

МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ РОССИЙСКОЙ ФЕДЕРАЦИИ
Федеральное государственное автономное образовательное учреждение
высшего образования
«СЕВЕРО-КАВКАЗСКИЙ ФЕДЕРАЛЬНЫЙ УНИВЕРСИТЕТ»

Методические указания

по дисциплине

«Менеджмент инцидентов информационной безопасности
информационных систем»

для студентов

Специальности 10.05.03 Информационная безопасность
автоматизированных систем

Специализация «Анализ безопасности информационных систем»

Ставрополь
2026

Лабораторная работа 1

Принципы системного подхода и этапы системных исследований при проектировании сложных систем

Цель работы: ознакомиться с базовыми принципами системного подхода, изучить основные этапы системных исследований, а также понять их значение и применение при проектировании сложных технических, организационных и информационных систем.

Теоретическая часть

Системный подход — это методологическая основа анализа, проектирования и управления сложными объектами и процессами, основанная на рассмотрении объекта как целостной системы, состоящей из взаимосвязанных и взаимодействующих элементов. Он позволяет рассматривать проблему не просто как сумму отдельных частей, а как единую структуру, в которой важна каждая часть и её взаимодействие с другими.

Основные принципы системного подхода включают целостность, иерархичность, целенаправленность, открытость системы, управление, обратную связь и динамичность. Каждый из этих принципов отражает ключевые особенности системного мышления и помогает выявлять закономерности, оптимизировать процессы и принимать обоснованные решения.

Целостность подразумевает рассмотрение системы как единого объекта, где свойства целого не сводятся к сумме свойств частей. Иерархичность отражает организацию систем на различных уровнях, что позволяет более эффективно управлять сложностью. Целенаправленность означает, что система функционирует для достижения определённых целей, а управление и обратная связь обеспечивают возможность корректировки поведения системы в зависимости от изменений во внешней среде.

Проектирование сложных систем требует системных исследований, включающих последовательные этапы, позволяющие обеспечить глубокое понимание объекта, выявление проблем, формулирование требований и разработку решений. Типичные этапы системных исследований следующие: формулирование проблемы, сбор и анализ данных, построение моделей системы, проведение экспериментов и оценка результатов, разработка рекомендаций и внедрение решений.

На первом этапе — формулирование проблемы — происходит определение цели исследования, постановка задач и выделение границ системы. Затем осуществляется сбор информации о системе и её окружении, что позволяет выявить ключевые характеристики и ограничения. Построение моделей —

важный этап, когда создаются абстрактные или математические представления системы для анализа её поведения и прогноза изменений. Экспериментальные исследования дают возможность проверить корректность моделей и оценить эффективность предложенных решений. Финальный этап связан с разработкой рекомендаций для практического применения и мониторингом их реализации.

Системный подход и этапы системных исследований лежат в основе современных методов проектирования сложных систем в различных областях: инженерии, экономике, управлении, информационных технологиях и других. Они обеспечивают системность, научность и комплексность в решении сложных задач, что критично для успешной реализации проектов.

Задания

1. Определите основные принципы системного подхода и приведите примеры их применения в проектировании сложных систем.
2. Проанализируйте пример реальной сложной системы (например, автоматизированная транспортная система, информационная система предприятия) с точки зрения системного подхода. Определите её границы, уровни и цели.
3. Опишите последовательность этапов системных исследований при проектировании выбранной системы. Какие методы и инструменты могут быть использованы на каждом этапе?
4. Постройте блок-схему типичного процесса системного исследования, выделив ключевые этапы и переходы между ними.
5. Рассмотрите роль обратной связи в управлении сложной системой. Как она влияет на устойчивость и адаптивность системы?
6. Сформулируйте проблему, связанную с проектированием сложной системы в выбранной области, и опишите, как системный подход помогает её решать.
7. Проанализируйте, каким образом иерархичность систем облегчает процесс управления и принятия решений.
8. Исследуйте влияние внешней среды на функционирование сложной системы и методы учёта этого влияния в системных исследованиях.

Таблица: Основные принципы системного подхода

Принцип	Описание	Пример применения
Целостность	Рассмотрение системы как единого целого, свойства которого не сводятся к свойствам частей	Анализ предприятия как единого организма

Иерархичность	Организация системы на уровнях, упрощение управления сложностью	Многоуровневая структура управления проектом
Целенаправленность	Система существует для достижения определённых целей	Автоматизированная система управления движением
Открытость	Взаимодействие с внешней средой, обмен ресурсами и информацией	Система обмена данными между отделами
Управление	Процесс регулирования поведения системы	Контроль качества продукции
Обратная связь	Механизм корректировки на основе результатов	Система автоматической настройки параметров
Динамичность	Изменение системы во времени, адаптация к изменениям среды	Обновление программного обеспечения

Системный подход и этапы системных исследований являются фундаментальными элементами современной инженерной и управленческой практики, обеспечивая качественное решение сложных проблем, повышение эффективности систем и достижение устойчивого развития в различных сферах человеческой деятельности. Данная лабораторная работа позволит студентам освоить ключевые концепции и методы, необходимые для успешного проектирования и управления сложными системами.

Лабораторная работа 2

Основные положения системного подхода к проектированию сложных систем

Цель работы: изучить ключевые положения системного подхода, раскрыть их значение и применимость при проектировании сложных технических и организационных систем, а также научиться использовать эти положения для анализа и проектирования систем.

Теоретическая часть

Системный подход к проектированию сложных систем базируется на ряде фундаментальных положений, которые обеспечивают целостное, комплексное и эффективное решение задач. Эти положения сформированы на основе многолетних исследований и практического опыта и служат основой для успешного создания и управления сложными системами.

Одним из основных положений является признание сложности систем как неизбежного свойства, требующего системного мышления и специальных методов управления. Сложные системы характеризуются большим числом

элементов и взаимосвязей, высокой степенью интеграции и динамичностью, что делает невозможным эффективное управление без системного анализа.

Важнейшее положение — целостность, которая требует рассматривать систему не просто как набор частей, а как единое целое, обладающее собственными свойствами, не сводимыми к сумме свойств элементов. Это положение помогает выявлять скрытые взаимосвязи и оптимизировать работу всей системы.

Следующее положение — иерархичность, которое отражает структурирование сложных систем на уровни, позволяющие разделять задачи и управлять ими с разных масштабов. Иерархичность способствует упрощению анализа и позволяет внедрять управленческие решения, адаптированные к конкретным уровням системы.

Положение о целенаправленности подчеркивает, что система проектируется и функционирует для достижения определённых целей, которые должны быть чётко сформулированы и измеримы. Это помогает сфокусировать усилия и ресурсы на ключевых результатах.

Не менее важным является положение об открытости системы, которое подразумевает её взаимодействие с внешней средой через обмен информацией, материалами, энергией. Учет влияния внешней среды позволяет создавать адаптивные и устойчивые системы.

Положение об управлении и обратной связи раскрывает необходимость наличия механизмов контроля и коррекции поведения системы, позволяющих реагировать на изменения и сохранять стабильность.

Динамичность систем отражает их способность изменяться во времени, приспосабливаться к новым условиям и развиваться, что требует гибкости в проектировании и управлении.

При проектировании сложных систем эти положения используются в комплексе, что обеспечивает системный и всесторонний подход к решению задач. Они помогают не только описывать систему, но и моделировать её поведение, прогнозировать изменения, выявлять узкие места и разрабатывать эффективные решения.

Задания

1. Опишите каждое из основных положений системного подхода к проектированию сложных систем, приведите примеры из практики, иллюстрирующие применение каждого положения.
2. Рассмотрите конкретный пример сложной системы (например, система управления производством или транспортная система) и

- проанализируйте, как каждое положение системного подхода реализуется на практике.
3. Постройте схему иерархической структуры выбранной системы, обозначив уровни управления и основные элементы.
 4. Опишите, каким образом положение о целенаправленности влияет на постановку задач и определение критериев успешности проектирования системы.
 5. Проанализируйте влияние открытости системы на её устойчивость и адаптивность к внешним изменениям.
 6. Исследуйте роль обратной связи в управлении сложной системой и опишите методы её реализации.
 7. Обсудите, каким образом динамичность систем требует использования гибких методов проектирования и управления.
 8. Составьте таблицу, сопоставляющую основные положения системного подхода с возможными рисками при их игнорировании в процессе проектирования.

Таблица: Основные положения системного подхода и последствия их игнорирования

Положение системного подхода	Описание	Последствия игнорирования
Сложность	Признание многогранности и взаимосвязанности элементов	Неспособность эффективно управлять системой
Целостность	Рассмотрение системы как единого целого	Фрагментарный анализ и принятие ошибочных решений
Иерархичность	Структурирование системы на уровни	Потеря контроля и хаос в управлении
Целенаправленность	Четкое определение целей и задач	Распыление ресурсов и отсутствие результата
Открытость	Взаимодействие с внешней средой	Невозможность адаптации к изменениям
Управление и обратная связь	Наличие механизмов контроля и коррекции	Стабильность и эффективность снижаются
Динамичность	Способность системы к изменению и развитию	Устаревание и потеря конкурентоспособности

Основываясь на изучении основных положений системного подхода, студенты смогут глубже понять суть проектирования сложных систем, выявлять и учитывать ключевые характеристики систем в своих исследованиях и проектах, а также использовать системное мышление для

повышения качества принимаемых решений и успешной реализации проектов.

Лабораторная работа 2. Основные положения системного подхода к проектированию сложных систем

Цель работы: изучить ключевые положения системного подхода, раскрыть их значение и применимость при проектировании сложных технических и организационных систем, а также научиться использовать эти положения для анализа и проектирования систем.

Теоретическая часть

Системный подход к проектированию сложных систем базируется на ряде фундаментальных положений, которые обеспечивают целостное, комплексное и эффективное решение задач. Эти положения сформированы на основе многолетних исследований и практического опыта и служат основой для успешного создания и управления сложными системами.

Одним из основных положений является признание сложности систем как неизбежного свойства, требующего системного мышления и специальных методов управления. Сложные системы характеризуются большим числом элементов и взаимосвязей, высокой степенью интеграции и динамичностью, что делает невозможным эффективное управление без системного анализа.

Важнейшее положение — целостность, которая требует рассматривать систему не просто как набор частей, а как единое целое, обладающее собственными свойствами, не сводимыми к сумме свойств элементов. Это положение помогает выявлять скрытые взаимосвязи и оптимизировать работу всей системы.

Следующее положение — иерархичность, которое отражает структурирование сложных систем на уровни, позволяющие разделять задачи и управлять ими с разных масштабов. Иерархичность способствует упрощению анализа и позволяет внедрять управленческие решения, адаптированные к конкретным уровням системы.

Положение о целенаправленности подчеркивает, что система проектируется и функционирует для достижения определённых целей, которые должны быть чётко сформулированы и измеримы. Это помогает сфокусировать усилия и ресурсы на ключевых результатах.

Не менее важным является положение об открытости системы, которое подразумевает её взаимодействие с внешней средой через обмен информацией, материалами, энергией. Учет влияния внешней среды позволяет создавать адаптивные и устойчивые системы.

Положение об управлении и обратной связи раскрывает необходимость наличия механизмов контроля и коррекции поведения системы, позволяющих реагировать на изменения и сохранять стабильность.

Динамичность систем отражает их способность изменяться во времени, приспосабливаться к новым условиям и развиваться, что требует гибкости в проектировании и управлении.

При проектировании сложных систем эти положения используются в комплексе, что обеспечивает системный и всесторонний подход к решению задач. Они помогают не только описывать систему, но и моделировать её поведение, прогнозировать изменения, выявлять узкие места и разрабатывать эффективные решения.

Задания

1. Опишите каждое из основных положений системного подхода к проектированию сложных систем, приведите примеры из практики, иллюстрирующие применение каждого положения.
2. Рассмотрите конкретный пример сложной системы (например, система управления производством или транспортная система) и проанализируйте, как каждое положение системного подхода реализуется на практике.
3. Постройте схему иерархической структуры выбранной системы, обозначив уровни управления и основные элементы.
4. Опишите, каким образом положение о целенаправленности влияет на постановку задач и определение критериев успешности проектирования системы.
5. Проанализируйте влияние открытости системы на её устойчивость и адаптивность к внешним изменениям.
6. Исследуйте роль обратной связи в управлении сложной системой и опишите методы её реализации.
7. Обсудите, каким образом динамичность систем требует использования гибких методов проектирования и управления.
8. Составьте таблицу, сопоставляющую основные положения системного подхода с возможными рисками при их игнорировании в процессе проектирования.

Таблица: Основные положения системного подхода и последствия их игнорирования

Положение системного подхода	Описание	Последствия игнорирования
Сложность	Признание многогранности и взаимосвязанности элементов	Неспособность эффективно управлять системой
Целостность	Рассмотрение системы как единого целого	Фрагментарный анализ и принятие ошибочных решений
Иерархичность	Структурирование системы на уровни	Потеря контроля и хаос в управлении
Целенаправленность	Четкое определение целей и задач	Распыление ресурсов и отсутствие результата
Открытость	Взаимодействие с внешней средой	Невозможность адаптации к изменениям
Управление и обратная связь	Наличие механизмов контроля и коррекции	Стабильность и эффективность снижаются
Динамичность	Способность системы к изменению и развитию	Устаревание и потеря конкурентоспособности

Основываясь на изучении основных положений системного подхода, студенты смогут глубже понять суть проектирования сложных систем, выявлять и учитывать ключевые характеристики систем в своих исследованиях и проектах, а также использовать системное мышление для повышения качества принимаемых решений и успешной реализации проектов.

Лабораторная работа 3. Положения и задачи системного анализа. Понятие и характеристики проблемы

Цель работы: изучить основные положения системного анализа, выявить ключевые задачи данного метода, а также освоить понятие проблемы в контексте системных исследований и определить её основные характеристики.

Теоретическая часть

Системный анализ — это методологический подход, направленный на изучение и решение сложных проблем, возникающих в системах различной природы. Его цель — выявление причинно-следственных связей, оценка состояния системы, разработка эффективных решений и оптимизация процессов.

Основные положения системного анализа включают в себя целостный и комплексный подход к изучению систем, систематизацию информации, моделирование и прогнозирование поведения системы. При этом внимание уделяется не только отдельным элементам, но и их взаимодействию, а также внешним условиям функционирования.

Одной из ключевых задач системного анализа является постановка правильной проблемы. Проблема в системном подходе понимается как ситуация, в которой существующее состояние системы не удовлетворяет заданным критериям или целям, и требует изменений. Правильное понимание и формулирование проблемы — это фундамент для эффективного решения.

Проблема характеризуется рядом признаков: она всегда связана с существующей или потенциальной неопределённостью, содержит конфликт между желаемым и реальным состоянием, требует анализа и принятия управленческих решений. Важным является и то, что проблема существует в контексте системы, и её решение должно учитывать системные взаимосвязи.

Характеристики проблемы включают:

- Сложность, которая обусловлена множественностью факторов и взаимосвязей.
- Многоаспектность, так как проблема может иметь технические, экономические, социальные и другие аспекты.
- Динамичность, отражающая изменения условий и среды функционирования системы.
- Неоднозначность, когда отсутствует однозначное решение, требующее поиска компромиссов.
- Ограниченность ресурсов, что накладывает дополнительные условия на принятие решений.

Системный анализ предполагает последовательное выполнение этапов: определение проблемы, сбор и анализ информации, моделирование, разработка вариантов решений, оценка их эффективности и выбор оптимального варианта.

Важной частью системного анализа является формализация проблемы — переход от общих описаний к чётким моделям и параметрам, позволяющим объективно оценивать состояние системы и результаты воздействия на неё.

Использование системного анализа при проектировании сложных систем позволяет минимизировать риски, повысить качество решений и обеспечить сбалансированное развитие системы с учётом всех факторов.

Задания

1. Дайте определение системному анализу и опишите его основные положения.
2. Раскройте задачи системного анализа на различных этапах исследования.
3. Определите понятие проблемы в контексте системного подхода и опишите её ключевые характеристики.
4. Проанализируйте пример сложной технической или организационной системы, выявите в ней существующую проблему и охарактеризуйте её по основным признакам.
5. Выполните формализацию выбранной проблемы, представив её в виде структурированной модели с основными параметрами и взаимосвязями.
6. Опишите, каким образом многоаспектность и динамичность проблемы влияют на выбор методов системного анализа.
7. Составьте таблицу с характеристиками проблемы и возможными последствиями их игнорирования при проектировании систем.
8. Разработайте краткий план этапов системного анализа для решения выбранной проблемы, учитывая особенности системы и доступные ресурсы.

Таблица: Характеристики проблемы и их влияние на процесс системного анализа

Характеристика проблемы	Описание	Влияние на системный анализ
Сложность	Множество факторов и взаимосвязей	Требует комплексного подхода и детального моделирования
Многоаспектность	Наличие технических, экономических и социальных аспектов	Необходимость привлечения экспертов разных областей
Динамичность	Изменение условий функционирования системы	Требует адаптивных и гибких методов анализа
Неоднозначность	Отсутствие однозначного решения	Требует оценки альтернатив и поиска компромиссов
Ограниченность ресурсов	Недостаток времени, финансов или информации	Влияет на выбор приоритетов и оптимизацию решений

Изучение положений и задач системного анализа, а также характеристик проблем, позволит студентам лучше понимать сложность реальных ситуаций

и использовать системный подход для разработки эффективных и устойчивых решений. Это является основой для успешного проектирования и управления сложными системами в различных областях деятельности.

Лабораторная работа 4. Порядок обоснования и выработка требований к проектируемой системе

Цель работы: ознакомиться с методами обоснования проектирования систем, изучить процесс выработки требований к проектируемой системе, а также освоить навыки формализации и документирования этих требований.

Теоретическая часть

Обоснование проектирования системы — это ключевой этап в жизненном цикле сложных систем, который направлен на определение необходимости создания системы, выявление её целей и задач, а также на формулирование требований, обеспечивающих достижение заданных целей. От правильности и полноты обоснования зависит успешность всего проекта и эффективность будущей системы.

Процесс обоснования включает анализ текущей ситуации, выявление проблем и ограничений, а также оценку потребностей заинтересованных сторон (стейкхолдеров). Важным элементом является анализ альтернативных решений — сравнение существующих систем, технологий и методов, позволяющее выбрать наиболее подходящий вариант.

Выработка требований к проектируемой системе основывается на результатах обоснования и направлена на формализацию функциональных и нефункциональных потребностей системы. Функциональные требования описывают конкретные действия и процессы, которые система должна выполнять. Нефункциональные требования отражают качество системы, такие как надёжность, производительность, безопасность, удобство использования и т.д.

Требования могут быть сформулированы в различных формах: текстовые описания, схемы, диаграммы, формальные спецификации. Для системного подхода характерна необходимость строгой классификации и структурирования требований, что обеспечивает их однозначность и полноту.

Порядок выработки требований включает несколько этапов:

1. Сбор требований — проведение интервью, опросов, анализ документации и нормативных актов, изучение опыта эксплуатации аналогичных систем.

2. Анализ и уточнение требований — выявление противоречий, избыточности и недостаточности, оценка реалистичности и приоритетов.
3. Формализация требований — оформление требований в стандартизированном виде, использование моделей и шаблонов.
4. Верификация требований — проверка соответствия требований целям проекта и согласование с заинтересованными сторонами.
5. Управление требованиями — ведение изменений, отслеживание статуса и истории модификаций.

Правильно выработанные требования служат основой для последующих этапов проектирования, разработки и тестирования системы. Ошибки на данном этапе могут привести к значительным затратам и снижению качества итогового продукта.

Важной частью является документирование требований в техническом задании (ТЗ) или спецификации, где четко фиксируются все согласованные условия, ограничения и критерии приемки.

Особое внимание уделяется приоритетам требований, которые определяют очередность реализации и помогают управлять ресурсами. В условиях ограниченного времени и бюджета необходимо сфокусироваться на наиболее важных аспектах.

Современные методы системного проектирования используют различные инструменты для поддержки процесса выработки требований: CASE-средства, системы управления требованиями, методологии Agile и др.

Задания

1. Опишите этапы обоснования необходимости проектирования сложной системы на примере выбранной области (технической, социальной, экономической).
2. Составьте список заинтересованных сторон и опишите их основные потребности и ожидания от проектируемой системы.
3. Проведите анализ существующих решений в выбранной области и сформулируйте обоснование выбора нового проекта.
4. Разработайте функциональные требования к проектируемой системе, описав не менее пяти основных функций.
5. Сформулируйте нефункциональные требования, включив критерии качества, безопасности и удобства использования.
6. Представьте требования в виде таблицы, распределив их по категориям и указывая приоритеты.
7. Проведите проверку и уточнение требований, выявив возможные противоречия или дублирования.

8. Создайте краткий проект технического задания (ТЗ), включив в него цели, задачи, требования и критерии приемки системы.
9. Опишите методы управления изменениями требований на протяжении жизненного цикла системы.

Таблица: Пример структурирования требований к проектируемой системе

Категория требований	Описание	Приоритет	Примечания
Функциональные	Обработка пользовательских запросов	Высокий	Ключевая функция системы
Функциональные	Генерация отчетов по заданным параметрам	Средний	Требуется для управления проектом
Нефункциональные	Время отклика системы не более 2 секунд	Высокий	Важно для удобства пользователей
Нефункциональные	Обеспечение безопасности данных	Высокий	Критично для соответствия нормам
Нефункциональные	Возможность расширения функционала в будущем	Средний	Предусмотреть модульную архитектуру

Данная работа позволит студентам освоить системный подход к формированию требований и научит формализовывать потребности, что является основой успешного проектирования сложных систем. Понимание порядка обоснования и выработки требований способствует снижению рисков и повышению качества создаваемых продуктов.

Лабораторная работа 5. Порядок и содержание постановки сложной проблемы

Цель работы: изучить основные этапы и методы постановки сложных проблем в процессе системных исследований и проектирования, освоить навыки формализации проблемной ситуации, а также выработки критериев и характеристик проблемы.

Теоретическая часть

Постановка проблемы — это фундаментальный этап системного подхода, который направлен на четкое определение и описание сложной проблемы, требующей решения в рамках проектирования сложной системы. Качество

постановки проблемы во многом определяет успешность дальнейших этапов исследования и разработки.

Постановка сложной проблемы включает не только формулировку задачи, но и понимание её контекста, ограничений, целей и взаимосвязей с внешней средой. В отличие от простых задач, сложные проблемы характеризуются множественностью факторов, неопределённостью, наличием противоречивых требований и большим числом заинтересованных сторон.

Основные этапы постановки проблемы:

1. **Идентификация проблемы.** На этом этапе необходимо выделить и зафиксировать существующую проблему, её проявления и причины. Важно отделить симптомы от корневых причин.
2. **Анализ проблемной ситуации.** Изучение окружающей среды, факторов, влияющих на проблему, и взаимосвязей между элементами системы и внешними объектами.
3. **Определение границ проблемы.** Чёткое выделение сферы действия проблемы, ограничение поля исследования для повышения управляемости и фокусировки усилий.
4. **Формулирование цели и задач исследования.** Определение желаемых результатов и критериев успешного решения проблемы.
5. **Выработка критериев и характеристик проблемы.** Определение параметров, по которым будет оцениваться степень её разрешения или усугубления.
6. **Выявление заинтересованных сторон и их позиций.** Определение влияния разных участников и их требований к результату.
7. **Документирование постановки проблемы.** Формализация постановки в виде отчёта, технического задания или иного документа.

Сложные проблемы зачастую обладают следующими характеристиками: высокая степень неопределённости, противоречивость требований, множественность вариантов решения, динамичность условий и наличие рисков. Для успешной постановки важно использовать методы системного анализа, моделирования, а также коллективного обсуждения с участием экспертов.

Постановка проблемы связана с выявлением ключевых факторов, влияющих на ситуацию, и построением моделей, которые отражают причинно-следственные связи. Для этого применяются методы причинно-следственного анализа, диаграммы Исикавы, SWOT-анализ, структурные и функциональные схемы.

Чёткая и полноформатная постановка позволяет избежать недоразумений в ходе проектирования и оптимизирует использование ресурсов. Ошибки на

этом этапе ведут к неправильной ориентации проекта и могут стать причиной провалов и перерасходов.

Системный подход требует комплексного и многоуровневого рассмотрения проблемы, с привлечением различных специалистов и учётом мнений всех заинтересованных сторон.

Задания

1. Проанализируйте выбранную вами сложную проблему (техническую, экономическую, социальную или организационную) и опишите её основные проявления и причины.
2. Проведите анализ проблемной ситуации с выделением ключевых факторов, влияющих на проблему.
3. Определите и обоснуйте границы проблемы, указав, какие аспекты включены, а какие исключены из рассмотрения.
4. Сформулируйте цель исследования и основные задачи, необходимые для её достижения.
5. Определите критерии и характеристики, которые будут использоваться для оценки успешности решения проблемы.
6. Составьте перечень заинтересованных сторон и опишите их интересы и требования к результату.
7. Разработайте причинно-следственную диаграмму (например, диаграмму Исикавы), отражающую основные факторы проблемы.
8. Оформите постановку проблемы в виде краткого документа, включающего все ключевые элементы.
9. Обсудите возможные риски и неопределённости, связанные с постановкой проблемы, и предложите способы их минимизации.

Таблица: Критерии оценки постановки сложной проблемы

Критерий	Описание	Оценка (от 1 до 5)	Примечания
Чёткость формулировки	Насколько ясно и однозначно сформулирована проблема		
Полнота описания	Учитываются ли все важные аспекты и факторы		
Определённость границ	Насколько точно определены границы и область применения		
Соответствие целей	Цели исследования логично вытекают из поставленной проблемы		

Учёт заинтересованных сторон	Насколько полно идентифицированы и учтены интересы всех участников		
Уровень анализа причин	Насколько глубоко проведён причинно-следственный анализ		
Реалистичность и выполнимость	Насколько постановка проблемы соответствует возможностям и ресурсам проекта		

Данная Лабораторная работа позволяет студентам понять сложность и многоаспектность постановки проблем в системных исследованиях. Освоение порядка и содержания постановки проблемы способствует развитию аналитического мышления и навыков комплексного подхода к решению сложных задач проектирования. Это критически важно для успешного управления проектами и разработки эффективных систем.

Лабораторная работа 6. Этапы решения сложной проблемы

Цель работы: ознакомиться с ключевыми этапами процесса решения сложных проблем в системном подходе, изучить методы и инструменты, применяемые на каждом из этапов, а также развить умение планировать и проводить системные исследования.

Теоретическая часть

Решение сложной проблемы в рамках системного подхода — это комплексный процесс, который требует последовательного и структурированного выполнения ряда этапов. Каждый этап направлен на более глубокое понимание проблемы, формирование адекватных моделей, разработку и реализацию оптимальных решений.

Основные этапы решения сложной проблемы включают:

1. **Постановка и формализация проблемы.** На этом этапе происходит точное определение проблемы, установление её границ и целей, а также выявление заинтересованных сторон. Формализация включает создание моделей и описание исходных условий задачи.
2. **Анализ и моделирование проблемы.** Проводится детальный анализ факторов, влияющих на проблему, выявляются взаимосвязи между элементами системы. Создаются модели (математические, логические, графические), которые помогают визуализировать и исследовать проблему.

3. **Разработка вариантов решения.** На основе моделей генерируются возможные варианты решения, которые учитывают ограничения и цели. Каждый вариант оценивается с точки зрения эффективности, рисков, затрат и других критериев.
4. **Выбор оптимального решения.** Сравнение и отбор наиболее подходящего варианта решения с использованием методов многокритериального анализа, экспертных оценок, анализа чувствительности и др.
5. **Реализация решения.** Внедрение выбранного варианта на практике с учётом организационных, технических и экономических аспектов. На этом этапе важна координация действий всех участников.
6. **Мониторинг и контроль.** Осуществляется наблюдение за ходом реализации решения, оценка результатов, выявление отклонений от планируемых показателей и принятие корректирующих мер.
7. **Анализ результатов и обратная связь.** По завершении реализации проводится анализ достигнутых результатов, сопоставление их с первоначальными целями и задачами. Обратная связь позволяет корректировать дальнейшие действия и улучшать процессы решения проблем.

Данный процесс не всегда является линейным — на практике возможны возвраты к предыдущим этапам для уточнения постановки или корректировки модели. Решение сложных проблем требует итеративного подхода и гибкости.

Особое внимание уделяется междисциплинарности, вовлечению экспертов из различных областей, а также учёту социальных, экономических и технических факторов, влияющих на проблему.

Методы, используемые на различных этапах, включают: системный анализ, методы оптимизации, моделирование, методы принятия решений, экспертные оценки, SWOT-анализ, анализ рисков и др. Знание этих инструментов позволяет повысить качество и обоснованность решений.

Важной частью этапов решения является эффективное управление информацией, коммуникациями и ресурсами, что требует координации и планирования.

Освоение этапов решения сложных проблем способствует развитию навыков комплексного мышления, критического анализа и способности работать в условиях неопределённости.

Вопросы и задания

1. Опишите основные этапы решения сложной проблемы и их последовательность.

2. Почему важно формализовать проблему на ранних этапах?
3. Какие методы моделирования могут быть применены для анализа сложных проблем?
4. Как оценивать и сравнивать варианты решений?
5. Какие трудности могут возникнуть на этапе реализации решения?
6. Почему необходим мониторинг и контроль результатов?
7. Как итеративный характер процесса решения помогает повысить качество результата?
8. Какие методы принятия решений вы знаете и как они применяются в системном подходе?
9. Опишите роль заинтересованных сторон на различных этапах решения проблемы.
10. В чем заключается значимость обратной связи и анализа результатов?

Задания

Задание 1. Выберите реальную или гипотетическую сложную проблему из своей профессиональной области и сформулируйте её постановку.

Задание 2. Выполните анализ выбранной проблемы, выделите ключевые факторы и создайте модель, иллюстрирующую взаимосвязи.

Задание 3. Сгенерируйте не менее трёх вариантов решения проблемы, опишите их основные характеристики и предположительные риски.

Задание 4. Проведите сравнительный анализ вариантов с использованием таблицы критериев (эффективность, затраты, риски, время реализации).

Задание 5. Опишите план реализации выбранного варианта, включая этапы, ресурсы и контрольные точки.

Задание 6. Разработайте систему мониторинга для оценки хода реализации и достижения целей.

Задание 7. Составьте отчёт по результатам проведённой работы с выводами и рекомендациями.

Таблица: Пример сравнительного анализа вариантов решения сложной проблемы

Критерий	Вариант 1	Вариант 2	Вариант 3	Примечания
Эффективность	Высокая	Средняя	Высокая	Оценка на основе экспертных данных
Затраты	Средние	Низкие	Высокие	Включая финансовые и временные

Риски	Средние	Низкие	Высокие	Вероятность возникновения проблем
Время реализации	Краткосрочный (3 мес.)	Среднесрочный (6 мес.)	Долгосрочный (1 год)	
Соответствие целям	Полное	Частичное	Полное	Насколько вариант отвечает целям

Данная Лабораторная работа направлена на развитие у студентов системного и комплексного подхода к решению сложных задач, обучает методам анализа, генерации и оценки вариантов, а также формированию планов реализации и контролю исполнения. Это создает базу для эффективной профессиональной деятельности в области проектирования и управления сложными системами.

Лабораторная работа 7. Стадии разработки системы защиты АСУ. Метод OpSec

Цель работы: изучить основные стадии разработки системы защиты автоматизированных систем управления (АСУ), освоить принципы и методы информационной безопасности, а также подробно ознакомиться с методикой OpSec (Operational Security) и её применением на практике.

Теоретическая часть

Автоматизированные системы управления (АСУ) — это сложные комплексные системы, предназначенные для управления технологическими процессами, производством, объектами инфраструктуры и другими критически важными сферами. Надёжная защита АСУ от различных угроз и атак является одной из ключевых задач обеспечения безопасности объектов.

Разработка системы защиты АСУ представляет собой многопроцессный и многоуровневый процесс, включающий следующие основные стадии:

1. **Анализ угроз и уязвимостей.** На этом этапе проводится всесторонний анализ возможных источников угроз, уязвимых точек системы, а также потенциальных воздействий на работоспособность и конфиденциальность информации. Включает сбор информации, оценку рисков, идентификацию критически важных компонентов.
2. **Определение требований к безопасности.** Формируются конкретные требования к системе защиты, исходя из результатов анализа угроз, нормативных документов, стандартов и специфики объекта управления.

3. **Разработка архитектуры системы защиты.** Создается концепция и архитектура системы безопасности, включающая выбор технических и программных средств, распределение зон ответственности и уровней доступа, схемы шифрования и контроля.
4. **Проектирование и внедрение средств защиты.** На данном этапе реализуются конкретные технические решения — установка межсетевых экранов, систем обнаружения вторжений, средств контроля доступа, шифрования данных и прочих компонентов.
5. **Тестирование и оценка эффективности защиты.** Проводятся комплексные проверки, включая моделирование атак, тесты на проникновение, оценку устойчивости системы и соответствия требованиям.
6. **Эксплуатация и мониторинг.** Включает постоянное наблюдение за состоянием системы, обновление средств защиты, реакцию на инциденты и поддержание политики безопасности.
7. **Анализ и совершенствование.** На основе полученного опыта и меняющихся условий разрабатываются рекомендации и планы по улучшению защиты.

Метод OpSec (Operational Security) — это комплексный подход, направленный на выявление и минимизацию рисков, связанных с утечкой критически важной информации. Основная идея OpSec заключается в том, что защита должна охватывать не только технические средства, но и процессы, поведение людей, организационные меры.

Ключевые этапы метода OpSec:

- **Идентификация критически важной информации.** Определение данных, раскрытие которых может нанести ущерб.
- **Анализ угроз и рисков.** Выявление, кто может быть заинтересован в получении информации и какими способами.
- **Определение уязвимостей.** Анализ мест и способов возможной утечки информации.
- **Разработка и внедрение мер защиты.** Технические, организационные и административные меры для минимизации рисков.
- **Постоянный контроль и обучение персонала.** Обеспечение осведомлённости сотрудников и поддержание дисциплины.

Метод OpSec является неотъемлемой частью комплексной системы безопасности АСУ, особенно в условиях современных киберугроз и сложных атак.

Вопросы и задания

1. Какие основные стадии разработки системы защиты АСУ можно выделить?

2. Почему важен анализ угроз и уязвимостей на ранних этапах проектирования?
3. Что включает в себя определение требований к безопасности?
4. Опишите основные компоненты архитектуры системы защиты АСУ.
5. В чем заключается роль тестирования и оценки эффективности системы защиты?
6. Как обеспечивается эксплуатация и мониторинг системы безопасности?
7. Что представляет собой метод OpSec и какие задачи он решает?
8. Какие этапы включает метод OpSec?
9. Почему важна организационная составляющая в обеспечении информационной безопасности?
10. Как можно снизить риски утечки информации с помощью метода OpSec?

Задания

Задание 1. Проанализируйте выбранную автоматизированную систему (реальную или условную), определите возможные угрозы и уязвимости.

Задание 2. Сформулируйте требования к безопасности для данной системы, учитывая выявленные угрозы.

Задание 3. Разработайте архитектуру системы защиты, включающую основные компоненты и уровни защиты.

Задание 4. Опишите план тестирования и оценки эффективности внедрённой защиты.

Задание 5. Разработайте мероприятия по эксплуатации и мониторингу безопасности системы.

Задание 6. Проанализируйте критически важную информацию в рамках выбранной системы и примените метод OpSec для снижения рисков её утечки.

Задание 7. Составьте краткую инструкцию по обучению сотрудников по вопросам OpSec.

Таблица: Пример классификации угроз для АСУ

Тип угрозы	Описание	Возможное воздействие	Меры защиты
Внешние атаки	Хакерские взломы, вирусы, DDoS	Нарушение работы, утечка данных	Межсетевые экраны, антивирусы
Внутренние угрозы	Ошибки персонала, злонамеренные действия	Нарушение целостности, доступ к конфиденциальным данным	Контроль доступа, обучение

Технические сбои	Отказы оборудования, программных средств	Простой системы, потеря данных	Резервирование, отказоустойчивость
Физические угрозы	Пожары, затопления, несанкционированный доступ к оборудованию	Физическое повреждение, кража оборудования	Контроль доступа, пожарная безопасность

Данная Лабораторная работа направлена на формирование системного понимания этапов разработки защиты АСУ и освоение методики OpSec, которая усиливает безопасность за счёт комплексного анализа и минимизации рисков утечки критически важной информации. Это позволит студентам применять полученные знания для защиты сложных автоматизированных систем в профессиональной деятельности.

Лабораторная работа 8. Методология построения системы информационной безопасности АСУ: концептуальная модель

Цель работы: изучить методологию проектирования системы информационной безопасности (СИБ) автоматизированных систем управления (АСУ), понять роль концептуальной модели в обеспечении защиты, сформировать представление о её структуре, этапах разработки и применении на практике.

Теоретическая часть

Информационная безопасность автоматизированных систем управления — это совокупность организационных, технических и программных мер, направленных на защиту информации и поддержание устойчивого функционирования системы. Сложность и критическая важность АСУ требуют строго структурированного и научно обоснованного подхода к проектированию защиты, где ключевым элементом становится построение концептуальной модели системы информационной безопасности.

Концептуальная модель представляет собой обобщённое, логически непротиворечивое описание архитектуры и принципов функционирования системы защиты информации в АСУ. Она используется как теоретическая основа для дальнейшего проектирования, реализации и тестирования компонентов СИБ.

Основные компоненты концептуальной модели СИБ АСУ:

1. **Объекты защиты.** Данные, каналы передачи, программное обеспечение, устройства управления и хранения, персонал.
2. **Актуальные угрозы.** Внешние и внутренние угрозы, в том числе кибератаки, несанкционированный доступ, вредоносное ПО, ошибки персонала, сбои оборудования.
3. **Уязвимости.** Технические и организационные недостатки, через которые угрозы могут реализоваться.
4. **Механизмы защиты.** Технические средства (антивирусы, межсетевые экраны, системы обнаружения атак), организационные меры (политики безопасности, инструкции), криптографическая защита, разграничение доступа.
5. **Цели и задачи СИБ.** Конфиденциальность, целостность, доступность информации и стабильность функционирования АСУ.
6. **Принципы построения СИБ.** Системность, комплексность, многоуровневость, непрерывность, соответствие нормативным требованиям.

Этапы построения концептуальной модели:

1. **Анализ защищаемой системы.** Изучение структуры АСУ, определение критически важных элементов.
2. **Идентификация угроз и уязвимостей.** Построение модели угроз, выявление потенциальных сценариев атак.
3. **Определение целей и критериев безопасности.** Постановка задач, выработка показателей оценки защищённости.
4. **Формирование принципов и подходов к защите.** Определение базовых методологических основ (например, модель доверия, зона ответственности, зоны безопасности).
5. **Проектирование архитектуры СИБ.** Распределение мер защиты по уровням системы: физический, сетевой, программный, прикладной и административный.
6. **Документирование модели.** Формализация концепции в виде документа с графическими схемами, описанием механизмов защиты и организационной структуры.

Пример уровневой архитектуры концептуальной модели СИБ:

Уровень системы	Меры защиты
Физический	Контроль доступа в помещения, видеонаблюдение, замки
Сетевой	Межсетевые экраны, VPN, система обнаружения вторжений
Системный	Контроль учётных записей, антивирусная защита, патч-менеджмент

Прикладной	Контроль прав доступа, шифрование данных, аудит действий
Административный	Политики безопасности, инструкции, обучение персонала

Роль концептуальной модели в СИБ:

Концептуальная модель позволяет структурировать подход к защите, выявить слабые места ещё на ранней стадии проектирования, обеспечить согласованность всех элементов защиты, минимизировать вероятность уязвимостей и повысить устойчивость системы к внешним и внутренним воздействиям.

Такая модель также служит основой для стандартизации и обеспечения соответствия системы требованиям национальных и международных регуляторов.

Задания

Задание 1. Выберите условную или реальную АСУ (например, система управления производственным процессом) и составьте перечень объектов защиты.

Задание 2. Определите актуальные угрозы и уязвимости в выбранной системе.

Задание 3. Сформулируйте цели и задачи системы информационной безопасности.

Задание 4. Определите принципы построения концептуальной модели.

Задание 5. Разработайте уровневую структуру архитектуры защиты с кратким описанием механизмов на каждом уровне.

Задание 6. Нарисуйте схему концептуальной модели СИБ для выбранной системы.

Задание 7. Подготовьте документ (в текстовой форме), содержащий полное описание концептуальной модели, включая анализ, цели, методы защиты и архитектурные решения.

Вопросы и задания

1. Что такое концептуальная модель СИБ и какова её роль при проектировании защиты АСУ?
2. Какие компоненты включает в себя концептуальная модель?
3. Опишите этапы её построения.
4. Какие угрозы и уязвимости необходимо учитывать при разработке защиты?
5. Почему важно структурировать архитектуру защиты по уровням?
6. Какие принципы следует соблюдать при формировании модели?

7. Как концептуальная модель помогает в обеспечении соответствия нормативным требованиям?
8. Чем отличается архитектурная модель СИБ от концептуальной?
9. Какие ошибки чаще всего допускаются при проектировании концептуальной модели?
10. Как документируется и используется модель на практике?

Вывод:

Построение концептуальной модели системы информационной безопасности АСУ является ключевым этапом в обеспечении защиты сложных информационно-технологических систем. Освоение методологии проектирования таких моделей позволяет эффективно систематизировать знания о потенциальных угрозах, спроектировать устойчивую архитектуру и применить лучшие практики в области защиты информации.

Лабораторная работа 9. Методология построения системы информационной безопасности АСУ: этапы построения системы информационной безопасности

Цель работы: изучить последовательность этапов построения системы информационной безопасности автоматизированной системы управления (АСУ), освоить методы анализа, проектирования и внедрения защиты информации, получить представление о жизненном цикле СИБ и критериях её эффективности.

Теоретическая часть

Автоматизированные системы управления (АСУ) представляют собой критически важные элементы информационной инфраструктуры, особенно в сферах промышленности, энергетики, транспорта и связи. Надёжная защита информации в АСУ необходима для предотвращения сбоев, утечек данных и несанкционированного вмешательства, которые могут привести к тяжёлым последствиям. Методология построения системы информационной безопасности (СИБ) в таких системах опирается на комплексный, поэтапный подход.

Основные этапы построения СИБ:

1. Анализ объекта защиты.

На данном этапе проводится исследование архитектуры АСУ: её компонентов, функций, процессов и информационных потоков. Определяются критически важные элементы, которые подлежат защите. Оцениваются существующие меры безопасности и их эффективность.

2. Идентификация угроз и уязвимостей.

Разрабатывается модель угроз, включающая внутренние, внешние,

случайные и преднамеренные воздействия. Анализируются слабые места системы — аппаратные, программные и организационные. На основе этого формируются сценарии возможных атак.

3. Формирование требований к информационной безопасности.

Определяются цели и задачи СИБ: обеспечение конфиденциальности, целостности, доступности, а также правомерности обработки информации. Разрабатываются нормативно-правовые и организационные требования, которым должна соответствовать система защиты.

4. Проектирование архитектуры СИБ.

На этом этапе создаётся структура системы безопасности с распределением мер по уровням: физический, сетевой, системный, прикладной и административный. Разрабатываются регламенты, механизмы разграничения доступа, политики безопасности, процедуры реагирования на инциденты.

5. Реализация технических и организационных решений.

Осуществляется внедрение проектных решений: установка оборудования, программного обеспечения, настройка сетей, реализация политик доступа, обучение персонала. Также формируется система мониторинга и контроля.

6. Тестирование и аудит.

Проводятся тесты защищённости, стресс-тесты, имитация вторжений. Проверяется соответствие системы требованиям и стандартам, оценивается степень устойчивости к угрозам. При необходимости выполняется корректировка решений.

7. Эксплуатация и сопровождение.

Система вводится в действие. Организуется постоянный мониторинг, обновление компонентов защиты, реагирование на инциденты, анализ журналов событий, регулярное обучение сотрудников.

8. Модернизация.

С учётом изменений в архитектуре АСУ, появления новых угроз, развития технологий осуществляется адаптация системы информационной безопасности, обновление её архитектуры и средств защиты.

Диаграмма жизненного цикла СИБ АСУ:

Этап	Основное содержание
Анализ объекта	Изучение архитектуры, компонентов, потоков данных
Модель угроз	Выявление уязвимостей, построение сценариев атак
Требования	Постановка целей защиты, нормативные критерии
Проектирование	Архитектура, политики, процедуры, разграничение доступа
Реализация	Внедрение мер защиты, обучение

Тестирование	Аудит, проверка соответствия, корректировка
Эксплуатация	Мониторинг, сопровождение, реагирование на инциденты
Модернизация	Обновление, адаптация к изменениям и угрозам

Особенности построения СИБ в АСУ:

АСУ обладают специфическими особенностями: наличие физических процессов, реального времени, специфических протоколов и ограниченных ресурсов. Поэтому защита должна учитывать совместимость с производственными системами, минимальное влияние на их функционирование и устойчивость к отказам. Часто применяются сегментация сети, изоляция критичных узлов, специальные шлюзы и сертифицированные средства защиты.

Задания

Задание 1. Выберите типовую АСУ (например, АСУ ТП на заводе, система управления распределением электроэнергии). Проведите краткий анализ её архитектуры.

Задание 2. Постройте модель угроз для данной системы. Определите уязвимости.

Задание 3. Сформулируйте требования к СИБ на основе целей и нормативных документов (например, ГОСТ Р 57580, ISO/IEC 27001).

Задание 4. Разработайте схему архитектуры СИБ с указанием уровней защиты.

Задание 5. Составьте план реализации СИБ: какие средства защиты устанавливаются, какие организационные меры принимаются.

Задание 6. Опишите процедуры тестирования и мониторинга системы.

Задание 7. Приведите примеры ситуаций, требующих модернизации СИБ.

Вопросы и задания

1. Перечислите и кратко охарактеризуйте этапы построения системы информационной безопасности АСУ.
2. В чём заключается важность анализа объекта защиты?
3. Как осуществляется идентификация угроз и уязвимостей?
4. Какие требования к СИБ обычно выдвигаются в рамках нормативного регулирования?
5. Какие меры реализуются на разных уровнях архитектуры СИБ?
6. Чем отличается внедрение технических средств от организационных мер?
7. В чём суть этапа тестирования? Какие инструменты при этом используются?
8. Как осуществляется сопровождение СИБ в условиях эксплуатации?

9. Когда и почему требуется модернизация системы защиты?
10. Какие особенности СИБ связаны со спецификой АСУ?

Вывод:

Построение системы информационной безопасности в АСУ — это многоэтапный процесс, требующий комплексного подхода, глубокого анализа и учёта особенностей управляемых процессов. Каждый этап, от анализа архитектуры до модернизации, играет ключевую роль в формировании надёжной, устойчивой и гибкой системы защиты. Владение методологией проектирования СИБ позволяет создавать устойчивые к угрозам системы, обеспечивающие непрерывность и безопасность производственных и информационных процессов.

Лабораторная работа 10. Методология построения системы информационной безопасности АСУ: анализ этапов построения системы информационной безопасности

Цель работы: подробно изучить каждый из этапов построения системы информационной безопасности (СИБ) в автоматизированной системе управления (АСУ), выявить взаимосвязь этапов и проанализировать характер применяемых решений на разных стадиях жизненного цикла СИБ.

Теоретическая часть

Построение системы информационной безопасности в АСУ — это не разовая задача, а непрерывный процесс, который охватывает все стадии жизненного цикла системы. Его можно представить как последовательность логически связанных этапов, каждый из которых обеспечивает основу для перехода к следующему. Пропуск или упрощение любого этапа может привести к ослаблению всей системы защиты, поскольку надёжность СИБ определяется слабыми звеньями в её структуре.

Анализ этапов построения СИБ включает изучение задач, методов и результатов, характерных для каждого шага. Рассмотрим более подробно основные этапы, их внутреннюю структуру и взаимосвязи.

Этап 1. Исследование объекта защиты

Цель — получить целостное представление об автоматизированной системе, включая её архитектуру, состав компонентов, структуру информационных потоков и взаимодействие с внешними системами. Важно понять, какие элементы критичны с точки зрения безопасности и какова степень их уязвимости.

Этап 2. Построение модели угроз и уязвимостей

На этом этапе проводится комплексная оценка потенциальных источников угроз: случайных и преднамеренных, внешних и внутренних. Для каждой

угрозы выявляются возможные точки приложения, оцениваются вероятности реализации, а также последствия. Используются такие инструменты, как SWOT-анализ, STRIDE, DREAD, атака по дереву.

Этап 3. Формирование требований к СИБ

Формулируются требования к защищаемой системе на основе анализа угроз, уязвимостей и действующих нормативных документов (ГОСТ Р ИСО/МЭК 27001, 57580 и др.). Требования подразделяются на функциональные (например, обеспечение аутентификации) и нефункциональные (например, устойчивость к отказам).

Этап 4. Проектирование архитектуры СИБ

Разрабатывается многослойная структура системы защиты, охватывающая физические, сетевые, системные и организационные уровни. Проектирование опирается на принципы минимизации доверия, сегментации сетей, отказоустойчивости, принципов нулевого доверия (Zero Trust).

Этап 5. Внедрение и реализация технических и административных решений

На этом этапе происходит развёртывание средств защиты: межсетевых экранов, систем обнаружения вторжений, средств шифрования, контроля доступа. Также формируются административные меры: обучение персонала, назначение ответственных, регламентация действий при инцидентах.

Этап 6. Оценка эффективности и тестирование СИБ

Включает проведение тестов на проникновение (penetration testing), аудитов безопасности, стресс-тестов. Проводится анализ соответствия системы установленным требованиям, выявляются недоработки и определяются пути их устранения.

Этап 7. Эксплуатация и сопровождение СИБ

Организуется постоянный мониторинг состояния информационной безопасности, обновление сигнатур, выявление инцидентов, анализ логов, ведение отчётности. Назначаются ответственные за сопровождение и аудит системы.

Этап 8. Обновление и адаптация

По мере появления новых угроз, изменений в законодательстве или расширения системы происходит её модернизация. Обновляются политики безопасности, программное обеспечение, усиливаются меры защиты.

Связи между этапами:

Этапы построения СИБ не являются строго линейными — между ними возможны обратные переходы. Например, по результатам тестирования может потребоваться возврат к этапу проектирования, а при изменении объекта защиты — к первичному анализу архитектуры.

Итоговая схема анализа этапов:

Этап	Цель	Основные действия	Результат
Исследование объекта	Получение полной картины системы	Анализ архитектуры, потоков, компонентов	Карта объекта защиты
Модель угроз	Оценка рисков	Определение уязвимостей, угроз, вероятностей	Модель угроз
Требования	Формирование критериев СИБ	Анализ рисков и нормативных требований	Список требований
Проектирование	Формирование структуры СИБ	Разработка архитектуры защиты	Проект СИБ
Внедрение	Реализация защиты	Установка ПО, обучение, регламенты	Рабочая СИБ
Тестирование	Проверка эффективности	Аудит, тесты, анализ логов	Отчёт об уязвимостях
Эксплуатация	Поддержание функционирования	Мониторинг, анализ, реагирование	Поддерживаемая система
Обновление	Адаптация к изменениям	Модернизация, доработка	Современная СИБ

Задания

Задание 1. Составьте подробную блок-схему этапов построения СИБ, указывая ключевые задачи и промежуточные результаты на каждом этапе.

Задание 2. Выберите один из этапов (например, анализ угроз) и разработайте пример его реализации для конкретной АСУ (например, энергосистема).

Задание 3. Разработайте перечень функциональных требований к системе защиты для условного объекта (например, автоматизированная система видеонаблюдения в промышленности).

Задание 4. Оцените преимущества и недостатки линейной и итеративной моделей построения СИБ.

Задание 5. На основе приведённой теории, предложите алгоритм реагирования на выявленные недостатки в ходе эксплуатации.

Вопросы и задания

1. Какова основная цель каждого из этапов построения СИБ?
2. Почему важен этап анализа объекта защиты?
3. В чём разница между формулировкой требований и проектированием архитектуры?
4. Какие методы используются для моделирования угроз?
5. В чём заключается важность постоянного сопровождения системы?
6. Почему этап обновления нельзя исключить из жизненного цикла СИБ?
7. Какие инструменты применяются на стадии тестирования?
8. Какие угрозы могут возникнуть при несоблюдении этапности построения СИБ?
9. Приведите примеры межэтапных связей и их влияния на эффективность системы.
10. Как обеспечить гибкость и масштабируемость построенной системы защиты?

Вывод:

Эффективное построение системы информационной безопасности в АСУ невозможно без чёткого понимания содержания каждого этапа и взаимосвязей между ними. Последовательный анализ позволяет избежать дублирования решений, своевременно выявлять уязвимости и выстраивать структуру защиты, способную адаптироваться к меняющимся условиям. Практическое владение методологией построения СИБ является основой профессиональной подготовки специалистов в области защиты информации и информационных технологий.

Лабораторная работа 11. Принципы, понятия политики и уровней безопасности. Задачи этапа предпроектного обследования

Цель работы: изучить фундаментальные принципы обеспечения информационной безопасности (ИБ), понятия политики и уровней защиты информации, а также рассмотреть ключевые задачи, решаемые в рамках этапа предпроектного обследования автоматизированной системы (АС).

Теоретическая часть

Построение эффективной системы информационной безопасности невозможно без предварительного понимания концептуальных основ защиты информации, а также без качественно проведённого этапа предпроектного обследования. Этот этап закладывает фундамент для разработки архитектуры ИБ и позволяет определить фактическое состояние защищённости.

Принципы информационной безопасности

Система информационной безопасности строится на ряде базовых принципов, среди которых особое значение имеют:

Принцип целостности — защита информации от несанкционированных изменений.

Принцип конфиденциальности — ограничение доступа к информации исключительно уполномоченным лицам.

Принцип доступности — обеспечение доступа к информации и ресурсам для легитимных пользователей в требуемое время.

Принцип аутентичности — подтверждение подлинности источника информации или пользователя.

Принцип контролируемости — возможность мониторинга, регистрации и анализа действий, происходящих в системе.

Политика информационной безопасности

Политика безопасности — это свод официальных внутренних правил и регламентов, определяющих подходы к защите информации в организации. Она устанавливает цели безопасности, допустимый уровень риска, обязанности пользователей, права администраторов, механизмы доступа и правила реагирования на инциденты. Политика должна быть адаптивной, учитывать текущие угрозы, а также подлежать регулярному пересмотру.

Различают **глобальную политику безопасности** (в масштабах всей организации) и **локальные политики** (на уровне отдельных подразделений или ИТ-средств). Также часто выделяют технические, организационные и административные политики.

Уровни обеспечения безопасности

Выделяют несколько уровней ИБ:

Физический уровень — защита оборудования и каналов связи (замки, охрана, экранирование).

Технический уровень — защита программного и аппаратного обеспечения (антивирусы, межсетевые экраны).

Сетевой уровень — защита данных в передаче (шифрование, VPN, контроль трафика).

Прикладной уровень — обеспечение безопасности на уровне приложений (аутентификация, логирование, права доступа).

Организационный уровень — административные меры, регламенты, политика ИБ, ответственность сотрудников.

Понимание и реализация принципов защиты на каждом уровне позволяют построить многослойную модель безопасности, известную как **Defense in Depth** — «глубокоэшелонированная защита».

Предпроектное обследование

Этап предпроектного обследования выполняется до начала непосредственного проектирования системы ИБ. Его цель — получить объективное представление о текущем состоянии системы, выявить слабые места и сформулировать исходные данные для будущей архитектуры защиты.

Ключевые задачи этапа предпроектного обследования:

1. **Анализ архитектуры и структуры АС**
Изучаются технические средства, логическая структура системы, топология сети, маршрутизация, межсетевые взаимодействия и используемые протоколы.
2. **Аудит действующих средств защиты**
Оценивается наличие и состояние уже реализованных средств ИБ: систем аутентификации, антивирусов, межсетевых экранов, систем обнаружения вторжений.
3. **Оценка уязвимостей и потенциальных угроз**
Проводится анализ рисков, моделируются возможные сценарии атак, рассматриваются типовые угрозы с учётом специфики отрасли.
4. **Интервьюирование персонала**
Уточняется уровень подготовки сотрудников, их осведомлённость в вопросах ИБ, понимание процедур реагирования на инциденты.
5. **Сбор нормативной и организационной документации**
Изучаются внутренние регламенты, положения, стандарты, ранее утверждённые политики ИБ и инструкции.
6. **Подготовка аналитического отчёта**
По итогам обследования формируется отчёт, содержащий выводы об уровне защищённости, рекомендации по улучшению и перечень проблемных зон.

Задания

Задание 1. Составьте иерархию уровней информационной безопасности с кратким описанием применяемых на каждом уровне средств и мер.

Задание 2. Разработайте проект фрагмента политики ИБ для организации среднего масштаба, содержащий цели, принципы и ключевые положения.

Задание 3. На основе гипотетической архитектуры ИТ-системы предприятия составьте перечень задач, которые необходимо решить в ходе предпроектного обследования.

Задание 4. Разработайте шаблон опросника для интервью с сотрудниками

предприятия, направленного на выявление угроз внутреннего характера.

Задание 5. Проведите сравнение двух подходов: реализации политики безопасности на физическом уровне и на прикладном уровне. Определите преимущества и ограничения каждого.

Вопросы и задания

1. Что понимается под принципом «многослойной защиты» в ИБ?
2. Каковы основные отличия глобальной политики ИБ от локальных политик?
3. Почему этап предпроектного обследования критичен для всей системы защиты?
4. Как классифицируются уровни ИБ и какие задачи они решают?
5. Какие методы используются для оценки текущего состояния защищённости?
6. В чём заключается цель политики безопасности и кто несёт ответственность за её соблюдение?
7. Какие уязвимости могут быть выявлены в ходе интервьюирования персонала?
8. Каковы особенности составления отчёта по итогам предпроектного обследования?
9. Приведите примеры реальных угроз, которые можно выявить только на стадии обследования.
10. Какие документы следует запросить у заказчика при проведении анализа существующей системы?

Вывод

Формирование устойчивой и функциональной системы информационной безопасности невозможно без глубокого понимания принципов защиты, грамотной разработки политики ИБ и комплексного обследования существующей ИТ-инфраструктуры. Предпроектное обследование играет ключевую роль в этом процессе, позволяя на начальном этапе выявить проблемы и на их основе построить эффективную модель защиты. Успешное выполнение заданий по данной теме формирует у студентов навыки аналитической работы и закладывает основы для профессиональной деятельности в сфере информационной безопасности.

Лабораторная работа 12. Задача этапа анализа и управления рисками

Цель работы: изучить основные цели, этапы и методы анализа и управления рисками в процессе проектирования систем, в том числе систем информационной безопасности, а также приобрести навыки идентификации рисков, оценки их последствий и выбора стратегий управления.

Теоретическая часть

В условиях постоянно возрастающей сложности автоматизированных систем (АС) и расширения спектра потенциальных угроз одной из центральных задач системного подхода становится проведение всестороннего анализа и управления рисками. Это особенно важно при проектировании систем защиты информации, где неверная оценка рисков может привести к серьёзным последствиям, включая утечку данных, потерю управляемости и финансовые убытки.

Понятие риска

Под риском понимается вероятность возникновения события, оказывающего негативное влияние на функционирование системы, сопровождающегося ущербом. В контексте системной инженерии и информационной безопасности под рисками понимаются потенциальные угрозы, способные привести к сбоям, потерям или уязвимостям в системе.

Риск характеризуется двумя основными параметрами:

- **Вероятность события (P)** — насколько часто может произойти угроза.
- **Ущерб (L)** — насколько значительным может быть последствие.

Интегральный риск определяется произведением:

$$R = P \times L$$

Цели этапа анализа рисков

Основная цель анализа и управления рисками заключается в том, чтобы выявить слабые места системы, оценить последствия потенциальных инцидентов и разработать мероприятия, направленные на снижение вероятности наступления негативных событий или минимизацию их последствий. Этот этап обеспечивает обоснованность проектных решений и позволяет определить приоритеты в разработке защитных мер.

Этапы анализа и управления рисками

1. Идентификация рисков

На этом этапе проводится сбор информации о возможных источниках

угроз. Учитываются как внешние, так и внутренние риски. Используются сценарии атак, модели нарушителя, анализ уязвимостей.

2. Оценка рисков

Каждому риску присваивается количественная или качественная оценка на основе вероятности возникновения и ущерба. Применяются методы экспертного оценивания, матрицы рисков, вероятностные и статистические модели.

3. Классификация и ранжирование рисков

Риски группируются по степени критичности и приоритетности. Обычно применяют классификацию: высокие, средние и низкие риски.

4. Выбор стратегии управления рисками

Разрабатываются мероприятия по реагированию. Возможны стратегии:

- снижение риска (внедрение защитных мер),
- уклонение от риска (избежание опасных сценариев),
- передача риска (страхование, аутсорсинг),
- принятие риска (в случае допустимого уровня угрозы).

5. Разработка плана действий

На основании анализа создаётся дорожная карта реализации защитных мер, включающая ресурсы, сроки и ответственных.

6. Мониторинг и пересмотр рисков

Риск-менеджмент не является разовым процессом. Он требует регулярного пересмотра, верификации моделей угроз и адаптации к новым условиям.

Методы анализа рисков

На практике применяются различные методы, включая:

- **FAIR** (Factor Analysis of Information Risk)
- **OCTAVE** (Operationally Critical Threat, Asset, and Vulnerability Evaluation)
- **ISO/IEC 27005** — международный стандарт по управлению ИБ-рисками
- **Метод дерева отказов (FTA)**
- **Метод анализа воздействия (BIA)**
- **SWOT-анализ**
- **Методы матриц вероятности и ущерба**

Пример таблицы оценки рисков:

Идентификатор риска	Описание угрозы	Вероятность	Ущерб	Риск (P×L)	Стратегия управления
R1	Утечка данных через e-mail	Средняя	Высокий	Высокий	Внедрение DLP-системы

R2	Отказ оборудования сервера	Низкая	Высокий	Средний	Резервное копирование
R3	Фишинг сотрудника	Высокая	Средний	Высокий	Обучение персонала
R4	Атака извне через интернет	Средняя	Средний	Средний	МСЭ, IDS/IPS

Задания

Задание 1. На основе предложенной архитектуры организации (локальная сеть, сервер, рабочие станции) выполните идентификацию возможных угроз.

Задание 2. Проведите оценку риска для каждой угрозы по шкале: вероятность (низкая, средняя, высокая), ущерб (низкий, средний, высокий).

Задание 3. Заполните матрицу рисков и разработайте стратегии управления для трёх наиболее критичных рисков.

Задание 4. Используя метод SWOT, оцените сильные и слабые стороны подходов вашей организации к ИБ.

Задание 5. Разработайте план мониторинга и пересмотра рисков с указанием периодичности и ответственных лиц.

Вопросы и задания

1. Что представляет собой риск в контексте информационной безопасности?
2. Какие параметры определяют уровень риска?
3. В чём заключается задача этапа идентификации рисков?
4. Какие существуют методы количественной и качественной оценки рисков?
5. Назовите основные стратегии управления рисками.
6. Что включает в себя процесс мониторинга и пересмотра рисков?
7. Приведите пример ситуации, когда принятие риска является оправданным.
8. Какие стандарты и методики используются при анализе рисков?
9. Почему анализ рисков является неотъемлемой частью предпроектного обследования?
10. Как классифицируются риски по степени приоритетности?

Вывод

Этап анализа и управления рисками является краеугольным камнем в проектировании устойчивых и защищённых систем. Грамотно проведённый анализ позволяет не только выявить критические уязвимости, но и выстроить систему защиты с оптимальным распределением ресурсов. Практическое

освоение методов анализа рисков развивает у студентов системное мышление, формирует навыки оценки угроз и принятия проектных решений, основанных на управлении рисками.