Документ подписан квалифицированной электронной подписью
Сертификат: 03489EA30058B4708C45B74E4D79B70F27
Владелец: "АНО ВО ""РОССИЙСКИЙ НОВЫЙ УНИВЕРСИТЕТ"""
Действителен: с 28.05.2026 по 28.08.2027

АВТОНОМНАЯ НЕКОММЕРЧЕСКАЯ ОРГАНИЗАЦИЯ ВЫСШЕГО ОБРАЗОВАНИЯ «РОССИЙСКИЙ НОВЫЙ УНИВЕРСИТЕТ»
(АНО ВО «РосНОУ»)

Методические рекомендации

по выполнению лабораторных работ
по дисциплине
«Эксплуатация автоматизированных систем в защищенном исполнении»

Специальность: 10.02.05 Информационная безопасность автоматизированных систем

Москва 2026

Оглавление

Введение 4
Лабораторная работа №1 Принципы системного подхода и этапы системных исследований при проектировании сложных систем 5
Лабораторная работа №2 Основные положения системного подхода к проектированию сложных систем 8
Лабораторная работа №3 Положения и задачи системного анализа. Понятие и характеристики проблемы 11
Лабораторная работа №4 Порядок обоснования и выработка требований к проектируемой системе 15
Лабораторная работа №5 Порядок и содержание постановки сложной проблемы 19
Лабораторная работа №6 Этапы решения сложной проблемы 22
Лабораторная работа №7 Стадии разработки системы защиты АСУ. Метод OpSec 25
Лабораторная работа №8 Методология построения системы информационной безопасности АСУ: концептуальная модель 29
Лабораторная работа №9 Методология построения системы информационной безопасности АСУ: этапы построения системы информационной безопасности 32
Лабораторная работа №10 Методология построения системы информационной безопасности АСУ: анализ этапов построения системы информационной безопасности 36
Лабораторная работа №11 Принципы, понятия политики и уровней безопасности. Задачи этапа предпроектного обследования 40
Лабораторная работа №12 Задача этапа анализа и управления рисками 44
Лабораторная работа №13 Методы и средства обеспечения информационной безопасности в АСУ 47
Лабораторная работа №14 Нормативно-правовая база информационной безопасности 51
Лабораторная работа № 15 Архитектура защищённых автоматизированных систем 54
Лабораторная работа №16 *Методы оценки защищённости АСУ* 58
Лабораторная работа №17 Защита АСУ от современных киберугроз 61
Лабораторная работа №18 Обеспечение отказоустойчивости и восстановления АСУ 64
Список литературы 68

Введение

Современные автоматизированные системы (АС) представляют собой сложные программно-аппаратные комплексы, критически важные для функционирования предприятий и организаций. Особое значение приобретает разработка и эксплуатация таких систем в защищенном исполнении, что подразумевает обеспечение их устойчивости к различным видам угроз, включая кибератаки, аппаратные сбои и человеческий фактор.

Ключевой аспект защиты АС - противодействие вредоносному программному обеспечению, которое может нарушать работоспособность систем, похищать конфиденциальные данные или выводить из строя критически важные компоненты. Исторически проблема вредоносного ПО восходит к фундаментальным исследованиям самовоспроизводящихся алгоритмов, однако сегодня она приобрела ярко выраженную практическую значимость.

Особое внимание уделяется комплексному подходу, сочетающему технические, организационные и методические меры защиты, что позволяет создавать автоматизированные системы, соответствующие современным требованиям информационной безопасности.

Курс лабораторных работ состоит из восемнадцати лабораторных работ, списка литературы и оглавления. Предлагаемое учебное пособие предназначено для студентов, обучающихся по специальности: 10.02.05 «Информационная безопасность автоматизированных систем».

Лабораторная работа №1 Принципы системного подхода и этапы системных исследований при проектировании сложных систем

Цель и содержание работы

Целью данной лабораторной работы является изучение принципов системного подхода и этапов системных исследований, применяемых при проектировании сложных технических и информационных систем. В ходе работы рассматриваются основные понятия системного анализа, методы декомпозиции и синтеза систем, а также практические аспекты их применения в инженерии.

Теоретическое обоснование

1. Понятие системы и системного подхода

Система – это совокупность взаимосвязанных элементов, объединенных общей функциональной целью и обладающих свойствами, не сводимыми к простой сумме свойств отдельных компонентов.

Системный подход – это методология исследования сложных объектов, основанная на рассмотрении их как целостных систем с анализом структуры, функций, взаимодействий и динамики развития.

2. Основные принципы системного подхода

1. **Принцип целостности** – система рассматривается как единое целое, а не как набор отдельных частей.
2. **Принцип иерархичности** – система может быть декомпозирована на подсистемы, которые, в свою очередь, также являются системами.
3. **Принцип взаимосвязи** – элементы системы взаимодействуют между собой, что определяет её поведение.
4. **Принцип адаптивности** – система способна изменяться в ответ на внешние воздействия.

5. **Принцип целеполагания** – система создается для достижения определенных целей.

3. Этапы системных исследований

Проектирование сложных систем включает следующие этапы:

1. **Формулирование проблемы**
    - Определение целей и задач системы.
    - Анализ требований и ограничений.
2. **Структурный анализ**
    - Декомпозиция системы на подсистемы и элементы.
    - Построение функциональных и структурных схем.
3. **Функциональное моделирование**
    - Описание поведения системы с помощью математических моделей, алгоритмов и блок-схем.
4. **Синтез системы**
    - Интеграция подсистем в единое целое.
    - Оптимизация структуры и параметров.
5. **Верификация и тестирование**
    - Проверка соответствия системы заданным требованиям.
    - Выявление и устранение ошибок.
6. **Эксплуатация и развитие**
    - Внедрение системы в реальные условия.
    - Модернизация и адаптация к изменяющимся условиям.

4. Применение системного подхода в проектировании сложных систем

Системный подход широко используется в различных областях, включая:

- **Информационные системы** (разработка ПО, архитектура ЭВМ).

- **Автоматизированные системы управления** (АСУ ТП, робототехника).
- **Телекоммуникационные сети** (проектирование сетевой инфраструктуры).

Аппаратура и материалы

1. Персональный компьютер с установленным ПО для моделирования (например, MATLAB, Simulink, AnyLogic).
2. Методические материалы по системному анализу.

Методика и порядок выполнения работы

1. **Изучить теоретические основы системного подхода.**
2. **Выполнить декомпозицию заданной системы на подсистемы.**
3. **Построить структурную схему системы.**
4. **Разработать функциональную модель системы.**
5. **Провести анализ полученных результатов.**

Содержание отчета

Отчет должен включать:

1. **Титульный лист**
2. **Теоретическую часть** (основные понятия системного подхода).
3. **Практическую часть** (результаты декомпозиции, схемы, модели).
4. **Выводы** (анализ проделанной работы, возможные улучшения).

Вопросы для защиты работы

1. Что такое система и каковы её основные свойства?
2. Какие принципы лежат в основе системного подхода?
3. Перечислите этапы системных исследований.
4. Как применяется системный подход в проектировании ЭВМ?
5. В чем заключается процесс декомпозиции системы?
6. Какие методы моделирования используются в системном анализе?

Лабораторная работа №2 Основные положения системного подхода к проектированию сложных систем

Цель и содержание работы

Целью лабораторной работы является изучение фундаментальных принципов системного подхода, применяемых при проектировании сложных технических и информационных систем. В ходе работы рассматриваются методологические основы системного анализа, этапы проектирования, а также практические аспекты их применения в инженерии.

Теоретическое обоснование

1. Понятие системы и системного подхода

Система — это совокупность взаимосвязанных и взаимодействующих элементов, объединенных общей функциональной целью и обладающих свойствами, которые не сводятся к простой сумме характеристик отдельных компонентов.

Системный подход — это методология исследования и проектирования сложных объектов, основанная на их рассмотрении как целостных систем с анализом структуры, функций, взаимосвязей и динамики развития.

2. Основные принципы системного подхода

1. **Принцип целостности** — система рассматривается как единое целое, где свойства системы определяются не только свойствами её элементов, но и связями между ними.
2. **Принцип иерархичности** — система может быть декомпозирована на подсистемы, которые, в свою очередь, также являются системами.
3. **Принцип взаимосвязи** — элементы системы взаимодействуют между собой, что определяет её поведение и функциональность.

4. **Принцип адаптивности** — система способна изменяться и приспосабливаться к изменяющимся внешним условиям.
5. **Принцип целеполагания** — система создается и функционирует для достижения определенных целей.

3. Этапы проектирования сложных систем

Проектирование сложных систем включает следующие этапы:

1. **Формулирование проблемы и постановка целей**
    - Определение назначения системы.
    - Анализ требований и ограничений.
2. **Структурный анализ системы**
    - Декомпозиция системы на подсистемы и элементы.
    - Построение функциональных и структурных схем.
3. **Функциональное моделирование**
    - Разработка математических и алгоритмических моделей системы.
    - Описание поведения системы с помощью блок-схем и диаграмм.
4. **Синтез системы**
    - Интеграция подсистем в единое целое.
    - Оптимизация структуры и параметров системы.
5. **Верификация и тестирование**
    - Проверка соответствия системы заданным требованиям.
    - Выявление и устранение ошибок.
6. **Эксплуатация и развитие**
    - Внедрение системы в реальные условия.
    - Модернизация и адаптация к новым требованиям.

4. Применение системного подхода в проектировании сложных систем

Системный подход широко используется в различных областях, включая:

- **Информационные системы** (разработка программного обеспечения, архитектура ЭВМ).
- **Автоматизированные системы управления** (АСУ ТП, робототехника).
- **Телекоммуникационные сети** (проектирование сетевой инфраструктуры).

Аппаратура и материалы

1. Персональный компьютер с установленным ПО для моделирования (например, MATLAB, Simulink, AnyLogic).
2. Методические материалы по системному анализу.

Методика и порядок выполнения работы

1. **Изучить теоретические основы системного подхода.**
2. **Выполнить декомпозицию заданной системы на подсистемы.**
3. **Построить структурную схему системы.**
4. **Разработать функциональную модель системы.**
5. **Провести анализ полученных результатов.**

Содержание отчета

Отчет должен включать:

1. **Титульный лист**
2. **Теоретическую часть** (основные понятия системного подхода).
3. **Практическую часть** (результаты декомпозиции, схемы, модели).
4. **Выводы** (анализ проделанной работы, возможные улучшения).

Вопросы для защиты работы

1. Что такое система и каковы её основные свойства?
2. Какие принципы лежат в основе системного подхода?
3. Перечислите этапы проектирования сложных систем.

4. Как применяется системный подход в проектировании информационных систем?
5. В чем заключается процесс декомпозиции системы?
6. Какие методы моделирования используются в системном анализе?

Лабораторная работа №3 Положения и задачи системного анализа. Понятие и характеристики проблемы

1. Цель работы

1. Изучить теоретические основы системного анализа как методологии исследования сложных систем.
2. Определить ключевые задачи системного анализа и их практическое применение.
3. Рассмотреть понятие проблемы в системном подходе, изучить ее характеристики и классификацию.
4. Приобрести навыки структуризации проблем и разработки моделей систем.

2. Теоретическая часть

2.1. Основные положения системного анализа

Системный анализ – это междисциплинарная методология, направленная на исследование сложных систем путем их декомпозиции, моделирования и оптимизации.

Основные принципы:

- **Системность** – объект рассматривается как совокупность взаимосвязанных элементов, образующих единое целое.
- **Иерархичность** – система состоит из подсистем, которые, в свою очередь, могут быть разбиты на более мелкие компоненты.

- **Целенаправленность** – система существует для достижения определенных целей.
- **Обратная связь** – процессы в системе регулируются на основе информации о ее состоянии.
- **Адаптивность** – способность системы изменяться под воздействием внешней среды.

Области применения:

- Управление проектами
- Информационные технологии
- Экономика и бизнес-анализ
- Инженерия и проектирование сложных технических систем

2.2. Задачи системного анализа

1. **Идентификация проблемы**
    - Определение границ системы
    - Выявление ключевых факторов влияния
    - Формулировка целей исследования
2. **Структуризация системы**
    - Выделение элементов и подсистем
    - Определение связей между компонентами
    - Построение функциональных и структурных схем
3. **Формализация и моделирование**
    - Математические модели (линейное программирование, теория игр)
    - Имитационное моделирование (AnyLogic, Simulink)
    - Графические модели (IDEF0, UML-диаграммы)
4. **Анализ альтернатив**
    - Генерация возможных решений
    - Оценка вариантов по заданным критериям

- Выбор оптимальной стратегии

5. **Принятие решений и внедрение**
    - Разработка плана реализации
    - Контроль выполнения
    - Корректировка модели при необходимости

2.3. Понятие и характеристики проблемы

Проблема – это несоответствие между текущим и желаемым состоянием системы, требующее решения.

Классификация проблем:

Критерий	**Типы проблем**
Степень структурированности	Структурированные, слабоструктурированные, неструктурированные
Масштаб влияния	Локальные, глобальные
Временной фактор	Статические, динамические
Количество участников	Индивидуальные, групповые, организационные

Характеристики проблем:

- **Сложность** – количество взаимосвязанных факторов
- **Неопределенность** – недостаток данных для принятия решений
- **Динамичность** – изменение параметров во времени
- **Конфликтность** – наличие противоречивых интересов участников

Пример:

Проблема снижения продаж в компании

- **Сложность:** влияние маркетинга, логистики, ценообразования
- **Неопределенность:** колебания спроса на рынке
- **Динамичность:** изменение предпочтений потребителей
- **Конфликтность:** разногласия между отделами продаж и производства

3. Практическая часть

3.1. Аппаратура и материалы

- Компьютер с ПО для моделирования (Excel, AnyLogic, Visio)
- Методические указания
- Примеры кейсов для анализа

3.2. Порядок выполнения

1. **Выбор объекта исследования** (например: "Оптимизация работы call-центра")
2. **Формулировка проблемы**
    - Текущее состояние: длительное время обработки звонков
    - Желаемое состояние: сокращение времени на 20%
3. **Структуризация системы**
    - Элементы: операторы, ПО, клиенты
    - Связи: поток звонков, база данных, отчетность
4. **Анализ альтернатив**
    - Вариант 1: Увеличение штата
    - Вариант 2: Внедрение чат-бота
    - Вариант 3: Оптимизация скриптов

3.3. Обработка результатов

- Сравнение вариантов по критериям:
    - Затраты
    - Время внедрения
    - Эффективность

4. Содержание отчета

1. **Титульный лист**
2. **Введение** (цель, актуальность)
3. **Теоретическая часть** (конспект ключевых положений)
4. **Практический раздел**
    - Описание исследуемой системы
    - Графические модели
    - Таблицы сравнения альтернатив
5. **Выводы**
    - Найденные закономерности
    - Рекомендации по решению проблемы

5. Вопросы для защиты

1. В чем отличие системного подхода от традиционного анализа?
2. Какие методы используются для формализации слабоструктурированных проблем?
3. Как учитывается фактор неопределенности при построении моделей?
4. Приведите пример иерархической структуры системы из реальной жизни.
5. Почему при системном анализе важно рассматривать обратные связи?

Лабораторная работа №4 Порядок обоснования и выработка требований к проектируемой системе

Цель и содержание работы

Целью лабораторной работы является изучение методологии обоснования и формирования требований к проектируемой автоматизированной системе в защищенном исполнении. В ходе выполнения работы студенты должны

освоить принципы анализа предметной области, выявления угроз информационной безопасности, а также научиться формулировать функциональные и нефункциональные требования к системе с учетом требований защиты информации.

Теоретическое обоснование

1. Основные этапы проектирования защищенных автоматизированных систем

Проектирование автоматизированных систем (АС) в защищенном исполнении включает следующие этапы:

1. **Предпроектное обследование** – анализ предметной области, сбор исходных данных, определение целей и задач системы.
2. **Формирование требований** – разработка функциональных и нефункциональных требований, включая требования по информационной безопасности.
3. **Разработка технического задания (ТЗ)** – документ, регламентирующий основные параметры системы.
4. **Проектирование архитектуры системы** – выбор средств защиты, разработка схемы взаимодействия компонентов.
5. **Реализация и тестирование** – внедрение системы, проверка соответствия требованиям.
6. **Эксплуатация и сопровождение** – мониторинг безопасности, обновление защитных механизмов.

2. Обоснование требований к системе

Требования к АС формируются на основе:

- **Нормативных документов** (ФЗ №152 "О персональных данных", приказы ФСТЭК, ФСБ).

- **Анализа угроз** (модели нарушителя, возможные каналы утечки данных).
- **Бизнес-процессов заказчика** (функциональные требования к автоматизации).

Требования делятся на:

- **Функциональные** (что должна делать система).
- **Нефункциональные** (производительность, надежность, безопасность).

3. Требования к защищенности системы

В соответствии с ГОСТ Р 51583-2020, защищенная АС должна обеспечивать:

- **Конфиденциальность** – защиту от несанкционированного доступа (НСД).
- **Целостность** – предотвращение искажения данных.
- **Доступность** – устойчивость к отказам и атакам.

Для этого применяются:

- **Аутентификация и авторизация** (пароли, сертификаты, биометрия).
- **Шифрование данных** (криптографические алгоритмы).
- **Межсетевые экраны и системы обнаружения вторжений (СОВ).**

4. Разработка технического задания

Техническое задание должно включать:

- Цели и задачи системы.
- Описание угроз и мер защиты.
- Требования к аппаратно-программной платформе.
- Регламенты администрирования и аудита безопасности.

Методика и порядок выполнения работы

1. Анализ предметной области

- Изучить документы, регламентирующие работу системы (положения, регламенты).
- Выявить ключевые процессы, подлежащие автоматизации.

2. Формирование требований

- Составить список функциональных требований (например: "Система должна вести журнал аудита").
- Определить требования по защите (например: "Доступ к данным только после двухфакторной аутентификации").

3. Разработка модели угроз

- Определить возможные угрозы (утечка данных, DDoS-атаки).
- Оценить риски (вероятность и последствия).

4. Оформление отчета

- Описать выбранные меры защиты.
- Привести схему взаимодействия компонентов системы.

Содержание отчета

1. **Титульный лист**
2. **Введение** (цель и задачи работы).
3. **Основная часть**:
    - Описание предметной области.
    - Список требований к системе.
    - Модель угроз и меры защиты.
4. **Выводы** (итоги анализа, предложения по защите).

Вопросы для защиты

1. Какие этапы включает проектирование защищенных АС?
2. Как формируются требования к системе?
3. Какие нормативные документы регулируют защиту информации?

4. В чем разница между функциональными и нефункциональными требованиями?
5. Какие методы защиты данных применяются в АС?
6. Что должно входить в техническое задание на разработку системы?

Лабораторная работа №5 Порядок и содержание постановки сложной проблемы

Цель и содержание работы

Целью данной лабораторной работы является изучение методологии постановки сложных проблем в рамках проектирования и эксплуатации автоматизированных систем (АС) в защищенном исполнении. В ходе работы рассматриваются основные этапы формализации проблемы, методы анализа требований, а также подходы к разработке решений с учетом требований информационной безопасности.

Теоретическое обоснование

1. Понятие сложной проблемы в автоматизированных системах

Сложная проблема в контексте автоматизированных систем представляет собой задачу, для решения которой необходимо учитывать множество взаимосвязанных факторов, включая:

- **Технические аспекты** (архитектура системы, алгоритмы обработки данных, аппаратные ограничения);
- **Организационные аспекты** (распределение ролей, регламенты работы);
- **Безопасность** (защита от несанкционированного доступа, обеспечение целостности и конфиденциальности данных).

Примеры сложных проблем:

- Разработка системы контроля доступа с многофакторной аутентификацией.
- Оптимизация производительности распределенной АС в условиях высоких нагрузок.
- Обеспечение отказоустойчивости критически важных компонентов.

2. Этапы постановки сложной проблемы

1. **Идентификация проблемы**
    - Определение границ и контекста.
    - Выявление стейкхолдеров (пользователи, администраторы, разработчики).
    - Формулировка ключевых вопросов.
2. **Сбор и анализ требований**
    - Функциональные требования (что должна делать система).
    - Нефункциональные требования (производительность, безопасность, надежность).
    - Ограничения (бюджет, сроки, законодательные нормы).
3. **Декомпозиция проблемы**
    - Разбиение на подзадачи (например, разделение системы на модули: аутентификация, журналирование, шифрование).
    - Определение приоритетов.
4. **Выбор методологии решения**
    - Применение стандартов (ГОСТ Р 57580, ISO 27001).
    - Использование моделей угроз (например, STRIDE или OCTAVE).
    - Проектирование архитектуры с учетом принципов безопасности (минимальные привилегии, защита в глубину).
5. **Верификация и валидация**
    - Тестирование на соответствие требованиям.
    - Анализ уязвимостей (сканирование кода, пентесты).

- Документирование решений.

3. Инструменты и методы анализа

- **Диаграммы потоков данных (DFD)** – визуализация процессов обработки информации.
- **Моделирование угроз (Threat Modeling)** – выявление потенциальных атак.
- **FMEA (Failure Mode and Effects Analysis)** – анализ отказов и их последствий.
- **Использование CASE-средств (например, Rational Rose, Enterprise Architect)** для проектирования.

Аппаратура и материалы

1. Персональный компьютер с установленным ПО для моделирования (например, Microsoft Threat Modeling Tool).
2. Документация по стандартам информационной безопасности (ГОСТ, NIST SP 800-53).
3. Примеры технических заданий на разработку защищенных АС.

Методика и порядок выполнения работы

1. **Ознакомление с теоретической частью**
   - Изучить принципы постановки сложных проблем.
   - Разобрать примеры из реальных проектов.
2. **Анализ кейса**
   - Получить описание проблемы (например, необходимость внедрения системы защиты персональных данных в медицинской организации).
   - Провести декомпозицию:
     - Требования закона 152-ФЗ.
     - Риски (утечки, несанкционированный доступ).
     - Технические решения (шифрование, разграничение прав).

3. **Разработка концепции решения**
    - Создать модель угроз.
    - Предложить архитектурные решения (например, использование HSM для хранения ключей).
4. **Оформление отчета**
    - Описание проблемы.
    - Анализ требований.
    - Предложенное решение.
    - Выводы.

Содержание отчета

1. **Титульный лист**
2. **Введение** (актуальность темы, цель работы).
3. **Основная часть**:
    - Описание проблемы.
    - Методы анализа.
    - Результаты моделирования (диаграммы, таблицы).
4. **Выводы** (эффективность предложенного подхода, возможные улучшения).

Вопросы для защиты работы

1. Какие этапы включает постановка сложной проблемы?
2. Как учитываются требования информационной безопасности при проектировании АС?
3. В чем преимущества декомпозиции проблемы?
4. Назовите методы анализа рисков в защищенных АС.
5. Какие инструменты используются для моделирования угроз?

Лабораторная работа №6 Этапы решения сложной проблемы

Цель и содержание работы

Целью лабораторной работы является изучение методологии решения сложных проблем в контексте разработки и эксплуатации автоматизированных систем в защищенном исполнении. В ходе работы рассматриваются основные этапы анализа, проектирования и реализации решений для сложных задач, а также методы обеспечения информационной безопасности на каждом этапе.

Теоретическое обоснование

1. Понятие сложной проблемы

Сложная проблема – это задача, для решения которой требуется комплексный подход, включающий анализ, декомпозицию, моделирование и поэтапную реализацию. В области автоматизированных систем сложные проблемы часто связаны с обеспечением безопасности, отказоустойчивости, производительности и совместимости компонентов.

2. Этапы решения сложной проблемы

2.1. Анализ и постановка задачи

На первом этапе необходимо четко определить проблему, ее границы и требования к решению. Включает:

- **Формулировку цели** – что должно быть достигнуто.
- **Выявление ограничений** – технические, временные, ресурсные, законодательные.
- **Анализ рисков** – угрозы безопасности, возможные сбои, уязвимости.

2.2. Декомпозиция проблемы

Сложная задача разбивается на подзадачи, которые решаются независимо или последовательно. Используются методы:

- **Функциональная декомпозиция** – разделение по выполняемым функциям.

- **Объектно-ориентированный подход** – выделение сущностей и их взаимодействий.

2.3. Проектирование решения

Разрабатывается архитектура системы, выбираются методы и инструменты. Основные аспекты:

- **Выбор технологий** – языки программирования, СУБД, криптографические алгоритмы.
- **Моделирование процессов** – UML-диаграммы, потоковые схемы.
- **Обеспечение безопасности** – разграничение доступа, шифрование, аудит.

2.4. Реализация и тестирование

- **Кодирование** – разработка программных модулей с учетом требований безопасности.
- **Интеграция** – объединение компонентов в единую систему.
- **Тестирование** – проверка функциональности, нагрузочные тесты, анализ уязвимостей.

2.5. Внедрение и сопровождение

- **Развертывание** – установка системы в рабочую среду.
- **Мониторинг** – контроль работоспособности, обнаружение аномалий.
- **Обновление и доработка** – устранение ошибок, адаптация к новым условиям.

3. Особенности защищенного исполнения

При разработке автоматизированных систем в защищенном исполнении необходимо учитывать:

- **Конфиденциальность** – защита данных от несанкционированного доступа.
- **Целостность** – предотвращение несанкционированных изменений.
- **Доступность** – обеспечение бесперебойной работы.

Методика выполнения работы

1. **Изучение теоретического материала** – анализ литературы по методам решения сложных задач и защите информации.
2. **Разбор кейсов** – рассмотрение примеров из практики (например, защита корпоративной сети, разработка безопасного ПО).
3. **Практическое задание** – разработка алгоритма решения конкретной проблемы (например, защита передачи данных в распределенной системе).
4. **Анализ результатов** – проверка корректности решения, выявление возможных улучшений.

Содержание отчета

1. **Титульный лист**
2. **Введение** – цель и задачи работы.
3. **Теоретическая часть** – описание этапов решения сложной проблемы.
4. **Практическая часть** – пример решения конкретной задачи.
5. **Выводы** – анализ полученных результатов.

Вопросы для защиты работы

1. Какие этапы включает процесс решения сложной проблемы?
2. Как декомпозиция помогает в решении сложных задач?
3. Какие методы обеспечения безопасности применяются на этапе проектирования?
4. Как тестирование влияет на надежность системы?
5. Каковы особенности защищенного исполнения автоматизированных систем?

Лабораторная работа №7 Стадии разработки системы защиты АСУ. Метод OpSec

1. Цель работы

1. Изучить поэтапный процесс создания системы защиты автоматизированных систем управления (АСУ)

2. Освоить методологию Operational Security (OpSec) для защиты информации
3. Научиться применять OpSec для анализа угроз и разработки защитных мер в АСУ

2. Теоретическая часть

2.1. Стадии разработки системы защиты АСУ

2.1.1. Предпроектное обследование

- Инвентаризация ресурсов АСУ (аппаратное обеспечение, ПО, данные)
- Анализ нормативных требований (ФСТЭК, ФСБ, отраслевые стандарты)
- Определение классов защищенности по ГОСТ Р 57580

2.1.2. Анализ угроз и моделирование нарушителя

- Составление перечня угроз (по методике ФСТЭК):
  - Несанкционированный доступ
  - Утечка информации
  - Отказ в обслуживании
- Построение модели нарушителя (внутренний/внешний, уровень подготовки)

2.1.3. Проектирование системы защиты

Архитектурные решения:

- Сегментация сети (DMZ, VLAN)
- Многофакторная аутентификация
- Системы обнаружения вторжений (IDS/IPS)

Технические средства:

Средство защиты	**Пример реализации**
Криптография	ГОСТ 28147-89, TLS 1.3
Контроль доступа	RBAC, мандатное управление

Средство защиты	Пример реализации
Мониторинг	SIEM-системы (Splunk, MaxPatrol)

2.1.4. Внедрение и тестирование

- Фазированное развертывание защиты
- Проведение:
  - Стресс-тестов
  - Тестов на проникновение
  - Аудит безопасности

2.1.5. Эксплуатация и сопровождение

- Политика обновлений (ежеквартальные патчи)
- Регламент реагирования на инциденты (SOP)
- Периодический пересмотр мер защиты

2.2. Методология OpSec

2.2.1. Базовые принципы

1. **Идентификация критических данных**
   - Картирование информационных потоков
   - Классификация данных (секретно, для служебного пользования, открыто)
2. **Анализ угроз**
   - Методика OCTAVE Allegro
   - Матрица рисков (вероятность × ущерб)
3. **Контрмеры**
   - Технические: DLP-системы, HSM
   - Организационные: инструктажи, разделение обязанностей

2.2.2. Применение в АСУ

Пример для SCADA-систем:

1. Критические данные: параметры технологических процессов

2. Угрозы:
   - Перехват данных OPC-серверов
   - Подмена команд управления
3. Контрмеры:
   - Шифрование Modbus TCP
   - "Воздушный зазор" для критических сегментов

3. Практическая часть

3.1. Кейс: Защита системы диспетчеризации

Исходные данные:

- АСУ ТП теплосетей
- 50 контроллеров, 3 сервера SCADA
- Удаленный доступ для обслуживания

Этапы работы:

1. Анализ угроз:
   - Риск: взлом VPN-доступа (CVSS 7.5)
   - Последствия: остановка котельных
2. Реализация OpSec:
   - Внедрение ГОСТ Р 34.10-2012 для аутентификации
   - Журналирование всех команд (аудит 90 дней)
3. Тестирование:
   - Сканирование уязвимостей (OpenVAS)
   - Составление отчета по модели "Красная команда"

4. Выводы

1. Разработка защиты АСУ требует системного подхода с учетом отраслевых стандартов
2. OpSec обеспечивает проактивную защиту через анализ операционных рисков

3. Эффективность защиты должна регулярно проверяться тестами на проникновение

5. Вопросы для защиты

1. Какие нормативные документы регламентируют защиту АСУ в РФ?
2. Как строится модель нарушителя для промышленных систем?
3. В чем отличие IDS и IPS в контексте АСУ?
4. Как метод OpSec интегрируется с ISO 27001?
5. Какие криптостандарты предпочтительны для АСУ ТП?

Лабораторная работа №8 Методология построения системы информационной безопасности АСУ: концептуальная модель

Цель и содержание работы

Целью лабораторной работы является изучение методологии построения системы информационной безопасности (СИБ) автоматизированных систем управления (АСУ) на основе концептуальной модели. В ходе работы рассматриваются основные принципы, этапы и компоненты разработки СИБ, а также анализируются угрозы и методы защиты информации в АСУ.

Теоретическое обоснование

1. Понятие системы информационной безопасности АСУ

Автоматизированная система управления (АСУ) — это комплекс аппаратно-программных средств, предназначенный для автоматизации процессов управления в различных сферах деятельности. В условиях роста киберугроз обеспечение информационной безопасности (ИБ) АСУ становится критически важной задачей.

Система информационной безопасности (СИБ) — это совокупность организационных и технических мер, направленных на защиту информации от несанкционированного доступа, модификации, уничтожения или утечки.

2. Концептуальная модель СИБ АСУ

Концептуальная модель СИБ АСУ представляет собой абстрактное описание структуры, принципов и механизмов защиты информации. Она включает следующие ключевые элементы:

1. **Объекты защиты** – данные, программное обеспечение, аппаратные средства, каналы связи.
2. **Угрозы информационной безопасности** – случайные или преднамеренные воздействия, приводящие к нарушению конфиденциальности, целостности или доступности информации.
3. **Методы и средства защиты** – криптография, аутентификация, контроль доступа, антивирусная защита, межсетевые экраны.
4. **Политика безопасности** – совокупность правил и процедур, регламентирующих защиту информации в АСУ.

3. Принципы построения СИБ АСУ

1. **Комплексность** – защита должна охватывать все компоненты системы.
2. **Непрерывность** – защитные меры должны действовать на всех этапах жизненного цикла АСУ.
3. **Гибкость** – возможность адаптации к изменяющимся угрозам.
4. **Эшелонированность** – использование нескольких уровней защиты.

4. Этапы разработки СИБ АСУ

1. **Анализ рисков** – выявление угроз и уязвимостей.
2. **Разработка политики безопасности** – определение правил и процедур защиты.

3. **Реализация защитных мер** – внедрение технических и организационных средств.
4. **Мониторинг и аудит** – контроль эффективности защиты.

5. Основные стандарты и нормативные документы

- ГОСТ Р 50922-2006 "Защита информации. Основные термины и определения".
- ФСТЭК России: руководящие документы по защите информации.
- ISO/IEC 27001 – международный стандарт по информационной безопасности.

Аппаратура и материалы

1. Компьютер с установленным ПО для моделирования систем защиты (например, *Kali Linux*, *Wireshark*).
2. Учебные материалы по информационной безопасности.
3. Нормативные документы (ГОСТ, ФСТЭК).

Методика и порядок выполнения работы

1. **Изучить теоретические основы** построения СИБ АСУ.
2. **Разработать концептуальную модель** защиты для конкретной АСУ.
3. **Провести анализ угроз** и предложить методы противодействия.
4. **Оформить отчет** с описанием модели и выводов.

Содержание отчета

1. **Титульный лист**
2. **Введение** (цель и задачи работы).
3. **Теоретическая часть** (основные понятия, концептуальная модель).
4. **Практическая часть** (анализ угроз, предложенные меры защиты).
5. **Выводы** (итоги работы, значимость изученной темы).

Вопросы для защиты работы

1. Что такое система информационной безопасности АСУ?

2. Какие элементы включает концептуальная модель СИБ?
3. Назовите основные принципы построения СИБ.
4. Какие этапы включает разработка СИБ АСУ?
5. Какие нормативные документы регламентируют защиту информации?
6. Какие методы защиты информации применяются в АСУ?

Лабораторная работа №9 Методология построения системы информационной безопасности АСУ: этапы построения системы информационной безопасности

Цель

Исследовать методологию построения системы информационной безопасности автоматизированных систем управления, изучить последовательность этапов создания СИБ и их содержание.

Задачи:

1. Изучить теоретические основы построения СИБ АСУ
2. Рассмотреть поэтапную методологию создания системы защиты
3. Проанализировать особенности реализации каждого этапа
4. Исследовать нормативную базу информационной безопасности
5. Разработать рекомендации по построению СИБ для конкретной АСУ

2. Теоретическая часть

2.1. Основные понятия и определения

Система информационной безопасности (СИБ) - это комплекс организационных и технических мер, направленных на:

- обеспечение конфиденциальности информации
- сохранение целостности данных

- гарантирование доступности информационных ресурсов

Автоматизированная система управления (АСУ) - совокупность программно-аппаратных средств, предназначенных для автоматизации процессов управления в различных отраслях деятельности.

2.2. Этапы построения СИБ АСУ

1. Предпроектное обследование:

- Анализ объекта защиты
- Инвентаризация информационных ресурсов
- Выявление критически важных данных
- Оценка потенциальных угроз
- Анализ существующих рисков

2. Разработка концепции безопасности:

- Формирование политики безопасности
- Определение требований к защите
- Выбор модели безопасности
- Разработка архитектуры защиты

3. Проектирование системы защиты:

- Создание технического задания
- Разработка проектной документации
- Выбор средств защиты
- Проектирование подсистем безопасности

4. Реализация СИБ:

- Установка и настройка средств защиты
- Интеграция компонентов системы
- Тестирование работоспособности

- Обучение персонала

5. Эксплуатация и сопровождение:

- Мониторинг безопасности
- Анализ защищенности
- Реагирование на инциденты
- Обновление и модернизация

2.3. Методы и средства защиты информации

1. Организационные меры:

- Разработка регламентов
- Распределение прав доступа
- Контроль деятельности персонала

2. Технические средства:

- Криптографическая защита
- Системы аутентификации
- Межсетевые экраны
- Системы обнаружения вторжений

3. Программные решения:

- Антивирусная защита
- Средства контроля доступа
- Системы мониторинга

3. Практическая часть

3.1. Анализ объекта защиты

Для примера рассмотрим АСУ промышленного предприятия, включающую:

- Серверное оборудование

- Рабочие станции операторов
- Промышленные контроллеры
- Сетевую инфраструктуру
- Базы данных технологических процессов

3.2. Разработка поэтапного плана создания СИБ

1. Предпроектный этап:

- Составление перечня информационных активов
- Классификация данных по степени важности
- Анализ возможных угроз (внешние атаки, внутренние нарушения, техногенные факторы)
- Оценка рисков с использованием методики ГОСТ Р ИСО/МЭК 27005

2. Проектный этап:

- Разработка политики безопасности
- Создание модели угроз
- Проектирование архитектуры защиты:
    - Сегментация сети
    - Система разграничения доступа
    - Средства криптозащиты
    - Резервное копирование

3. Этап реализации:

- Внедрение межсетевого экрана
- Настройка системы аутентификации
- Установка средств антивирусной защиты
- Развертывание системы мониторинга

3.3. Пример реализации подсистемы защиты

Для подсистемы контроля доступа:

- Реализация многофакторной аутентификации
- Настройка политик парольной защиты
- Разграничение прав доступа по ролям
- Ведение журналов учета действий

4. Выводы и рекомендации

1. Построение СИБ АСУ требует системного подхода и последовательного выполнения всех этапов.
2. Особое внимание следует уделять:

- Тщательному анализу рисков на начальном этапе
- Грамотному проектированию архитектуры защиты
- Комплексному использованию организационных и технических мер

3. Для эффективной защиты рекомендуется:

- Регулярно обновлять средства защиты
- Проводить аудит безопасности
- Обучать персонал вопросам ИБ
- Разрабатывать планы реагирования на инциденты

5. Вопросы для самоконтроля

1. Перечислите основные этапы построения СИБ АСУ
2. Какие документы разрабатываются на предпроектном этапе?
3. Как проводится анализ рисков информационной безопасности?
4. Какие технические средства защиты наиболее эффективны для АСУ?
5. Как организовать мониторинг работоспособности СИБ?

Лабораторная работа №10 Методология построения системы

информационной безопасности АСУ: анализ этапов построения системы информационной безопасности

Цель:

Изучить методологию построения системы информационной безопасности (СИБ) автоматизированной системы управления (АСУ), проанализировать ключевые этапы разработки и внедрения защитных механизмов.

Содержание:

1. Изучение теоретических основ построения СИБ.
2. Анализ этапов проектирования системы защиты информации в АСУ.
3. Рассмотрение современных методов и стандартов обеспечения информационной безопасности.

Теоретическое обоснование

1. Понятие системы информационной безопасности АСУ

Автоматизированная система управления (АСУ) представляет собой комплекс программных и аппаратных средств, предназначенных для сбора, обработки, хранения и передачи данных в рамках управления технологическими или бизнес-процессами.

Информационная безопасность (ИБ) – состояние защищенности информации от несанкционированного доступа, уничтожения, модификации, блокирования, копирования, распространения, а также от иных неправомерных действий.

Система информационной безопасности (СИБ) – совокупность организационных и технических мер, направленных на обеспечение конфиденциальности, целостности и доступности информации в АСУ.

2. Основные принципы построения СИБ

1. **Комплексность** – защита должна охватывать все компоненты АСУ (аппаратные, программные, сетевые, человеческие).
2. **Непрерывность** – защитные меры должны действовать на всех этапах жизненного цикла системы.
3. **Гибкость** – возможность адаптации к изменяющимся угрозам.
4. **Эшелонированность** – многоуровневая защита (физическая, программная, криптографическая).
5. **Стандартизация** – использование общепринятых стандартов (ГОСТ Р ИСО/МЭК 27001, ФСТЭК, ФСБ).

3. Этапы построения СИБ в АСУ

3.1. Анализ рисков и угроз

- **Идентификация активов** (данные, ПО, оборудование, персонал).
- **Выявление угроз** (внешние атаки, инсайдеры, сбои оборудования).
- **Оценка уязвимостей** (анализ защищенности системы).
- **Расчет рисков** (вероятность реализации угрозы × возможный ущерб).

3.2. Разработка политики безопасности

- Определение правил доступа.
- Регламентация работы с конфиденциальной информацией.
- Установка требований к защите данных.

3.3. Проектирование системы защиты

- **Физическая защита** (контроль доступа в помещения, видеонаблюдение).
- **Программно-аппаратные меры** (брандмауэры, антивирусы, системы обнаружения вторжений).
- **Криптографическая защита** (шифрование данных, электронная подпись).
- **Резервное копирование и восстановление**.

3.4. Внедрение и тестирование

- Установка защитных механизмов.
- Проведение тестов на проникновение (pentesting).
- Аудит безопасности.

3.5. Мониторинг и сопровождение

- Постоянный контроль защищенности.
- Обновление средств защиты.
- Реагирование на инциденты.

4. Стандарты и нормативные документы

- **ГОСТ Р ИСО/МЭК 27001** – международный стандарт по управлению информационной безопасностью.
- **Приказы ФСТЭК России** (№ 17, № 21) – требования к защите информации в госструктурах.
- **Федеральный закон № 152-ФЗ "О персональных данных"**.

Аппаратура и материалы

1. Компьютер с ОС Windows/Linux.
2. Программное обеспечение для анализа защищенности (Nessus, Wireshark, Metasploit).
3. Нормативные документы по ИБ.

Методика и порядок выполнения работы

1. Изучить теоретические основы построения СИБ.
2. Провести анализ угроз для типовой АСУ.
3. Разработать модель защиты на основе стандартов.
4. Протестировать предложенные меры с использованием ПО для аудита безопасности.

Содержание отчета

1. **Титульный лист**
2. **Введение** (цель и задачи работы).

3. **Теоретическая часть** (основы методологии построения СИБ).
4. **Практическая часть** (анализ угроз, проектирование защиты).
5. **Выводы** (результаты, предложения по улучшению).

Вопросы для защиты работы

1. Каковы основные принципы построения СИБ в АСУ?
2. Назовите ключевые этапы проектирования системы защиты.
3. Какие стандарты регулируют информационную безопасность в РФ?
4. Какие методы криптографической защиты применяются в АСУ?
5. Как проводится анализ рисков при построении СИБ?

Лабораторная работа №11 Принципы, понятия политики и уровней безопасности. Задачи этапа предпроектного обследования

Цель:

Изучить основные принципы и понятия политики безопасности, уровни защиты информации, а также задачи, решаемые на этапе предпроектного обследования автоматизированных систем.

Содержание:

1. Изучение базовых принципов информационной безопасности.
2. Анализ политики безопасности и ее уровней.
3. Рассмотрение задач предпроектного обследования при разработке защищенных АСУ.

Теоретическое обоснование
1. Основные принципы информационной безопасности

Информационная безопасность (ИБ) в автоматизированных системах базируется на трех ключевых принципах:

1. **Конфиденциальность** – обеспечение доступа к информации только авторизованным пользователям.
2. **Целостность** – защита данных от несанкционированного изменения или уничтожения.
3. **Доступность** – гарантия того, что информация и сервисы доступны для авторизованных пользователей в нужное время.

Дополнительные принципы:

- **Подотчетность** – фиксация действий пользователей и администраторов.
- **Аутентичность** – подтверждение подлинности данных и пользователей.

2. Политика безопасности: понятие и виды

Политика безопасности – совокупность правил и процедур, регламентирующих управление, защиту и распределение информационных ресурсов в организации.

Виды политик безопасности:

1. **Общая политика безопасности** – определяет стратегические цели и подходы к защите информации.
2. **Функциональные политики** – детализируют меры защиты для отдельных компонентов системы (доступ к данным, работа с персональными данными и т. д.).
3. **Регламентирующие документы** – инструкции, стандарты и методики, обеспечивающие выполнение политик.

3. Уровни безопасности

В зависимости от критичности информации и систем, выделяют несколько уровней защиты:

1. **Физический уровень** – защита оборудования и носителей информации (контроль доступа, видеонаблюдение, защита от пожаров и перебоев электропитания).
2. **Программно-аппаратный уровень** – использование межсетевых экранов, систем обнаружения вторжений (IDS), антивирусного ПО.
3. **Организационный уровень** – регламенты работы персонала, обучение сотрудников, управление инцидентами.
4. **Законодательный уровень** – соблюдение нормативных требований (152-ФЗ, ГОСТ Р ИСО/МЭК 27001).

4. Этап предпроектного обследования

Предпроектное обследование – начальная фаза разработки защищенной АСУ, включающая анализ текущего состояния системы и выявление требований к безопасности.

Основные задачи этапа:

1. **Анализ предметной области** – изучение бизнес-процессов, информационных потоков, критичных данных.
2. **Идентификация активов** – определение ценных информационных ресурсов (базы данных, серверы, рабочие станции).
3. **Оценка угроз и уязвимостей** – выявление возможных каналов утечки информации, слабых мест в защите.
4. **Определение требований к безопасности** – формулировка условий, при которых система будет считаться защищенной.
5. **Разработка концепции безопасности** – предварительный план внедрения защитных мер.

Методы проведения обследования:

- Анкетирование и интервью с сотрудниками.
- Аудит существующих систем защиты.
- Тестирование на проникновение (если допустимо).

Аппаратура и материалы

1. Компьютер с доступом к нормативной документации (ГОСТ, ФСТЭК, ФСБ).
2. Программные средства для анализа защищенности (например, Nessus, OpenVAS).
3. Шаблоны политик безопасности.

Методика и порядок выполнения работы

1. Изучить теоретические основы политики безопасности и уровней защиты.
2. Провести анализ требований к защите информации в заданной предметной области.
3. Разработать фрагмент политики безопасности для условной организации.
4. Сформулировать перечень задач предпроектного обследования для выбранной АСУ.

Содержание отчета

1. **Титульный лист**
2. **Введение** (цель и задачи работы).
3. **Теоретическая часть** (принципы ИБ, политика безопасности, уровни защиты).
4. **Практическая часть** (анализ требований, разработка политики, задачи предпроектного обследования).
5. **Выводы** (итоги работы, рекомендации).

Вопросы для защиты работы

1. Каковы три основных принципа информационной безопасности?
2. Что включает в себя политика безопасности?
3. Назовите уровни защиты информации в АСУ.
4. Какие задачи решаются на этапе предпроектного обследования?
5. Какие методы используются при предпроектном анализе?

Лабораторная работа №12 Задача этапа анализа и управления рисками

Цель и содержание работы

Целью лабораторной работы является изучение задач, методов и инструментов, применяемых на этапе анализа и управления рисками в автоматизированных системах (АС) защищенного исполнения. В ходе работы рассматриваются основные подходы к идентификации, оценке и минимизации рисков, а также практические аспекты их применения в условиях реальных угроз информационной безопасности.

Теоретическое обоснование

1. Понятие риска в защищенных АС

Риск в контексте автоматизированных систем – это вероятность реализации угрозы безопасности, приводящей к нарушению конфиденциальности, целостности или доступности информации. Управление рисками включает:

- **Идентификацию рисков** – определение потенциальных угроз и уязвимостей.
- **Оценку рисков** – анализ вероятности и последствий их реализации.
- **Выбор мер противодействия** – разработку стратегий снижения рисков (принятие, снижение, передача, избегание).

2. Этапы анализа и управления рисками

1. **Идентификация активов** – определение критически важных компонентов АС (данные, ПО, оборудование, персонал).
2. **Выявление угроз и уязвимостей** – анализ возможных источников рисков (кибератаки, сбои оборудования, человеческий фактор).
3. **Оценка рисков** – качественный (экспертный анализ) или количественный (вероятностные модели) методы.
4. **Разработка мер защиты** – внедрение технических (шифрование, контроль доступа) и организационных (регламенты, обучение) мер.
5. **Мониторинг и переоценка** – периодический контроль эффективности принятых мер.

3. Методологии анализа рисков

- **ГОСТ Р ИСО/МЭК 27005** – международный стандарт управления рисками ИБ.
- **OCTAVE** (Operationally Critical Threat, Asset, and Vulnerability Evaluation) – фокус на бизнес-процессах.
- **NIST SP 800-30** – методика оценки рисков от Национального института стандартов США.

4. Инструменты управления рисками

- **Системы мониторинга (SIEM)** – сбор и анализ данных об угрозах.
- **Сканеры уязвимостей (OpenVAS, Nessus)** – автоматизированное выявление слабых мест.
- **Матрицы рисков** – визуализация уровня угроз для принятия решений.

Аппаратура и материалы

1. **Компьютер с ОС Windows/Linux** – для моделирования угроз.
2. **Программное обеспечение:**

- *OpenVAS* – сканер уязвимостей.
- *Wireshark* – анализатор сетевого трафика.
- *Excel* – построение матрицы рисков.

3. **Нормативные документы:** ГОСТ Р ИСО/МЭК 27005, NIST SP 800-30.

Методика и порядок выполнения работы

Часть 1. Идентификация рисков

1. Составьте перечень активов АС (серверы, БД, пользовательские рабочие станции).
2. Проведите мозговой штурм для выявления угроз (например: DDoS-атака, утечка данных через фишинг).

Часть 2. Оценка рисков

1. Используя шкалы вероятности (1–5) и последствий (1–5), оцените каждый риск. Пример:

- *Угроза:* Внедрение вредоносного ПО.
- *Вероятность:* 4 (высокая из-за частых атак).
- *Последствия:* 5 (критичные для бизнеса).
- *Уровень риска:* 4×5 = 20 (максимальный).

2. Постройте матрицу рисков в Excel, выделив зоны (низкий, средний, высокий риск).

Часть 3. Разработка мер защиты

1. Для рисков с высоким уровнем предложите меры:

- *Технические:* Внедрение EDR-систем (например, CrowdStrike).
- *Организационные:* Обучение сотрудников киберграмотности.

Часть 4. Практическое задание

1. Запустите сканер OpenVAS для проверки узла сети.
2. Проанализируйте отчет, выделив критические уязвимости (например, CVE-2023-1234).

Содержание отчета

1. **Титульный лист**
2. **Теоретическая часть** – краткое изложение методов анализа рисков.

3. **Практическая часть** – результаты идентификации угроз, матрица рисков, предложенные меры.
4. **Выводы** – эффективность примененных методик, сложности, рекомендации.

Вопросы для защиты

1. Какие этапы включает процесс управления рисками?
2. В чем разница между качественной и количественной оценкой рисков?
3. Как матрица рисков помогает в принятии решений?
4. Назовите 3 метода снижения рисков в защищенных АС.
5. Какие инструменты используются для автоматизации анализа уязвимостей?

Лабораторная работа №13 Методы и средства обеспечения информационной безопасности в АСУ

Цель:

Исследование методов и средств обеспечения информационной безопасности в автоматизированных системах управления (АСУ).

Содержание:

1. Анализ угроз информационной безопасности в АСУ.
2. Изучение методов защиты информации в автоматизированных системах.
3. Ознакомление с аппаратными и программными средствами обеспечения информационной безопасности.
4. Практическое исследование механизмов защиты данных в АСУ.

Теоретическое обоснование

1. Понятие информационной безопасности в АСУ

Автоматизированные системы управления (АСУ) представляют собой комплекс аппаратно-программных средств, предназначенных для сбора, обработки, хранения и передачи данных в различных отраслях промышленности, управления и бизнеса.

Информационная безопасность (ИБ) – это состояние защищенности информации от несанкционированного доступа, уничтожения, модификации, блокирования, копирования, распространения, а также от иных неправомерных действий.

2. Основные угрозы информационной безопасности в АСУ

- **Внешние угрозы:**
  - Кибератаки (DDoS, фишинг, вирусы, трояны).
  - Хакерские атаки на серверы и базы данных.
  - Утечки информации через каналы связи.
- **Внутренние угрозы:**
  - Несанкционированный доступ сотрудников.
  - Ошибки персонала при работе с данными.
  - Умышленный саботаж или кража информации.

3. Методы обеспечения информационной безопасности

- **Организационные меры:**
  - Разработка политики безопасности.
  - Контроль доступа к информации.
  - Регламентация работы с данными.
- **Технические меры:**
  - Шифрование данных (AES, RSA).
  - Межсетевые экраны (Firewall).
  - Системы обнаружения вторжений (IDS/IPS).
  - Антивирусная защита.
- **Программно-аппаратные средства:**

- Средства аутентификации (биометрия, токены).
- Виртуальные частные сети (VPN).
- Резервное копирование данных.

4. Средства защиты информации в АСУ

- **Криптографические методы:**
  - Симметричное шифрование (DES, AES).
  - Асимметричное шифрование (RSA, ECC).
  - Электронная подпись (ЭП).
- **Сетевые технологии защиты:**
  - VLAN для сегментации сети.
  - IPSec для безопасной передачи данных.
  - SIEM-системы для мониторинга угроз.
- **Физическая защита:**
  - Контроль доступа в серверные помещения.
  - Видеонаблюдение.
  - Защита от электромагнитных наводок.

Аппаратура и материалы

1. Персональный компьютер с ОС Windows/Linux.
2. Программное обеспечение:
   - Wireshark (анализатор сетевого трафика).
   - Nessus (сканер уязвимостей).
   - VeraCrypt (шифрование данных).
3. Учебные стенды с элементами АСУ.

Методика и порядок выполнения работы

1. Анализ угроз информационной безопасности

- Изучить возможные каналы утечки информации в АСУ.
- Провести моделирование атаки на тестовую систему.

2. Исследование методов защиты

- Настроить межсетевой экран (Firewall).
- Протестировать работу антивирусного ПО.
- Оценить эффективность шифрования данных.

3. Практическое применение средств защиты

- Развернуть VPN-соединение.
- Настроить систему обнаружения вторжений (Snort).
- Провести аудит безопасности с помощью Nessus.

Содержание отчета

Отчет должен включать:

1. **Титульный лист** (название дисциплины, тема, ФИО студента, группа, ФИО преподавателя).
2. **Теоретическую часть** (основные понятия, угрозы, методы защиты).
3. **Практическую часть** (результаты тестирования, настройки защиты).
4. **Выводы** (эффективность примененных мер, рекомендации).

Вопросы для защиты работы

1. Какие основные угрозы информационной безопасности существуют в АСУ?
2. Какие методы шифрования применяются для защиты данных?
3. Как работает система обнаружения вторжений (IDS)?
4. Какие организационные меры повышают безопасность АСУ?
5. В чем преимущества VPN для защиты передачи данных?
6. Как оценить эффективность антивирусной защиты?
7. Какие физические меры защиты применяются в серверных помещениях?

Лабораторная работа №14 Нормативно-правовая база информационной безопасности

Цель и содержание работы

Целью лабораторной работы является изучение нормативно-правовых актов, регулирующих вопросы информационной безопасности (ИБ) в автоматизированных системах (АС) защищенного исполнения. В ходе работы рассматриваются ключевые законы, стандарты и методические документы, определяющие требования к защите информации, а также практические аспекты их применения при проектировании и эксплуатации АС.

Теоретическое обоснование

1. Понятие нормативно-правовой базы информационной безопасности

Нормативно-правовая база (НПБ) ИБ – это совокупность законодательных актов, стандартов, руководящих документов и методических рекомендаций, регламентирующих защиту информации в автоматизированных системах. Основные категории документов:

- **Законы и подзаконные акты** – обязательные для исполнения нормативные документы (ФЗ, указы, постановления).
- **Государственные стандарты (ГОСТ)** – технические требования к защите информации.
- **Методические рекомендации** – практические руководства по реализации мер ИБ.

2. Основные законодательные акты в области ИБ

2.1. Федеральные законы РФ

1. **Федеральный закон № 149-ФЗ "Об информации, информационных технологиях и о защите информации"** (2006 г.) – определяет понятия информации, информационных систем и мер их защиты.

2. **Федеральный закон № 152-ФЗ "О персональных данных"** (2006 г.) – регулирует обработку и защиту персональных данных (ПДн).
3. **Федеральный закон № 187-ФЗ "О безопасности критической информационной инфраструктуры"** (2017 г.) – устанавливает требования к защите объектов КИИ.
4. **Федеральный закон № 390-ФЗ "О безопасности"** (2010 г.) – общие принципы обеспечения безопасности, включая ИБ.

2.2. Подзаконные акты

- **Постановление Правительства № 1119** (2011 г.) – требования к защите ПДн при их обработке в информационных системах.
- **Приказ ФСТЭК России № 21** (2013 г.) – требования по защите информации в государственных информационных системах.
- **Приказ ФСБ России № 378** (2018 г.) – порядок разработки и сертификации средств криптографической защиты информации (СКЗИ).

3. Государственные и международные стандарты

1. **ГОСТ Р 57580.1-2017** – требования к защите информации в АС.
2. **ГОСТ Р ИСО/МЭК 27001** – стандарт менеджмента информационной безопасности (аналог ISO/IEC 27001).
3. **ГОСТ Р 50922-2006** – основные термины и определения в области ИБ.
4. **NIST SP 800-53** (США) – стандарт защиты информационных систем.

4. Отраслевые и ведомственные документы

- **Методические рекомендации ФСТЭК** – по защите информации в облачных технологиях, IoT и других современных системах.
- **РД Гостехкомиссии РФ** – руководящие документы по защите от несанкционированного доступа (НСД).

Аппаратура и материалы

1. **Компьютер с доступом в интернет** – для поиска нормативных документов.
2. **Программное обеспечение:**

- *КонсультантПлюс* или *Гарант* – правовые базы данных.
- *Adobe Acrobat Reader* – для работы с PDF-версиями ГОСТов.

3. **Тексты нормативных актов:** ФЗ-149, ФЗ-152, ГОСТ Р 57580.1-2017.

Методика и порядок выполнения работы

Часть 1. Анализ законодательных актов

1. Изучите структуру Федерального закона № 152-ФЗ "О персональных данных". Выделите:

- Основные принципы обработки ПДн (ст. 5).
- Требования к защите ПДн (ст. 19).
- Права субъектов ПДн (ст. 14).

2. Сравните требования ФЗ-152 и Постановления № 1119. В чем различия в классификации информационных систем?

Часть 2. Работа с ГОСТами

1. Откройте ГОСТ Р 57580.1-2017. Определите:

- Категории защищаемой информации (конфиденциальная, служебная).
- Требования к средствам защиты информации (СЗИ).

2. Составьте таблицу соответствия между ГОСТ Р ИСО/МЭК 27001 и ISO/IEC 27001.

Часть 3. Практическое задание

1. С помощью системы *КонсультантПлюс* найдите все приказы ФСТЭК, касающиеся защиты АС. Выпишите их номера и основные положения.
2. Подготовьте примеры нарушений ИБ, подпадающих под ст. 13.11 КоАП РФ (нарушение требований к защите ПДн).

Содержание отчета

1. **Титульный лист**
2. **Теоретическая часть** – краткое описание ключевых законов и стандартов.
3. **Практическая часть** – результаты анализа документов, таблицы, примеры.

4. **Выводы** – значение НПБ ИБ для проектирования защищенных АС.

Вопросы для защиты

1. Назовите три основных федеральных закона в области ИБ.
2. Какие организации в РФ регулируют вопросы защиты информации (ФСТЭК, ФСБ, Роскомнадзор)?
3. В чем разница между ГОСТ и международным стандартом ISO?
4. Какие меры защиты ПДн предусмотрены ФЗ-152?
5. Как классифицируются информационные системы по Постановлению № 1119?

Лабораторная работа № 15 Архитектура защищённых автоматизированных систем

Цель и содержание работы

Целью лабораторной работы является изучение архитектурных принципов построения защищённых автоматизированных систем (АС), включая их структурные компоненты, механизмы защиты информации и особенности функционирования. В ходе работы рассматриваются базовые модели безопасности, методы обеспечения конфиденциальности, целостности и доступности данных, а также практические аспекты проектирования защищённых АС.

Теоретическое обоснование

1. Понятие защищённой автоматизированной системы

Защищённая автоматизированная система (ЗАС) — это комплекс программно-аппаратных средств, организационных мер и нормативных

требований, обеспечивающих безопасность информации при её обработке, хранении и передаче. Основные характеристики ЗАС:

- **Конфиденциальность** — предотвращение несанкционированного доступа к информации.
- **Целостность** — защита от несанкционированного изменения данных.
- **Доступность** — обеспечение бесперебойного доступа к информации для авторизованных пользователей.

2. Архитектурные модели защищённых АС

2.1. Многоуровневая модель защиты

Защищённые АС строятся на основе многоуровневой (эшелонированной) защиты, включающей:

1. **Физический уровень** — защита аппаратных компонентов (серверов, сетевого оборудования) от физического доступа и повреждений.
2. **Сетевой уровень** — использование межсетевых экранов (firewall), систем обнаружения вторжений (IDS), VPN.
3. **Операционный уровень** — защита операционных систем (разграничение прав доступа, антивирусное ПО).
4. **Прикладной уровень** — безопасность приложений (аутентификация, шифрование данных).
5. **Данные** — криптографическая защита информации (шифрование, электронная подпись).

2.2. Модель "Ядро-Периферия"

- **Ядро системы** — критически важные компоненты (СУБД, серверы аутентификации), защищаемые максимально строгими мерами.
- **Периферия** — пользовательские рабочие станции и внешние интерфейсы, где применяются стандартные меры защиты.

2.3. Микросегментация сети

Разделение сети на изолированные сегменты (зоны безопасности) для минимизации последствий взлома. Примеры зон:

- **DMZ (демилитаризованная зона)** — для публичных серверов (веб, почта).
- **Внутренняя сеть** — для сотрудников с контролируемым доступом.
- **Зона критичных данных** — для серверов БД и систем управления.

3. Компоненты защищённых АС

1. **Аппаратные средства:**
   - Серверы с аппаратными модулями безопасности (HSM).
   - Средства контроля физического доступа (чип-карты, биометрия).
2. **Программные средства:**
   - Средства криптографической защиты (СКЗИ, например, КриптоПро).
   - Системы мониторинга (SIEM-системы).
3. **Организационные меры:**
   - Регламенты доступа (ролевая модель).
   - Политики резервного копирования и аварийного восстановления.

4. Стандарты и нормативы

- **ГОСТ Р 57580.1-2017** — требования к защите информации в АС.
- **ФСТЭК России (Приказ № 21)** — требования к защите гос. информационных систем.
- **ISO/IEC 27001** — международный стандарт менеджмента информационной безопасности.

Аппаратура и материалы

1. **Компьютерный класс** — для моделирования архитектуры ЗАС.
2. **Программное обеспечение:**
   - *VMware/VirtualBox* — для создания изолированных сетевых сегментов.
   - *Wireshark* — анализ сетевого трафика.
   - *Cisco Packet Tracer* — проектирование защищённой сети.

3. **Нормативные документы:** ГОСТ Р 57580.1-2017, Приказ ФСТЭК № 21.

Методика и порядок выполнения работы

Часть 1. Анализ архитектурных решений

1. Изучите многоуровневую модель защиты на примере банковской системы. Определите:
   - Какие механизмы защиты применяются на каждом уровне.
   - Как обеспечивается изоляция критичных данных (например, платёжных реквизитов).
2. Сравните модели "Ядро-Периферия" и микросегментации. В каких случаях каждая из них предпочтительна?

Часть 2. Практическое моделирование

1. В *Cisco Packet Tracer* создайте сеть с тремя зонами безопасности:
   - DMZ (веб-сервер).
   - Внутренняя сеть (рабочие станции).
   - Зона БД (сервер SQL).
2. Настройте межсетевой экран между зонами. Запретите прямой доступ из DMZ в зону БД.

Часть 3. Аудит защиты

1. Проверьте настройки безопасности виртуальной машины (ОС Windows/Linux):
   - Отключите незащищённые протоколы (Telnet, FTP).
   - Включите шифрование дисков (BitLocker/LUKS).

Содержание отчета

1. **Титульный лист**
2. **Теоретическая часть** — описание архитектурных моделей и компонентов ЗАС.

3. **Практическая часть** — результаты моделирования сети, скриншоты настроек.
4. **Выводы** — эффективность применённых мер защиты, рекомендации.

Вопросы для защиты

1. Назовите три основных свойства защищённой АС (конфиденциальность, целостность, доступность).
2. В чём суть многоуровневой защиты?
3. Какие компоненты входят в "ядро" защищённой системы?
4. Для чего используется DMZ?
5. Как микросегментация повышает безопасность сети?

Лабораторная работа №16 *Методы оценки защищённости АСУ*

Цель:

Изучить методы оценки защищённости автоматизированных систем управления (АСУ), провести анализ существующих подходов к определению уровня безопасности и выявить уязвимости в защищённых системах.

Содержание:

1. Изучение теоретических основ оценки защищённости АСУ.
2. Анализ методов тестирования на проникновение (penetration testing).
3. Исследование стандартов и нормативных документов в области информационной безопасности.
4. Практическое применение методов оценки защищённости на примере моделируемой системы.

Теоретическое обоснование

1. Понятие защищённости АСУ

Автоматизированная система управления (АСУ) — это комплекс аппаратно-программных средств, предназначенных для автоматизации процессов управления в различных сферах (промышленность, транспорт, энергетика и др.). Защищённость АСУ — это её способность противостоять несанкционированному доступу, разрушению, модификации или утечке информации.

2. Основные угрозы безопасности АСУ

- **Внешние угрозы:** атаки хакеров, вредоносное ПО, DDoS-атаки.
- **Внутренние угрозы:** ошибки персонала, умышленные действия сотрудников.
- **Технические угрозы:** отказы оборудования, уязвимости ПО.

3. Методы оценки защищённости

1. **Анализ рисков** — выявление и оценка потенциальных угроз.
2. **Аудит безопасности** — проверка соответствия системы требованиям стандартов (ГОСТ Р ИСО/МЭК 15408, ГОСТ Р 57580).
3. **Тестирование на проникновение (pentest)** — имитация атак для выявления уязвимостей.
4. **Мониторинг защищённости** — непрерывный контроль состояния системы.
5. **Экспертные оценки** — анализ специалистами в области ИБ.

4. Стандарты и нормативные документы

- **ГОСТ Р 50922-2006** — Защита информации. Основные термины и определения.
- **ГОСТ Р 57580.1-2017** — Безопасность финансовых организаций.
- **ISO/IEC 27001** — Международный стандарт по информационной безопасности.

Аппаратура и материалы

1. Компьютер с установленным ПО для анализа защищённости (Kali Linux, Metasploit, Wireshark).
2. Виртуальная среда для моделирования АСУ (VMware, VirtualBox).
3. Нормативные документы и методические рекомендации.

Методика и порядок выполнения работы

1. Подготовительный этап

- Ознакомление с теоретическими основами.
- Настройка виртуальной среды для тестирования.

2. Проведение аудита безопасности

- Сканирование сети на уязвимости (Nmap, OpenVAS).
- Анализ журналов событий.

3. Тестирование на проникновение

- Использование фреймворка Metasploit для имитации атак.
- Проверка устойчивости к SQL-инъекциям и XSS.

4. Оформление отчёта

- Фиксация выявленных уязвимостей.
- Разработка рекомендаций по повышению защищённости.

Содержание отчёта

1. **Титульный лист**
2. **Введение** (цель и задачи работы).
3. **Теоретическая часть** (методы оценки защищённости АСУ).
4. **Практическая часть** (результаты тестирования).
5. **Выводы** (оценка уровня защищённости, рекомендации).

Вопросы для защиты работы

1. Какие существуют методы оценки защищённости АСУ?
2. В чём заключается тестирование на проникновение?
3. Какие стандарты регламентируют безопасность АСУ?

4. Какие инструменты используются для анализа защищённости?
5. Как проводится аудит информационной безопасности?

Лабораторная работа №17 Защита АСУ от современных киберугроз

Цель и содержание работы

Провести исследование методов и средств защиты автоматизированных систем управления (АСУ) от современных киберугроз. Рассмотреть основные виды атак, способы их предотвращения и обеспечения информационной безопасности АСУ.

Теоретическое обоснование

1. Понятие АСУ и их уязвимости

Автоматизированные системы управления (АСУ) — это комплекс аппаратно-программных средств, предназначенных для автоматизации процессов управления в различных сферах (промышленность, энергетика, транспорт и др.).

Основные компоненты АСУ:

- **Серверы управления** — обеспечивают обработку данных и управление процессами.
- **Промышленные контроллеры (PLC, SCADA)** — управляют технологическим оборудованием.
- **Сети передачи данных** — связывают компоненты системы.
- **Человеко-машинный интерфейс (HMI)** — обеспечивает взаимодействие оператора с системой.

Уязвимости АСУ:

- Устаревшее программное обеспечение.
- Открытые сетевые порты и слабая аутентификация.

- Отсутствие сегментации сети.
- Использование стандартных паролей и учетных записей.

2. Современные киберугрозы для АСУ

2.1. Виды атак

1. **Атаки на SCADA-системы**
   - Внедрение вредоносного ПО (Stuxnet, Industroyer).
   - Перехват данных через уязвимости OPC-серверов.
2. **DDoS-атаки**
   - Перегрузка каналов связи, приводящая к отказу в обслуживании.
3. **Атаки на промышленные контроллеры**
   - Изменение параметров работы оборудования (например, температуры или давления).
4. **Фишинг и социальная инженерия**
   - Получение доступа через инсайдеров или невнимательность персонала.

2.2. Методы защиты

1. **Сегментация сети**
   - Разделение на зоны (IT и OT) с помощью межсетевых экранов.
2. **Использование систем обнаружения вторжений (IDS/IPS)**
   - Мониторинг аномальной активности в сети.
3. **Регулярное обновление ПО и патчинг**
   - Закрытие известных уязвимостей.
4. **Многофакторная аутентификация (MFA)**
   - Усиление контроля доступа.
5. **Шифрование данных**
   - Защита информации при передаче (TLS, VPN).
6. **Резервное копирование и аварийное восстановление**
   - Минимизация последствий атак.

3. Нормативные требования

- **ГОСТ Р 57580.1-2017** — Безопасность финансовых организаций.
- **ФСТЭК РФ (приказы № 17, 21, 239)** — Требования к защите АСУ ТП.
- **IEC 62443** — Международный стандарт кибербезопасности промышленных систем.

Аппаратура и материалы

1. **Компьютер с установленным ПО:**
   - Виртуальная машина с Kali Linux (для тестирования уязвимостей).
   - Wireshark (анализ сетевого трафика).
   - Metasploit Framework (проверка защищенности).
2. **Учебный стенд с имитацией АСУ (например, на базе Raspberry Pi и Modbus).**

Методика и порядок выполнения работы

1. **Анализ защищенности сети АСУ**
   - Сканирование сети с помощью Nmap.
   - Проверка открытых портов и служб.
2. **Моделирование атаки на SCADA-систему**
   - Использование утилиты **Modbuspal** для тестирования уязвимостей Modbus TCP.
3. **Тестирование системы обнаружения вторжений**
   - Запуск аномального трафика и проверка реакции IDS (например, Suricata).
4. **Разработка рекомендаций по защите**
   - Настройка межсетевого экрана (iptables/pfSense).
   - Внедрение MFA для доступа к HMI.

Содержание отчета

1. **Титульный лист**
2. **Теоретическая часть** (краткое описание угроз и методов защиты).
3. **Практическая часть** (результаты сканирования, обнаруженные уязвимости).

4. **Выводы и рекомендации** (предложения по улучшению защиты).

Вопросы для защиты работы

1. Какие основные угрозы существуют для АСУ?
2. Как работает DDoS-атака и как от нее защититься?
3. Какие стандарты регулируют безопасность АСУ?
4. Для чего нужна сегментация сети в АСУ?
5. Как обнаружить аномальную активность в промышленной сети?
6. Какие методы шифрования применяются в АСУ?

Лабораторная работа №18 Обеспечение отказоустойчивости и восстановления АСУ

Цель и содержание работы

Исследовать методы и средства обеспечения отказоустойчивости и восстановления автоматизированных систем управления (АСУ) в защищенном исполнении. Рассмотреть принципы резервирования, мониторинга состояния системы, а также алгоритмы восстановления после сбоев.

Теоретическое обоснование

1. Понятие отказоустойчивости в АСУ

Отказоустойчивость – это способность системы сохранять работоспособность при возникновении отказов отдельных компонентов. В контексте автоматизированных систем управления (АСУ) отказоустойчивость обеспечивается за счет:

- **Резервирования** (дублирование критически важных узлов);
- **Самодиагностики** (автоматическое выявление сбоевых состояний);

- **Автоматического переключения** на резервные модули;
- **Восстановления работоспособности** после устранения неисправностей.

2. Основные методы обеспечения отказоустойчивости

1. **Аппаратное резервирование**
    - *Горячий резерв* – резервные компоненты находятся в активном состоянии и готовы к немедленному включению.
    - *Холодный резерв* – резервные компоненты активируются только после отказа основных.
    - *Скользящий резерв* – один резервный модуль может заменять несколько основных.
2. **Программное резервирование**
    - Реализация алгоритмов контрольных сумм и проверки целостности данных.
    - Использование механизмов транзакций (откат к последней стабильной версии при сбое).
3. **Мониторинг и диагностика**
    - Системы непрерывного контроля состояния оборудования (датчики, логи анализаторов).
    - Программные средства логирования и анализа ошибок (SYSLOG, SNMP).
4. **Механизмы восстановления**
    - Автоматическая перезагрузка узлов.
    - Восстановление из резервных копий (backup).
    - Использование RAID-массивов для сохранности данных.

3. Архитектура отказоустойчивых АСУ

В защищенных АСУ применяются следующие архитектурные решения:

- **Кластерные системы** – группа серверов, работающих как единое целое. При отказе одного узла нагрузка автоматически перераспределяется.
- **Распределенные вычисления** – выполнение задач на нескольких независимых узлах для минимизации последствий сбоев.
- **Двухконтурные системы** – основной и резервный контуры управления, переключаемые автоматически.

4. Стандарты и требования к отказоустойчивости

- **ГОСТ Р 54597-2011** – требования к надежности автоматизированных систем.
- **IEC 61508** – стандарт функциональной безопасности.
- **Специальные требования ФСТЭК и ФСБ** для защищенных АСУ.

Аппаратура и материалы

1. **Компьютерный класс** с установленным ПО для моделирования отказоустойчивых систем (например, VMware ESXi, Oracle VM).
2. **Стенд с резервированными серверами** (например, два сервера в режиме failover).
3. **Программные средства мониторинга** (Zabbix, Nagios, PRTG).

Методика и порядок выполнения работы

1. Исследование механизмов резервирования

- Запуск виртуальной машины с дублированным сервером.
- Имитация отказа основного узла и наблюдение за переключением на резервный.

2. Анализ систем мониторинга

- Настройка Zabbix для отслеживания состояния серверов.
- Генерация искусственного сбоя и проверка реакции системы.

3. Тестирование восстановления данных

- Создание резервной копии базы данных.
- Имитация повреждения данных и восстановление из backup.

Содержание отчета

1. **Титульный лист**
2. **Теоретическая часть** (краткое изложение принципов отказоустойчивости).
3. **Практическая часть** (описание проведенных экспериментов, скриншоты, логи).
4. **Выводы** (эффективность изученных методов, возможные улучшения).

Вопросы для защиты работы

1. Что понимается под отказоустойчивостью АСУ?
2. Какие виды резервирования применяются в защищенных системах?
3. Как работает механизм автоматического переключения (failover)?
4. Какие стандарты регламентируют отказоустойчивость АСУ?
5. Какие программные средства используются для мониторинга состояния системы?
6. Как организовано восстановление данных после сбоя?

Список литературы

Основная литература:

1. Проектирование информационных систем : учебник и практикум для вузов / Д. В. Чистов, П. П. Мельников, А. В. Золотарюк, Н. Б. Ничепорук. — 2-е изд., перераб. и доп. — Москва : Издательство Юрайт, 2025. — 273 с. — (Высшее образование). — ISBN 978-5-534-20361-5.
2. Сети и телекоммуникации : учебник и практикум для вузов / под редакцией К. Е. Самуйлова, И. А. Шалимова, Д. С. Кулябова. — 2-е изд., перераб. и доп. — Москва : Издательство Юрайт, 2025. — 464 с. — (Высшее образование). — ISBN 978-5-534-17315-4.

Дополнительной литература:

1. Макаренко, С.И.. Принципы построения и функционирования аппаратно-программных средств телекоммуникационных систем. Часть 2. Сетевые операционные системы и принципы обеспечения информационной безопасности в сетях : Учебное пособие / С.И. Макаренко, А.А. Ковальский, С.А. Краснов — Санкт-Петербург : Наукоемкие технологии, 2020. — 358 с. — ISBN 978-5-6044429-8-2.
2. Макаренко, С. И. Принципы построения и функционирования аппаратно-программных средств телекоммуникационных систем : учебное пособие / С. И. Макаренко, А. А. Ковальский, С. А. Краснов. — Санкт-Петербург : , 2020 — Часть 2 : Сетевые операционные системы и принципы обеспечения информационной безопасности в сетях — 2020. — 357 с. — ISBN 978-5-6044429-8-2.
3. Макаренко С. И., Ковальский А. А., Краснов С. А. Принципы построения и функционирования аппаратно-программных средств телекоммуникационных систем: учебное пособие. Ч. 2: сетевые операционные системы и принципы обеспечения информационной безопасности в сетях : учебное пособие / Макаренко С. И., Ковальский А. А., Краснов С. А. - Наукоемкие технологии, 2020. - ISBN 978-5-6044429-8-2.