии или ко всей организации в целом? От ответа на эти вопросы зависит *ответственность соответствующих лиц на уровне всей организации или ее отдельных технологий и систем*.

Приведем еще ряд дополнительных комментариев. Рекомендуется, чтобы все сотрудники организации давали письменное обязательство о соблюдении конфиденциальности, приверженности правилам корпоративной этики, включая требования по недопущению конфликта интересов [11]. При этом условие о соблюдении конфиденциальности должно распространяться на всю защищаемую от разглашения информацию, доверенную сотруднику или ставшую ему известной в процессе выполнения им своих служебных обязанностей. Обязанности сотрудников по выполнению требований ИБ в соответствии с ПолИБ должны включаться в трудовые контракты (соглашения, договоры). При приеме на работу новые сотрудники также должны подписывать соглашения об обязательности выполнении требований ПолИБ. При изменении служебных обязанностей сотрудников документы должны быть пересмотрены и подписаны заново. Для внешних организаций требования по соблюдению ПолИБ должны регламентироваться положениями, включаемыми в договоры (соглашения).

ПолИБ не должна налагать обязанности, которые не выполнимы на практике. Это будет провоцировать сотрудников на нарушение политики. Например, до сих пор встречаются требования ежедневного полного сканирования жесткого диска рабочей станции на наличие вирусов. Или требование официально оформлять каждый, даже самый мелкий инцидент ИБ. Понятно, что буквальное выполнение таких требований может просто парализовать бизнес-процесс.

Выводы

В данной главе было определено одно из базовых понятий теории управления ИБ – «политика информационной безопасности». Основное внимание было уделено основным видам ПолИБ – корпоративным и частным.

Для ПолИБ организации перечислены причины необходимости ее создания, среди которых главной является то, что она является базовым документом (или комплектом документов), в соответствии с которым определяется стратегия и тактика организации в отношении деятельности по ОИБ.

Для разработки действительно эффективной ПолИБ выделены основные требования и принципы, при соблюдении которых создается действительно «качественная» – жизнеспособная и реально осуществимая на практике политика.

Далее подробно представлено содержание разделов корпоративной ПолИБ и двух видов частных политик – для отдельных областей рассмотрения и для отдельных систем, используемых в организации.

Детально проанализированы четыре основные стадии жизненного цикла ПолИБ (разработка, внедрение, применение и аннулирование) и

соответствующие им более мелкие шаги: создание, ревизия, утверждение; коммуникации, соблюдение, исключения; информирование, мониторинг, правоприменение, сопровождение; изъятие из обращения.

В заключении рассмотрены роли и ответственность, связанные с исполнение положений и требований ПолИБ.

Вопросы для самоконтроля

1. Какие определения ПолИБ даются в различных международных стандартах?
2. В чем различие политик, стандартов, правил и процедур ОИБ?
3. Что такое трастовые модели?
4. С каких точек зрения и как можно описать виды ПолИБ?
5. Что понимают под ПолИБ в широком и узком смыслах?
6. Для чего разрабатываются организационные (административные) и технические ПолИБ?
7. Перечислите основные требования, предъявляемые в различных источниках к ПолИБ?
8. Каковы основные принципы, позволяющие разработать эффективную ПолИБ?
9. Каково содержание документа, описывающего корпоративную ПолИБ? Что излагается в каждом из разделов этой политики?
10. Назовите типовые цели корпоративной ПолИБ.
11. Каковы отличительные особенности содержания частной ПолИБ для отдельной области, требующей ОИБ, и для отдельной системы, используемой в организации? Что общего между этими политиками? Что излагается в каждом из разделов этих политик?
12. Назовите основные стадии жизненного цикла ПолИБ? Из каких шагов они состоят? Какие из этих шагов выполняются итерационно и почему?
13. Отдельно сформулируйте цель и основные мероприятия, осуществляемые на каждом шаге жизненного цикла ПолИБ.
14. Как происходит процесс информирования в отношении ПолИБ?
15. Для чего и кем осуществляются ревизия, мониторинг и аудит ПолИБ? В чем отличия этих шагов жизненного цикла ПолИБ?
16. Что понимается под исключениями из ПолИБ?
17. Зачем необходим пересмотр ПолИБ?
18. В каких случаях ПолИБ может быть аннулирована?
19. Что такое «роль»? Какие роли связаны с использованием ПолИБ?
20. Какие виды ответственности связаны со всеми стадиями жизненного цикла ПолИБ?
21. Какими принципами необходимо руководствоваться при установлении ответственности в отношении соблюдения ПолИБ?