**2. Нормативно-правовое обеспечение защиты информации в организации**

Стандарт BS ISO/IEC 27001:2005 описывает модель системы управления информационной безопасностью (СМИБ) и предлагает набор требований к организации информационной безопасности (ИБ) на предприятии без привязки к способам реализации, которые выбираются исполнителями организации.

В стандарте предложено применение модели PDCA (Plan-Do-Check-Act) к жизненному циклу СМИБ, который включает разработку, внедрение, эксплуатацию, контроль, анализ, поддержку и совершенствование (рисунок 2.1).

|  |
| --- |
| 1  Рисунок 2.1. – Применение модели PDCA к процессам СМИБ |

Решение о создании (и последующей сертификации) СМИБ принимается высшим руководством организации. Это демонстрирует поддержку и подтверждение руководством ценности СМИБ для бизнеса. Руководство организации инициирует создание группы по планированию СМИБ.

Группа, ответственная за планирование СМИБ, должна включать:

- представителей высшего руководства организации;

- представителей бизнес-подразделений, охватываемых СМИБ;

- специалистов подразделений ИБ;

- сторонних консультантов (при необходимости).

Рассмотрим этапы создания СМИБ.

**1 этап. Планирование СМИБ.**

Установление политики, целей, процессов и процедур, относящихся к управлению рисками и защите информации, в соответствии с общей политикой и целями организации.

**a) Определение области применения и границ СМИБ:**

- описание вида деятельности и бизнес-целей организации;

- указание границ систем, охватываемых СМИБ;

- описание активов организации (виды информационных ресурсов, программно-технические средства, персонал и организационная структура);

- описание бизнес-процессов, использующих защищаемую информацию;

**б) Определение политики в отношении СМИБ организации (расширенная версия ПБ).**

- содержание политики СМИБ:

- цели, направления и принципы деятельности в отношении защиты информации;

- ссылки на законодательные, нормативные и деловые требования, а также договорные обязательства по ЗИ, определение на их основе основных требований и положений политики ИБ организации;

- описание стратегии (подходов) управления рисками в организации, структуризация контрмер по защите информации по видам (правовые, организационные, аппаратно-программные, инженерно-технические);

- описание критериев значимости риска;

- позиция руководства, определение периодичности проведения совещаний по тематике ИБ на уровне руководства, включая периодический пересмотр положений политики ИБ, а также порядка обучения всех категорий пользователей информационной системы по вопросам ИБ.

**в) Определение подхода к оценке рисков в организации.**

Методология оценки риска выбирается в зависимости от СМИБ, установленных деловых требований защиты информации, законодательных и нормативных требований.

Выбор методологии оценки рисков зависит от уровня требований, предъявляемых в организации к режиму информационной безопасности, характера принимаемых во внимание угроз (спектра воздействия угроз) и эффективности потенциальных контрмер по защите информации. В частности различают базовые, а также повышенные или полные требования к режиму ИБ.

Минимальным требованиям к режиму ИБ соответствует базовый уровень ИБ. Такие требования применяются, как правило, к типовым проектным решениям. Существует ряд стандартов и спецификаций, в которых рассматривается минимальный (типовой) набор наиболее вероятных угроз, таких как: вирусы, сбои оборудования, несанкционированный доступ и т. д. Для нейтрализации этих угроз обязательно должны быть приняты контрмеры вне зависимости от вероятности их осуществления и уязвимости ресурсов. Таким образом, характеристики угроз на базовом уровне рассматривать не обязательно. Зарубежные стандарты в этой области ISO 27002, BSI, NIST и др.

В случаях, когда нарушения режима ИБ ведут к тяжелым последствиям, предъявляются дополнительно повышенные требования.

Для формулирования дополнительных повышенных требований, необходимо:

- определить ценность ресурсов;

- к стандартному набору добавить список угроз, актуальных для исследуемой информационной системы;

- оценить вероятности угроз;

- определить уязвимости ресурсов;

- оценить потенциальный ущерб от воздействий злоумышленников.

Необходимо подобрать такую методику оценки рисков, которую можно было бы использовать с минимальными изменениями на постоянной основе. Есть два пути: использовать существующие на рынке методики и инструментарий для оценки рисков или создать свою методику, адаптированную к специфике компании и охватываемой СМИБ области деятельности.

Последний вариант наиболее предпочтителен, поскольку пока большинство существующих на рынке продуктов, реализующих ту или иную методику анализа рисков, не отвечают требованиям Стандарта. Типичными недостатками таких методик являются:

- стандартный набор угроз и уязвимостей, который зачастую невозможно изменить;

- принятие в качестве активов только программно-технических и информационных ресурсов - без рассмотрения человеческих ресурсов, сервисов и других важных ресурсов;

- общая сложность методики с точки зрения ее устойчивого и повторяющегося использования.

Критерии принятия рисков и приемлемые уровни риска (должны базироваться на достижении стратегических, организационных и управленческих целей организации).

**в) Выявление рисков.**

Идентификация активов и их владельцев

Активы:

- информационные входные данные;

- информационные выходные данные;

- информационные записи;

- ресурсы: люди, инфраструктура, оборудование, программное обеспечение, инструменты, услуги.

Идентификация угроз (в стандартах по оценке рисков зачастую предлагаются классы угроз, которые можно дополнять и расширять).

Идентификация уязвимостей (также существуют списки наиболее распространенных уязвимостей, на которые можно опираться при анализе своей организации).

Определение ценности активов (возможные последствия от потери конфиденциальности, целостности и доступности активов). Информация о ценности актива может быть получена от его владельца или же от лица, которому владелец делегировал все полномочия по данному активу, включая обеспечение его безопасности.

**г) Оценка риска.**

- оценка ущерба, который может быть нанесен бизнесу от потери конфиденциальности, целостности и доступности активов.

- оценка вероятности реализации угроз через существующие уязвимости с учетом имеющихся средств управления ИБ и оценки возможного наносимого ущерба;

- определение уровня риска.

- применение критериев принятия риска (приемлемый/требующий обработки).

**д) Обработка рисков (в соответствии с выбранной стратегией управления рисками).**

Возможные действия:

- пассивные действия:

- принятие риска (решение о приемлемости полученного уровня риска);

- уклонение от риска (решение об изменении деятельности, вызывающей данный уровень риска – вынесение веб-сервера за границы локальной сети);

- активные действия:

- уменьшение риска (применением организационных и технических контрмер);

- передача риска (страхование (пожара, кражи, ошибок в ПО)).

Выбор возможных действий зависит от принятых критериев рисков (задается приемлемый уровень риска, уровни риска, которые могут быть понижены средствами управления ИБ, уровни риска, при которых рекомендуется отказаться или преобразовать вид деятельности, которая его вызывает, и риски, которые желательно передать другим сторонам).

**е) Выбор целей и средств управления для обработки риска.**

Цели и средства управления должны реализовывать стратегию управления рисками, учитывать критерии для принятия рисков и законодательные, нормативные и др. требования.

Стандарт ИСО 27001-2005 предлагает список целей и средств управления в качестве основы для построения плана обработки рисков (требований к СМИБ).

План обработки рисков содержит перечень первоочередных мероприятий по снижению уровней рисков с указанием:

- лиц, ответственных за реализацию данных мероприятий и средств;

- сроков реализации мероприятий и приоритетов их выполнения;

- ресурсов для реализации таких мероприятий;

- уровней остаточных рисков после внедрения мероприятий и средств управления.

Принятие плана обработки рисков и контроль за его выполнением осуществляет высшее руководство организации. Выполнение ключевых мероприятий плана является критерием, позволяющим принять решение о вводе СМИБ в эксплуатацию.

На данном этапе производится обоснование выбора различных контрмер по ЗИ, структурированных по нормативно-правовому, организационно-управленческому, технологическому и аппаратно-программному уровням обеспечения информационной безопасности. (Далее комплекс контрмер реализуется в соответствии с выбранной стратегией управления информационными рисками). При полном варианте анализа рисков, для каждого риска дополнительно оценивается эффективность контрмер.

**ж) Утверждение руководством предлагаемого остаточного риска.**

**з) Получение разрешения руководства на реализацию и ввод в эксплуатацию СМИБ.**

**и) Заявление о применимости (в соответствии с ИСО 27001-2005).**

Датой ввода СМИБ в эксплуатацию является дата утверждения высшим руководством компании Положения о применимости средств управления, которое описывает цели и средства, выбранные организацией для управления рисками:

- средства управления и контроля, выбранные на этапе обработки рисков;

- уже существующие в организации средства управления и контроля;

- средства, обеспечивающие выполнение требований законодательства и требований регулирующих организаций;

- средства, обеспечивающие выполнение требований заказчиков;

- средства, обеспечивающие выполнение общекорпоративных требований;

- любые другие соответствующие средства управления и контроля.

**2 этап. Реализация и эксплуатация СМИБ.**

Для внедрения и эксплуатации политики ИБ, средств управления, процессов и процедур в области ИБ выполняются следующие действия:

а) Разработка плана обработки рисков (описание запланированных средств управления, ресурсов (программные, аппаратные, персонал), которые требуются для их реализации, поддержки, контроля, и обязанностей руководства по управлению рисками ИБ (разработка документов на этапе планирования, поддержка целей ИБ, определение ролей и ответственности, обеспечение необходимыми ресурсами для создания СМИБ, аудит и анализ).

б) Распределение финансирования, ролей и ответственности по реализации плана обработки рисков.

в) Внедрение запланированных средств управления.

г) Определение контрольных показателей эффективности (метрик) средств управления, методов их измерения, которые обеспечат сравнимые и воспроизводимые результаты.

д) Повышение квалификации, осведомленности персонала в области ИБ в соответствии с их трудовыми обязанностями.

е) Управление эксплуатацией СМИБ, управление ресурсами для поддержки в рабочем состоянии, контроля и улучшения СМИБ.

з) Внедрение процедур и других средств управления для быстрого обнаружения и реагирования на инциденты ИБ.

**3 этап. Постоянный контроль и анализ функционирования СМИБ.**

Этап предполагает проведение оценки или измерений ключевых показателей эффективности процессов, анализ результатов и предоставление отчетов руководству для анализа и включает:

а) Проведение постоянного контроля и анализа (позволяет быстро обнаруживать ошибки функционирования СМИБ, быстро выявлять и реагировать на инциденты безопасности, разграничить роли персонала и автоматизированных систем в СМИБ, предотвращать инциденты безопасности за счет анализа необычного поведения, определять результативность обработки инцидентов безопасности).

б) Проведение регулярного анализа результативности СМИБ (анализируются соответствие политике и целям СМИБ, аудиты, ключевые показатели эффективности, предложения и реакция заинтересованных сторон).

в) Измерение эффективности средств управления для проверки выполнения требований защиты

г) Периодическая переоценка рисков, анализ остаточных рисков и определение приемлемых уровней риска при каких-либо изменениях в организации (бизнес-целей и процессов, выявленных угроз, новых выявленных уязвимостей и т.д.)

д) Периодическое проведение внутренних аудитов СМИБ.

**Аудит СМИБ** – проверка соответствия выбранных контрмер целям и задачам бизнеса, декларированным в ПБ организации, по его результатам проводится оценка остаточных рисков и, в случае необходимости, их оптимизация.

е) Регулярный анализ области применения и тенденции СМИБ руководством.

ж) Обновление планов управления рисками для учета результатов контроля и анализа.

з) Ведение журналов регистрации событий, оказавших негативное влияние на результативность или качество работы СМИБ.

**4 этап. Поддержка и улучшение СМИБ.**

По результатам внутреннего аудита СМИБ  и анализа со стороны руководства разрабатываются и внедряются корректирующие и предупреждающие действия, направленные на постоянное улучшение СМИБ:

а) Совершенствование политики ИБ, целей защиты информации, проведение аудита, анализ наблюдаемых событий.

б) Разработка и реализация корректирующих и предупреждающих действий для  устранения несоответствий СМИБ требованиям.

в) Контроль улучшений СМИБ.