Министерство науки и высшего образования Российской Федерации
Федеральное государственное автономное образовательное учреждение высшего образования
«Московский государственный технический университет имени Н. Э. Баумана
(национальный исследовательский университет)»
(МГТУ им. Н. Э. Баумана)

ФАКУЛЬТЕТ «Информатика и системы управления» (ИУ)
КАФЕДРА «Информационная безопасность» (ИУ8)

Доклад на тему

"Этап планирования СУИБ: основные действия и процессы"

по дисциплине «Основы управленческой деятельности»

Студент ИУ8-114 (Группа) Н.В. Железцов (И. О. Фамилия) _____ (Подпись, дата)

Преподаватель Е. И. Жук (И. О. Фамилия) _____ (Подпись, дата)

Оценка: _____

Москва, 2025 г.

СПИСОК ОБОЗНАЧЕНИЙ И СОКРАЩЕНИЙ

В настоящем документе применяют следующие сокращения и обозначения:

ИБ	—	информационная безопасность
ОИБ	—	обеспечение информационной безопасности
ПолИБ	—	политика информационной безопасности
СУИБ	—	система управления информационной безопасностью

СОДЕРЖАНИЕ

ВВЕДЕНИЕ

В современном цифровом мире информация является одним из ключевых стратегических активов любой организации. Ее защита от широкого спектра угроз — от кибератак до внутренних инцидентов — перестала быть второстепенной задачей и превратилась в необходимое условие устойчивого развития и конкурентоспособности. Эффективное управление этой защитой невозможно без системного подхода, который реализуется в рамках Системы Управления Информационной Безопасностью (СУИБ). СУИБ представляет собой не разрозненный набор технических средств, а целостную структуру политик, процессов, процедур и организационных мер, построенную на международных стандартах, таких как ISO/IEC 27001.

Особую значимость в жизненном цикле СУИБ приобретает начальный этап — планирование. Именно на этой стадии закладывается фундамент всей будущей системы безопасности, определяются ее цели, границы и основные механизмы функционирования. Этап планирования не сводится лишь к выбору технологических решений; это комплексный процесс, включающий анализ контекста организации, оценку рисков, постановку целей, определение ресурсов и разработку программы. Успех или неудача всей СУИБ во многом предопределены тщательностью и глубиной работ, выполненных на данной стадии.

Целью данного реферата является всестороннее исследование этапа планирования СУИБ. В работе будут последовательно рассмотрены основные действия и процессы, выполняемые на этой ключевой стадии: от определения области применения системы и оценки рисков до формулирования политики безопасности и разработки плана обработки рисков. Анализ этих элементов позволит сформировать целостное представление о том, как грамотное планирование обеспечивает создание адекватной, экономически обоснованной и интегрированной в бизнес-процессы системы защиты информации.

ОСНОВНАЯ ЧАСТЬ

1 Теоретические основы планирования в СУИБ

1.1 Циклическая модель улучшения процессов PDCA

Для структурирования всех процессов управления и для обеспечения учета всех значимых элементов процессного подхода применяется циклическая модель, или цикл, PDCA (от англ. PlanDoCheckAct – планируй, выполняй, проверяй, действуй), предложенная и развитая двумя американскими учеными и специалистами в теории управления качеством (рис. 1).

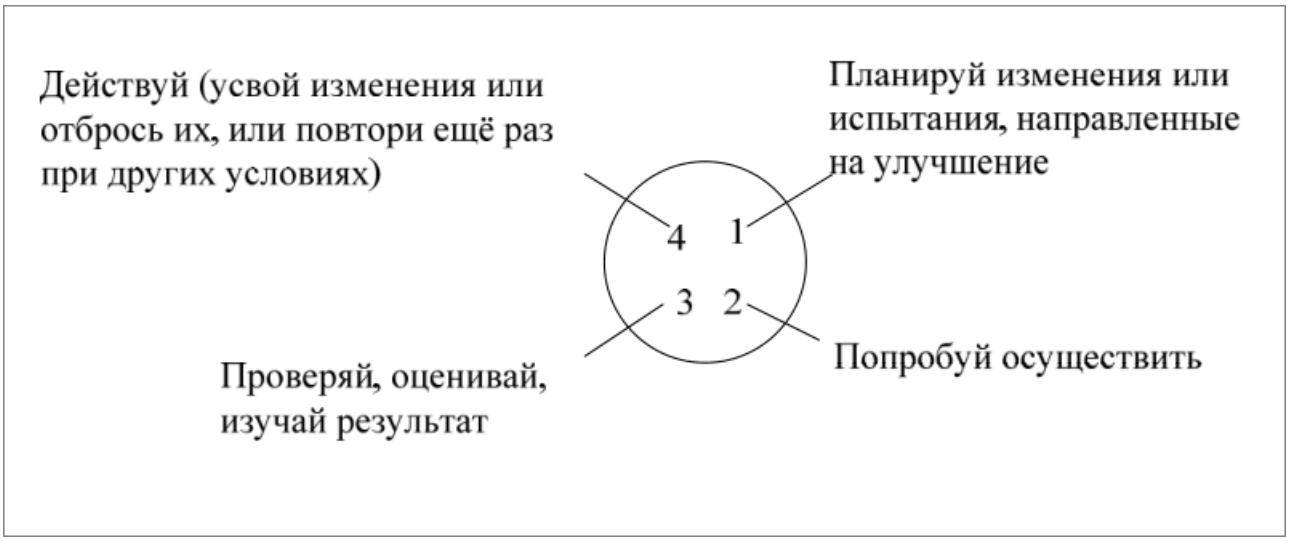

Рисунок 1 – Цикл PDCA

В. Шухарт впервые описал цикл PDCA в 1939 г. в своей книге «Статистические методы с точки зрения управления качеством». В. Деминг пропагандировал использование цикла PDCA в качестве основного способа достижения непрерывного улучшения процессов, и поэтому в современном мире эта формула больше известна как «цикл Деминга». Он также ввел модификацию цикла PDCA – цикл PDSA (от англ. study – изучай):

– Планируй» (Plan) – определение целей и задач, а также способов достижения целей. На данном этапе обеспечивается единое направление деятельности организации к достижению ее целей за счет установления процессов, необходимых для получения результатов в соответствии с существующими требованиями в обозначенный отрезок времени. Для этого определяются и описываются текущее и желаемое

состояния процессов за счет выявленных несоответствий и причин их появления. Планирование не является отдельным разовым событием, если организация стремится функционировать как можно дольше. Поэтому она пересматривает свои цели, если полное достижение первоначальных практически завершено или их выполнение невозможно в силу ряда причин. Вторая причина, по которой планирование должно осуществляться непрерывно, – это постоянная неопределенность будущего. Изменения в окружающей среде, ошибки в суждениях и другие факторы приводят к тому, что события разворачиваются не так, как это предвидело руководство при выработке первоначальных планов. Поэтому, чтобы планы согласовывались с реальностью, их необходимо регулярно пересматривать. В процессе планирования нужно консультироваться с владельцами процессов, которые обладают самими полными знаниями о них.

– «Осуществляй» (Do) – реализация процесса: обучение и подготовка кадров, выполнение работ. На данном этапе в первую очередь происходит создание некоторой структуры, которая должна выполнять намеченные планы и тем самым достигать цели организации. Внедряются процессы, осуществляется выполнение запланированных мероприятий. Здесь следует помнить о том, что стандарты всегда несовершенны, поэтому необходимо полагаться на опыт и знания квалифицированных работников. На всех этапах прохождения цикла Деминга возникает проблема нехватки квалифицированных и подготовленных работников. Поэтому необходимо внедрять программы обучения и целенаправленной подготовки кадров.
– «Проверяй» (Check) – проверка результатов выполнения работ, проведенных на предыдущем этапе. Данный этап говорит о том, что необходимо проводить мониторинг процессов и измерять их по отношению к политикам, целям и требованиям к продукции за определенный период и сообщать о полученных результатах в сравнении с ожидаемыми. Контроль и оценка обеспечивают организации достижение своих целей. Если все идет в соответствии с поставленными задачами и согласно

требованиям стандартов, то, соответственно, никакой корректировки не требуется. Однако если обнаружено отклонение, то вмешательство руководства для установления причин неэффективной работы процессов и планирования мер по улучшению становится необходимым.

– «Действуй, или воздействуй» (Act) – осуществление соответствующих управляющих воздействий по постоянному усовершенствованию (улучшению) показателей процессов. На данном этапе на основе результатов, полученных ранее, предпринимаются действия по коррекции отклонений от первоначальных планов и постоянному улучшению функционирования процессов. Если вносимые изменения не решают поставленную задачу, цикл следует повторить. Тогда одно из возможных действий – пересмотр целей для того, чтобы они стали более реалистичными и соответствовали ситуации.

Применение цикла PDCA в самых различных областях позволяет эффективно управлять деятельностью на системной основе [1]. Данный цикл может быть применен внутри каждого процесса организации, как высокого уровня, так и к простым производственным процессам, а также по отношению к системе процессов в целом. Он тесно связан с планированием, внедрением, управлением и постоянным улучшением как бизнес-процессов организации, так и других процессов системы управления. Управление следует организовывать на основе комплексов мероприятий, которые доказали свою эффективность.

1.2 Процессный подход в рамках управления ИБ

Чтобы функционировать эффективно, организация должна идентифицировать различные виды осуществляемой деятельности и управлять ими. Любое действие, использующее ресурсы и управляемое с целью преобразования входных данных в выходные, может рассматриваться как процесс. Применение системы процессов в организации, идентификация и взаимодействие этих процессов, а также управление этими процессами может быть названо процессным подходом. Все это справедливо и в отношении обеспечения и управления ИБ, так как любые действия в рамках данных видов деятельности могут рассматриваться как процессы.

К управлению ИБ применим процессный подход, который распространяется на разработку, реализацию, эксплуатацию, мониторинг, анализ, сопровождение и совершенствование СУИБ организации. Поддержание на должном уровне СУИБ требует применения такого же подхода, как и любая другая система управления. Используемая в ISO/IEC 27001 и ГОСТ Р ИСО/МЭК 27001 для описания процессов СУИБ циклическая модель Р ИСА предусматривает непрерывный цикл мероприятий: «планирование – реализация – проверка – совершенствование» [2], [3]. При таком подходе к управлению ИБ особое значение придается следующему:

- пониманию требований по ОИБ организации и необходимости определить политику и цели ОИБ;
- внедрению и использованию обоснованных защитных мер для управления рисками ИБ организации в контексте общих бизнес-рисков организации;
- мониторингу и анализу результативности и эффективности СУИБ;
- постоянному совершенствованию, основанному на объективных показателях.

На текущий момент интерес к циклической модели связан, прежде всего, с проблемами внедрения и совершенствования современных систем управления, в частности СУИБ. Одна из основных целей внедрения СУИБ – создание таких условий в организации, когда происходит постоянный мониторинг и улучшение каждого из процессов ОИБ и смежных процессов. Взаимно усиливая друг друга, эти улучшения позволяют создать все более совершенную систему.

Частным критерием улучшения каждого из процессов может служить снижение числа несоответствий, выявляемых в ходе различных проверок, таких как внутренние аудиты ИБ, мониторинг эффективности процессов и т. д. Появление несоответствий можно рассматривать как возникновение некоторой проблемы, решение которой ведет к улучшению процесса (после этого она не возникает снова), а следовательно, и к достижению запланированных результатов, удовлетворению всех заинтересованных сторон и реализации принципа постоянного улучшения.

Каждый факт появления несоответствия должен приводить к выполнению определенной последовательности действий, а именно:

- коррекция (устранение несоответствия);
- анализ несоответствия;
- установление коренной причины его появления;

– определение корректирующих действий, направленных на устранение причины несоответствия;
– выполнение этих действий;
– анализ их результативности и эффективности

Если же в ходе проверок удается выявить факты, которые могут в будущем привести к возникновению несоответствий, то следует осуществить все вышеперечисленные действия, но только теперь их целью должно быть устранение причин потенциальных несоответствий.

Процессный подход к СУИБ показан на рис. 2. СУИБ принимает в качестве входных данных требования по ОИБ и ожидания заинтересованных сторон, и в результате ряда необходимых действий и процессов на выходе получается управляемая ИБ, которая удовлетворяет этим требованиям и ожиданиям.

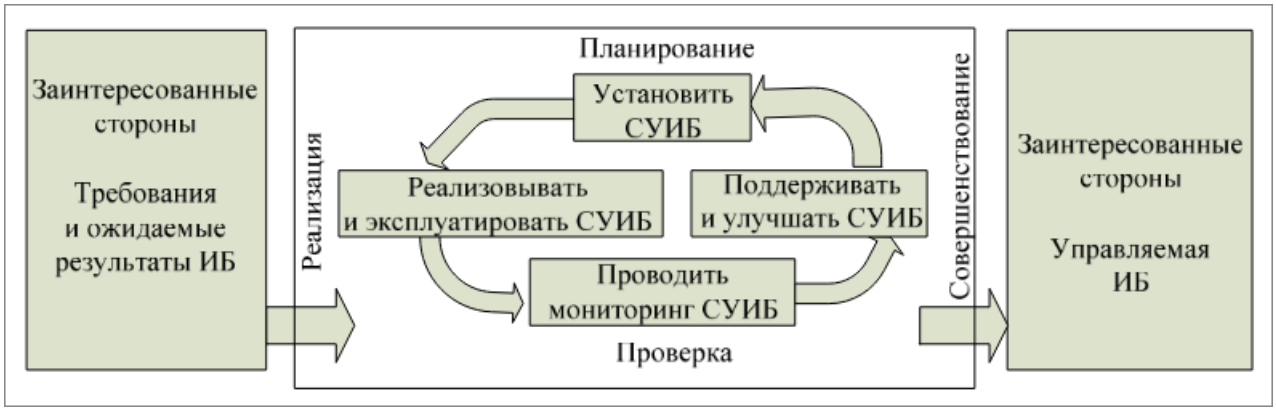

Рисунок 2 – Цикл PDCA в применении к процессам СУИБ

На стадии планирования обеспечивается правильное задание контекста и масштаба СУИБ, оцениваются риски ИБ, предлагается соответствующий план обработки этих рисков.

На стадии реализации внедряются решения, принятые во время планирования.

Чтобы гарантировать, что СУИБ в целом достигает своих целей, необходимы периодические проверки. На стадиях проверки и совершенствования усиливают, исправляют и совершенствуют решения по СУИБ, которые были определены и уже реализованы. В зависимости от конкретной ситуации проверки СУИБ могут проводиться в любое время и с любой периодичностью. В некоторых системах с целью обеспечения

немедленного выполнения и реагирования они должны быть встроены в автоматизированные процессы. Для других процессов реагирование требуется только в случае инцидентов ИБ, когда в защищаемые активы внесены изменения или дополнения или произошли изменения угроз ИБ и уязвимостей.

Процесс непрерывного совершенствования обычно требует первоначального инвестирования в документирование деятельности, формализацию подхода к управлению рисками ИБ, определению методов анализа и выделению ресурсов и т. п. Эти меры используются для приведения цикла в действие. Они не обязательно должны быть завершены, прежде чем будут активизированы стадии пересмотра СУИБ.

Детально содержание деятельности в рамках названных стадий показано на рис 3.

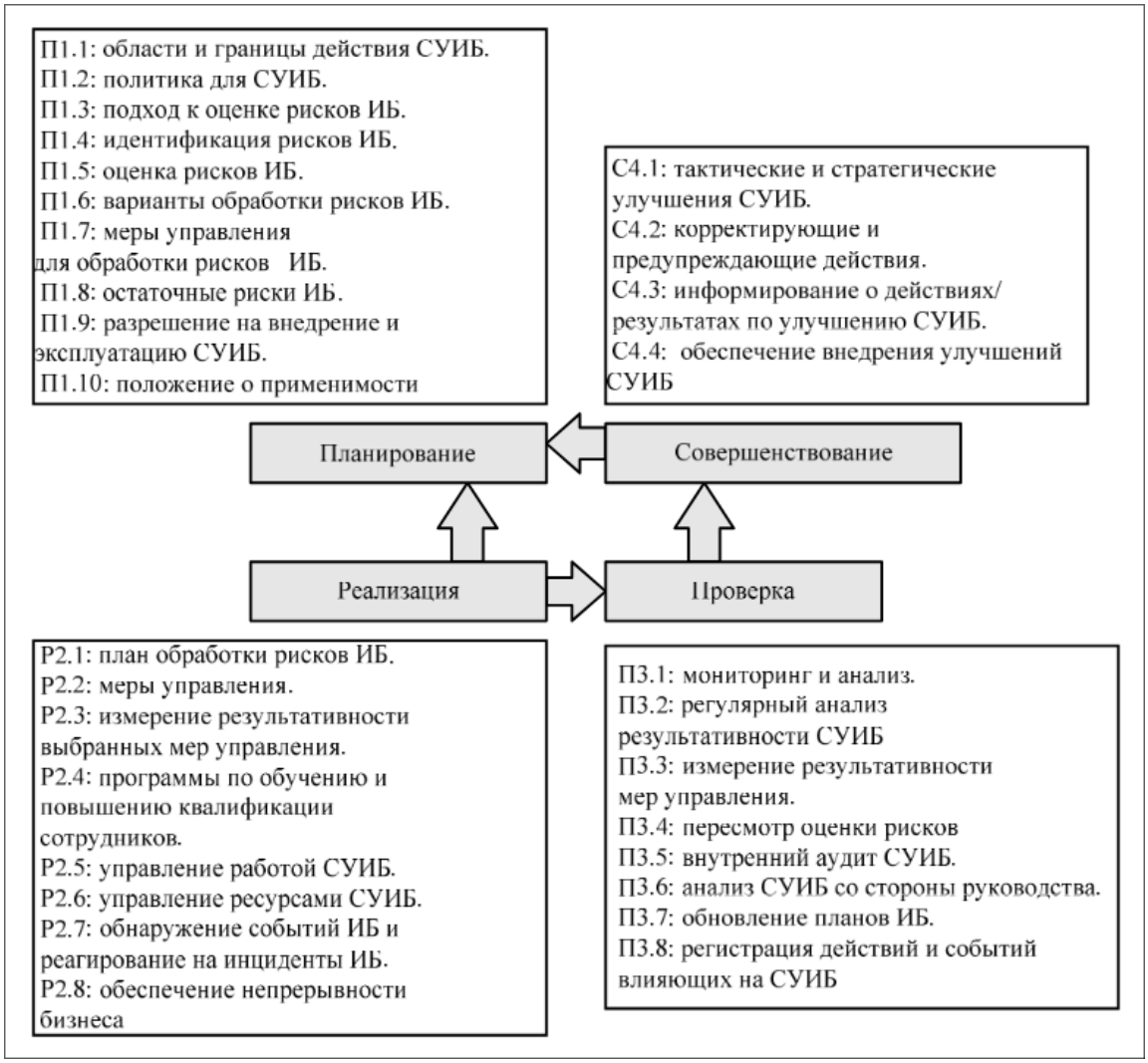

Рисунок 3 – Процессы цикла PDCA в применении к процессам СУИБ

2 Основные процессы и действия на стадии планирования в СУИБ

Применительно к СУИБ на этапе планирования осуществляется ее непосредственная разработка: устанавливается область действия и политика для СУИБ, определяются цели, задачи, процессы и процедуры, адекватные потребностям бизнеса в управлении рисками ИБ и позволяющие повысить уровень ИБ, а также получить результаты, соответствующие общим политикам и целям организации.

Целью выполнения деятельности в рамках группы процессов «планирование» является запуск цикла СУИБ путем определения первоначальных планов ее построения, ввода в действие и контроля, а также определения планов по совершенствованию на основании решений, принятых на этапе «Совершенствование» (если это уже не первый цикл).

Сочетая при создании СУИБ различные принципы управления в каждом отдельном контуре защиты объекта, можно добиться оптимального соотношения эффективности и стоимости ОИБ. Разработка СУИБ, как и любой другой системы управления, основывается на трех базовых принципах управления [4]:

а) **Разомкнутое управление.** Заранее сформированные требования реализуются исполнителями ОИБ, воздействуя на объект защиты. Достоинство – простота; недостаток – низкая эффективность защиты, так как трудно заранее предугадать момент воздействия и вид угрозы ИБ.

б) **Компенсация.** В контур управления ИБ оперативно вводится информация об обнаруженной угрозе ИБ, в результате чего исполнители ОИБ концентрируют свои усилия на ее локализации и противодействии ей. Достоинство – более высокая эффективность; недостатки – трудность правильного обнаружения угрозы ИБ и невозможность устранения последствий внутренних угроз.

в) **Обратная связь.** Обнаруживается не сама угроза ИБ, а реакция системы на нее и степень нанесенного ущерба. Достоинства – конкретность и точность отработки последствий внешних и внутренних угроз ИБ (экономическая целесообразность); недостаток – запаздывание (инерционность) принимаемых защитных мер.

Выполнение деятельности на данной стадии заключается в обследовании организации с целью определения степени соответствия требованиям по ОИБ и к СУИБ, определении/корректировке области действия СУИБ, разработке плана мероприятий по построению СУИБ с учетом выбранной области и степени соответствия требованиям к СУИБ в границах области деятельности, формализации подхода к оценке рисков ИБ и распределении ресурсов, проведении оценки рисков ИБ и определении/коррекции планов их обработки, разработке механизмов и процессов управления ИБ [2], [3].

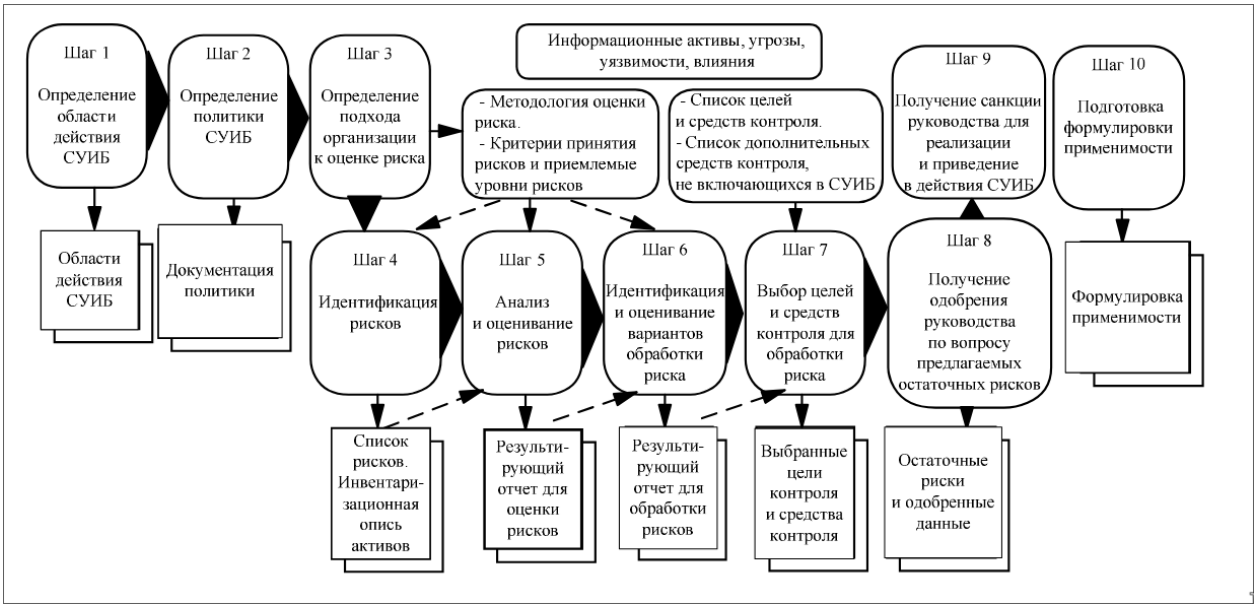

Рисунок 4 – Шаги планирования СУИБ

При проведении обследования организации основными источниками информации являются документы организации (политики, процедуры, инструкции и т. д.) и результаты интервьюирования сотрудников организации. После обследования организация должна выполнить следующие шаги (рис. 4) [2], [3], [5]:

1. Наметить/уточнить область и границы действия СУИБ с учетом характеристик бизнеса, организации, ее размещения, активов и технологий, также включая детали и обоснования любых исключений из области действия; при этом важно учесть все риски для организации (операционные, репутационные и т. п.).

2. Определить/уточнить политику СУИБ (она имеет приоритет по сравнению с ПолИБ организации, хотя они и могут быть представлены одним общим документом) на основе характеристик бизнеса организации, ее размещения, активов и технологий, которая:
   - включает в себя концепцию для установки целей, основных направлений и принципов действия в отношении ИБ;
   - учитывает бизнес-требования и нормативно-правовые требования (включая международные и национальные стандарты в области ОИБ), а также договорные обязательства по ОИБ;
   - согласуется со стратегическим управлением рисками организации, в рамках которого будет происходить разработка и поддержка СУИБ;
   - устанавливает критерии оценки рисков;
   - утверждается руководством.
3. Установить/уточнить подход к оценке рисков ИБ для наиболее критичных активов и бизнес-процессов организации, включая:
   - методологию оценки рисков ИБ, которая применима для СУИБ и соответствует установленным бизнес-требованиям по ОИБ и нормативно-правовым требованиям; она должна давать сравнимые и воспроизводимые результаты;
   - критерии принятия рисков и приемлемые уровни риска.
4. Выявить и идентифицировать риски ИБ, определив:
   - защищаемые активы в рамках области действия СУИБ, а также владельцев этих активов;
   - угрозы ИБ для этих активов;
   - уязвимости активов, которые могут быть использованы угрозами ИБ;
   - негативные последствия, которые ведут к потере конфиденциальности, целостности и доступности активов.
5. Проанализировать и оценить риски ИБ, для чего необходимо оценить:
   - ущерб для деятельности организации, который может быть нанесен в результате сбоя в ОИБ, с учетом возможных последствий нарушения конфиденциальности, целостности или доступности активов;

- реальную вероятность сбоя в ОИБ с учетом превалирующих угроз, уязвимостей и их последствий, связанных с этими активами, а также применяемых на текущий момент мер управления ИБ;
- уровни рисков;
- являются ли риски приемлемыми или требуют обработки с использованием критериев приемлемых рисков.

6. Определить и оценить различные варианты обработки рисков ИБ, среди которых:
   - применение подходящих мер управления;
   - сознательное и объективное принятие рисков при условии, что они полностью соответствуют требованиям политики и критериям организации в отношении принятия рисков;
   - избежание риска;
   - передача соответствующих бизнес-рисков сторонним организациям, например страховщикам или поставщикам.
7. Выбрать цели и меры управления (защитные меры) для обработки рисков ИБ, которые должны удовлетворять требованиям, определенным в процессе оценки и обработки рисков, с учетом критериев принятия рисков и нормативно-правовых требований и договорных обязательств.
8. Получить утверждение руководством предлагаемых остаточных рисков ИБ.
9. Получить разрешение руководства на внедрение и эксплуатацию СУИБ.
10. Подготовить Положение о применимости, которое включает:
    - цели и меры управления и обоснование этого выбора;
    - цели и меры управления, реализованные в настоящее время;
    - перечень исключений целей и мер управления и процедуру обоснования их исключения.

Фактически представленные шаги этапа планирования СУИБ преследуют цель принятия решения организацией по трем основным вопросам:

- установление области действия и политики СУИБ (шаги 1 и 2);
- выбор защитных мер на основе управления рисками ИБ (шаги 3–7);
- получение одобрения руководства для мер обработки рисков ИБ и подготовка формулировки применимости требований, так как это влечет организационные и, возможно, финансовые издержки организации (шаги 8–10).

Выходом данного этапа являются разработанные процессы управления ИБ, процедуры, поддерживающие и обеспечивающие работу этих процессов, а также инструкции для пользователей процессов и исполнителей ролей в рамках процессов.

3 Пример стадии планирования в СУИБ

Все перечисленные действия являются весьма объемными и трудоемкими. Для их выполнения необходимо создание рабочей группы специалистов из разных подразделений организации, обладающих достаточными знаниями и полномочиями для принятия управленческих решений на всех этапах построения и последующего внедрения СУИБ. Помимо этого руководство организации должено быть также заинтересовано в построении СУИБ. Важно, чтобы все решения на этапе «Планирование» были поддержаны и приняты руководством. Приверженность последнего может существенно облегчить разработку и внедрение системы.

Представленные ниже примеры, основанные на деятельности гипотетического ООО «Торговые сети», служат исключительно для иллюстрации логики и последовательности шагов этапа планирования. Они являются сильно упрощённой моделью, призванной сделать сложные концепции более наглядными и понятными. Переход от такого модельного примера к реальной работе требует осознания масштаба и глубины необходимых усилий.

1. Наметить/уточнить область и границы действия СУИБ

- Область действия: СУИБ в первую очередь охватывает бизнес-процессы, связанные с обработкой персональных данных клиентов (программа лояльности) и проведением финансовых транзакций (онлайн-оплата, эквайринг). В границы системы включены: центральный офис, серверная комната, корпоративный сайт и мобильное приложение для заказов.
- Исключения: СУИБ не распространяется на изолированную локальную сеть бухгалтерии, где хранятся архивные данные прошлых лет, не имеющие связи с внешними сетями.
- Обоснование исключения: Низкий уровень риска (данные неактуальны, сеть физически изолирована) и непропорционально высокие затраты на интеграцию устаревшей системы в общую СУИБ.
- Учтённые риски: Помимо прямых рисков ИБ, учтены операционные (остановка работы онлайн-касс) и репутационные (публикация в СМИ об утечке данных клиентов).

2. Определить/уточнить политику СУИБ

ПолИБ ООО «Торговые сети»»:

- Концепция и цели: «Целью Политики является обеспечение конфиденциальности данных клиентов, целостности и достоверности финансовых операций, а также высокой доступности (99.9%) корпоративного сайта и систем онлайн-платежей. Основополагающий принцип — уровень защиты актива должен быть адекватен его ценности для бизнеса и степени связанного с ним риска».
- Учтённые требования:
  - Бизнес-требования: Непрерывность процесса онлайн-торговли как ключевого канала продаж.
  - Нормативные требования: Федеральный закон № 152-ФЗ «О персональных данных», стандарт безопасности данных индустрии платёжных карт (PCI DSS).
  - Договорные обязательства: Соглашение с банком-эквайером об обеспечении безопасности платёжных транзакций.
- Согласование со стратегией управления рисками: Политика является частью общей корпоративной стратегии по управлению рисками, утверждённой Советом директоров.
- Критерии оценки рисков: Уровень риска определяется по матрице 5x5 как произведение балльной оценки потенциального ущерба (1 — незначительный, 5 — катастрофический) и вероятности (1 — крайне маловероятно, 5 — почти неизбежно). Риски с уровнем $\geq$12 требуют обязательной обработки.
- Утверждение: Политика подписана Генеральным директором 15.10.2023.

3. Установить/уточнить подход к оценке рисков ИБ

- Методология: Принята методология OCTAVE Allegro. Процесс оценки является качественно-количественным, фокусируется на активах и сценариях ущерба для бизнеса.
- Рабочая группа: Для проведения оценки сформирована группа в составе: IT-директор (руководитель), руководитель отдела продаж, юрист, системный администратор, специалист по защите персональных данных.

- Критерии принятия рисков: Установлены пороговые значения:
  - ≤ 4 — риск принимается без дополнительных действий.
  - $5 - 11$ — риск принимается к плановой обработке в рамках ежегодного бюджета ИБ.
  - ≥ 12 — риск требует немедленной или приоритетной обработки.

4. Выявить и идентифицировать риски ИБ

Рассматривается риск, связанный с базой данных клиентов программы лояльности.

- Актив: База данных персональных данных клиентов (ФИО, телефоны, e-mail, история покупок).
- Владелец актива: Директор по маркетингу.
- Угроза: Целенаправленная фишинговая атака на сотрудника отдела поддержки с целью получения учётных данных для доступа к базе.
- Уязвимость: Отсутствие обязательной двухфакторной аутентификации (2FA) для доступа к административному интерфейсу базы данных из корпоративной сети.
- Негативные последствия:
  - Конфиденциальность: Массовая утечка персональных данных.
  - Репутация: Существенный ущерб деловой репутации, потеря доверия клиентов.
  - Правовые: Штрафы от Роскомнадзора по 152-ФЗ, возможные иски от клиентов.

5. Проанализировать и оценить риски ИБ

Для идентифицированного риска проводится оценка:

- Ущерб (оценка 4/5): Крупный финансовый ущерб: штрафы до 300 тыс. руб., затраты на уведомление клиентов и услуги call-центра, компенсации, падение выручки. Репутационный ущерб — значительный.
- Вероятность (оценка 3/5): Фишинг — одна из наиболее распространённых угроз. Целевые фишинговые атаки на сотрудников среднего звена становятся частыми. Наличие уязвимости (простые пароли, отсутствие 2FA) повышает вероятность успеха.
- Уровень риска: $4 \times 3 = 12$.

– Решение: Уровень риска (12) соответствует критерию «требует обработки». Без принятия мер риск является неприемлемым.

6. Определить и оценить различные варианты обработки рисков ИБ

Рассмотрены следующие варианты для риска с уровнем 12:

а) Применение мер управления (Снижение риска):
   – Меры: Внедрить обязательную двухфакторную аутентификацию для всех административных доступов к базам данных. Внедрить ежегодное обязательное обучение и тестирование сотрудников на устойчивость к фишингу.
   – Ожидаемый результат: Уровень риска снижается до 6 (ущерб 4, вероятность 1.5).
   – Затраты: 150 тыс. руб. (лицензии на 2FA + работа подрядчика + час рабочего времени сотрудников на обучение).

б) Сознательное принятие риска:
   – Оставить существующее положение без изменений.
   – Недостаток: Не соответствует установленной политике и критериям (риск > 4), ведёт к вероятным значительным потерям.

в) Избежание риска:
   – Закрыть программу лояльности и уничтожить базу данных клиентов.
   – Недостаток: Полностью неприемлемо для бизнеса, ведёт к потере конкурентного преимущества и клиентской базы.

г) Передача риска:
   – Приобрести полис киберстрахования, покрывающий расходы на реагирование на инциденты утечки данных.
   – Применение: Может быть рассмотрено как дополнительная мера к варианту 1 для финансовой компенсации остаточного ущерба.

7. Выбрать цели и меры управления (защитные меры)

На основании анализа выбран Вариант 1 (снижение риска).

– Цель ИБ: Снизить риск несанкционированного доступа к конфиденциальным данным клиентов до приемлемого уровня (менее 12) в течение 202X финансового года.

- Выбранные меры управления (соотнесение с ISO/IEC 27001:2022):
  - A.5.14 (Управление доступом) — Внедрить двухфакторную аутентификацию для всех привилегированных учётных записей и доступов к критически важным информационным системам.
  - A.6.3 (Осведомленность в области ИБ) — Реализовать ежегодную программу обучения и тестирования всех сотрудников по вопросам фишинга и социальной инженерии.
  - A.5.24 (Обработка информации) — Классифицировать базу данных клиентов как «Конфиденциально» и применить соответствующие меры защиты.

8. Получить утверждение руководством предлагаемых остаточных рисков ИБ

- IT-директор готовит и представляет Генеральному директору «Отчёт об оценке и обработке рисков».
- В отчёте указывается, что после реализации выбранных мер (2FA, обучение) уровень риска снижается с 12 до 6.
- Уровень 6 попадает в категорию «принимается к плановой обработке» и соответствует установленным критериям.
- Генеральный директор визирует отчёт, тем самым формально утверждая новый (остаточный) уровень риска как приемлемый для компании.

9. Получить разрешение руководства на внедрение и эксплуатацию СУИБ

- На основе утверждённых планов обработки рисков и Положения о применимости готовится «План проекта по внедрению СУИБ».
- План включает: перечень конкретных работ (внедрение 2FA, проведение обучения), сроки (Q1-Q2 202X), бюджет (150 тыс. руб.), ответственных исполнителей.
- Генеральный директор издаёт Приказ № 45-К «О внедрении системы управления информационной безопасностью», которым утверждает план, выделяет ресурсы и назначает ответственных, давая официальный старт этапу внедрения (Do).

10. Подготовить Положение о применимости (SoA)

- Формируется итоговый документ — «Положение о применимости (Statement of Applicability) СУИБ ООО «Торговые сети»».
- Документ представляет собой таблицу, где для контролей из Приложения A ISO/IEC 27001 (или иного выбранного стандарта) указывается:

Контроль	Решение	Обоснование
A.5.14 (Двухфакторная аутентификация)	Применимо	Выбрано для обработки риска несанкционированного доступа к БД клиентов (ID риска RD-005).
A.6.3 (Обучение осведомлённости)	Применимо	Выбрано для снижения риска успешных фишинговых атак (ID риска RD-005). Реализуется с 202X г.
A.8.11 (Безопасная разработка)	Исключено	Организация не ведёт внутреннюю разработку программного обеспечения, использует готовые сторонние решения.

Этот документ становится основным артефактом, связывающим оценку рисков, выбранные меры защиты и требования стандарта.

Итог: ответ на три ключевых вопроса этапа планирования

а) Установление области и политики СУИБ (шаги 1 и 2): Для ООО «Торговые сети» область определена вокруг защиты данных клиентов и финансовых транзакций. Политика закрепила приоритеты и критерии, увязанные с бизнес-целями и законом.

б) Выбор защитных мер на основе управления рисками (шаги 3–7): Через систематическую оценку выявлен ключевой риск (фишинг → утечка). Проанализированы варианты, выбраны экономически обоснованные и эффективные меры (2FA и обучение).

в) Получение одобрения руководства и подготовка SoA (шаги 8–10): Руководство официально утвердило остаточные риски, санкционировало расходы и работы. Вся логика принятых решений задокументирована в Положении о применимости, что обеспечивает прозрачность и обоснованность СУИБ.

ЗАКЛЮЧЕНИЕ

Проведенное исследование этапа планирования в системе управления информационной безопасностью (СУИБ) позволяет сформулировать ряд основополагающих выводов, подтверждающих его критическую роль в создании жизнеспособной и эффективной системы защиты информации.

Во-первых, анализ теоретических основ показал, что планирование не является разовой процедурой, а представляет собой циклический и итерационный процесс, интегрированный в модель непрерывного улучшения PDCA (Plan-Do-Check-Act). Этот подход, унаследованный из теории управления качеством, обеспечивает системность и адаптивность СУИБ, позволяя организации гибко реагировать на изменения внутреннего и внешнего контекста. Планирование задает направление для всего последующего цикла, определяя политику, цели, области применения и методологию управления рисками, что делает его фундаментом для всех последующих стадий — внедрения, мониторинга и совершенствования.

Во-вторых, в работе детально рассмотрены ключевые процессы и действия, составляющие суть стадии планирования. Их можно структурировать в три логических блока, отвечающих на главные вопросы организации:

а) Установление рамок системы (определение области действия и разработка политики СУИБ).

б) Управление рисками как ядро планирования (выбор методологии оценки, идентификация, анализ, оценка и обработка рисков).

в) Формализация решений и получение санкции руководства (утверждение остаточных рисков, получение разрешения на внедрение, подготовка Положения о применимости).

Каждый из десяти шагов, проиллюстрированных на примере гипотетической компании, демонстрирует, как абстрактные принципы стандартов трансформируются в конкретные, измеримые и обоснованные управленческие решения. Важно подчеркнуть, что представленный пример является существенным упрощением; в реальности каждый из этих шагов требует значительных временных, кадровых и финансовых ресурсов, а также активного участия и поддержки высшего руководства.

Таким образом, можно утверждать, что этап планирования является стратегическим и определяющим для всей СУИБ. Его основная цель — не просто составить список мероприятий, а создать обоснованную, документированную и согласованную с бизнес-целями модель будущей системы безопасности. Качество проработки этого этапа напрямую определяет, будет ли СУИБ формальной обузой для организации или эффективным инструментом управления рисками, способствующим достижению ее стратегических целей в условиях современных цифровых угроз.

СПИСОК ИСПОЛЬЗОВАННЫХ ИСТОЧНИКОВ

1. Развитие производственных систем: стратегия бизнес-прорыва. Кайдзен. Лидерство. Бережливое производство / под ред. А. Баранов, Р. Нугайбеков. — СПб. : Питер, 2015. — С. 192—196. 272 с.

2. ГОСТ Р ИСО/МЭК 27001-2006: Информационная технология. Методы и средства обеспечения безопасности. Системы менеджмента информационной безопасности. Требования. — М. : Международная организация по стандартизации, 2008.

3. ISO/IEC 27001:2005: Information technology. Security techniques. Information security management systems. Requirements. — International Organization for Standardization, 2005. — URL: http : / / www . iso . org ; Электронный ресурс.

4. Теория автоматического управления: в 2 ч. / под ред. А. Воронов. — М. : Высшая школа, 1986. — 2 ч.

5. Обеспечение информационной безопасности бизнеса / под ред. А. И. Курило. — М. : Альпина Паблишерз, 2011.