**4. Политика информационной безопасности**

Процесс создания системы управления информационной безопасностью (СУИБ) в соответствии с рекомендациями большинства стандартов предполагает разработку следующих документов:

**‑ политика ИБ** (ПИБ) верхнего уровня, политика СУИБ;

**- частные (детальные) политики** в отдельных областях деятельности, охватываемых СУИБ;

**- процедуры** СУИБ.

Разрабатываемые политики и процедуры должны охватывать следующие ключевые процессы СУИБ:

**-**управление рисками;

**-**управление инцидентами;

**-**управление эффективностью системы;

**-**управление персоналом;

**-**управление документацией и записями системы управления ИБ;

**-**пересмотр и модернизация системы;

**-**управление непрерывностью бизнеса и восстановления после прерываний.

**Создание ПИБ позволяет:**

- снизить риски и повысить эффективность бизнеса;

- выполнить требования законодательства;

- выполнить требования клиентов и партнеров;

- осуществить подготовку к сертификации;

- повысить имидж компании.

В соответствии со стандартом ISO/IEC 27001 требуется, чтобы организации имели политику СУИБ и политику ИБ. Однако эти политики могут разрабатываться, как равноправные политики или являться расширенной версией другой (рисунок 2.2).

|  |
| --- |
| 1  Рисунок 2.2. – Иерархия политик организации |

Политика информационной безопасности (ПИБ) ‑ совокупность принципов, правил, процедур и практических приёмов в области безопасности, которые направлены на защиту информации.

Назначение ПИБ:

- формулирование целей и задач информационной безопасности организации с точки зрения бизнеса (позволяет определить это для руководства и продемонстрировать поддержку руководством значимости ИБ),

- определение правил организации работы в компании для минимизации рисков информационной безопасности и повышения эффективности бизнеса.

**Требования к ПИБ:**

- должна быть утверждена высшим административным органом компании (генеральный директор, совет директоров и т.п.) для демонстрации поддержки руководства;

- должна быть написана понятным языком для конечных пользователей и руководства компании и быть по возможности краткой;

- должна определять цели ИБ, способы их достижения и ответственность. Технические подробности реализации способов содержатся в инструкциях и регламентах, на которые даются ссылки в ПИБ;

- минимизация влияния ПИБ на производственный процесс

- непрерывность обучения сотрудников и руководства организации в вопросах обеспечения ИБ;

- непрерывный контроль выполнения правил ПИБ на этапе внедрения и в дальнейшем;

- постоянное совершенствование;

- согласованность во взглядах и создание корпоративной культуры безопасности.

**Предлагается следующая структура ПИБ:**

**Общие положения** (ссылки на законы, нормативные акты и др.руководящие документы, которым подчиняется деятельность организации),

Подтверждение значимости ИБ для организации и формулирование **целей защиты информации** с точки зрения бизнеса организации (выполнение требований законодательства и др. норм, удовлетворение ожиданий клиентов и партнеров, повышение конкурентоспособности, финансовой стабильности, имиджа организации).

Описание **стратегии** организации по обеспечению информационной безопасности (например, выполнение требований законодательства, оценка и управление рисками).

**Область применения** ПИБ (например, ПИБ обязательна для выполнения всеми сотрудниками и руководством организации, или отдельного филиала, или сотрудниками, использующими ноутбуки).

**Описание объекта защиты** (защищаемые ресурсы – информация различных категорий, информационная инфраструктура и т.д.).

**Цели и задачи** обеспечения информационной безопасности (например, снижение угроз ИБ до приемлемого уровня, выявление потенциальных угроз и уязвимостей ИБ, предотвращение инцидентов ИБ).

**Угрозы и модель нарушителя**, которые принимаются во внимание для данной организации (по источникам возникновения, по способам реализации, по направленности).

Краткое разъяснение **принципов политики** ИБ:

- подход к построению СУИБ;

- требования к подготовке и осведомленности персонала в области ИБ;

- последствия и ответственность за нарушение ПИБ;

- подход к управлению рисками;

- определение оргструктуры, общих и специальных обязанностей по управлению ИБ, включая отчеты об инцидентах;

- ссылки на документацию, которая может поддержать политику, например, частные политики и процедуры в области защиты для конкретных информационных систем или правила защиты, которым должны следовать пользователи;

- механизмы контроля за выполнением положений ПИБ;

- порядок пересмотра и принятия изменений в политике.

**После утверждения политики ИБ необходимо:**

1. Довести положения политики ИБ, процедур и инструкций под роспись до сведения рядовых сотрудников при их первоначальном и последующем периодическом обучении и информировании.

2. Разработать процедуры, инструкции и т.д., уточняющие и дополняющие политику (для специалистов отдела ИБ).

3. Периодически анализировать политику для поддержки ее адекватности и результативности.

4. Проводить периодический аудит на выполнение сотрудниками положений политики с предоставлением отчета Руководству организации.

Кроме того, в должностные инструкции ответственного персонала, положения о подразделениях, контрактные обязательства организации должны быть включены обязанности по обеспечению информационной безопасности.

Таким образом, в результате не только создается документальная база СУИБ, но и происходит реальное распределение обязанностей по обеспечению безопасности информации среди персонала организации.

**Жизненный цикл политики безопасности.**

**1. Планирование.**

Первоначальный аудит безопасности:

- проведение обследования;

- идентификация угроз безопасности;

- идентификация ресурсов, нуждающихся в защите;

- оценка рисков.

В ходе аудита производится анализ текущего состояния информационной безопасности, выявляются существующие уязвимости, наиболее критичные области функционирования и самые чувствительные к угрозам безопасности бизнес-процессы.

Разработка политики безопасности:

- определяются основные условия, требования и базовая система мер по обеспечению информационной безопасности в организации, позволяющие уменьшить риски до приемлемой величины;

- оформляются в виде согласованных в рамках рабочей группы решений и утверждаются руководством организации.

**2. Внедрение ПИБ.**

Решение технических, организационных и дисциплинарных проблем.

**3. Проверка.**

Аудит и контроль.

**4. Корректировка.**

Периодические пересмотр и корректировка, а также при изменении исходных данных.