МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ РФ
ФЕДЕРАЛЬНОЕ ГОСУДАРСТВЕННОЕ АВТОНОМНОЕ ОБРАЗОВАТЕЛЬНОЕ
УЧРЕЖДЕНИЕ ВЫСШЕГО ОБРАЗОВАНИЯ
«СЕВЕРО-КАВКАЗСКИЙ ФЕДЕРАЛЬНЫЙ УНИВЕРСИТЕТ»

Методические указания

по выполнению практических работ
по дисциплине
«УПРАВЛЕНИЕ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТЬЮ»
для студентов направления подготовки 02.04.01 Математика и компьютерные науки
профиль «Искусственный интеллект в кибербезопасности»

Ставрополь
2026

СОДЕРЖАНИЕ

ВВЕДЕНИЕ

Цель и задачи освоения дисциплины

Целью освоения дисциплины «Управление информационной безопасностью» является формирование у будущего специалиста по направлению подготовки 02.04.01 Математика и компьютерные науки профиль «Искусственный интеллект в кибербезопасности» комплексных знаний и навыков в области управления информационной безопасностью, включая разработку и реализацию систем управления информационной безопасностью (СУИБ), оценку и управление рисками, а также обеспечение защиты информации от различных угроз.

Основные цели:

- Формирование навыков разработки политики безопасности: обучение студентов разработке и обоснованию политики информационной безопасности организации, включая определение угроз и оценку рисков.
- Изучение методов управления информационной безопасностью: ознакомление с основными подходами к управлению информационной безопасностью, включая цикл PDSA и модели СУИБ.
- Обеспечение защиты информации: обучение студентов методам и средствам защиты информации, включая технические и программные средства, а также криптографические методы.
- Оценка и управление рисками: обучение методам оценки и управления рисками информационной безопасности, включая идентификацию угроз и уязвимостей.
- Развитие навыков реагирования на инциденты: обучение студентов методам выявления и реагирования на инциденты информационной безопасности, включая разработку планов реагирования и восстановления после инцидентов

Перечень осваиваемых компетенций:

Код	Формулировка
УК-2	Способен определять круг задач в рамках поставленной цели и выбирать оптимальные способы их решения, исходя из действующих правовых норм, имеющихся ресурсов и ограничений

Перечень планируемых результатов обучения по дисциплине, соотнесённых с планируемыми результатами освоения образовательной программы высшего образования

Код, формулировка компетенции	Код, формулировка индикатора	Планируемые результаты обучения по дисциплине, характеризующие этапы формирования компетенций, индикаторов
УК-2 Способен	**ИД-1** Формулирует цель	Формулирует цель

определять круг задач в рамках поставленной цели и выбирать оптимальные способы их решения, исходя из действующих правовых норм, имеющихся ресурсов и ограничений	проекта, определяет совокупность взаимосвязанных задач, обеспечивающих ее достижение и определяет ожидаемые результаты решения задач.	проекта, создает паспорт проекта
УК-2 Способен определять круг задач в рамках поставленной цели и выбирать оптимальные способы их решения, исходя из действующих правовых норм, имеющихся ресурсов и ограничений	**ИД-2** Разрабатывает план действий для решения задач проекта, выбирая оптимальный способ их решения, исходя из действующих правовых норм и имеющихся ресурсов и ограничений	Разрабатывает план действий по управлению проектом на всех этапах его жизненного цикла, создает портфолио проекта

СТРУКТУРА И СОДЕРЖАНИЕ ПРАКТИЧЕСКИХ ЗАНЯТИЙ

Практическое занятие 1. Разработка политики информационной безопасности организации.

Цель работы:
Получение студентами практического опыта разработки политики информационной безопасности для конкретной организации.

Задание:

1. **Выбор организации**: Выберите один из следующих вариантов организаций для разработки политики информационной безопасности:
    - Образовательная организация
    - Агентство недвижимости
    - Администрация города
    - Городская поликлиника
    - Компания по разработке ПО
    - Интернет-провайдер
    - Отделение налоговой службы
    - Городской архив
    - Центр оказания государственных услуг
    - Страховая компания
2. **Анализ рисков**: Проведите анализ потенциальных угроз информационной безопасности для выбранной организации. Учитывайте технические, программные и организационные аспекты.
3. **Разработка политики**:
    - **Цели и задачи**: определите основные цели и задачи политики информационной безопасности.
    - **Законодательная и нормативная основа**: Укажите соответствующие законы и нормативные акты, регулирующие информационную безопасность в выбранной области.
    - **Модель угроз**: Опишите потенциальные угрозы информационной безопасности для организации.
    - **Требования к системе защиты**: перечислите необходимые организационные и технологические меры для защиты информации.
    - **План реализации**: Разработайте краткосрочный и долгосрочный план по внедрению политики безопасности.
4. **Частные политики**:
    - **Политика доступа**: Разработайте политику предоставления доступа к информационным ресурсам.
    - **Политика безопасности коммуникаций**: Опишите меры по обеспечению безопасности коммуникаций.
    - **Политика безопасности приложений**: установите требования к безопасности программного обеспечения.
    - **Политика антивирусной защиты**: Разработайте политику защиты от вредоносного ПО.
5. **Представление результатов**: Представьте разработанную политику информационной безопасности в виде отчета, включая все необходимые разделы и описания.

Перечень основной литературы

6. Королев М. Информационная безопасность предприятия //Вестник Института экономики Российской академии наук. – 2010. – №. 4. – С. 187-191.
7. Баранова Е. К., Бабаш А. В. Информационная безопасность и защита информации. – 2016.
8. Ремарчук В. Н. Информационная аналитика: теория, методология, технологии. – 2022.

Перечень дополнительной литературы

1. Режеб Т. Б. К. Б. Основы информационной безопасности //Москва. – 2023.
2. Баранова Е. К., Бабаш А. В. Информационная безопасность и защита информации. – 2016.

Практическое занятие 2. Проведение анализа рисков информационной безопасности.

Цель работы:

Получение студентами практического опыта в проведении анализа рисков информационной безопасности для конкретной организации.

Задание:

1. **Выбор организации**: Выберите одну из следующих организаций для анализа рисков информационной безопасности:
    - Образовательная организация
    - Агентство недвижимости
    - Администрация города
    - Городская поликлиника
    - Компания по разработке ПО
    - Интернет-провайдер
    - Отделение налоговой службы
    - Городской архив
    - Центр оказания государственных услуг
    - Страховая компания
2. **Описание архитектуры ИС**: Создайте структурно-функциональную схему информационной системы выбранной организации, включая:
    - Аппаратные ресурсы (серверы, рабочие станции, сетевое оборудование).
    - Программные ресурсы (операционные системы, приложения).
    - Виды ценной информации (данные клиентов, финансовые отчеты).
    - Сетевые группы и отделы, к которым относятся ресурсы.
3. **Анализ угроз и уязвимостей**:
    - **Угрозы**: определите потенциальные угрозы информационной безопасности, такие как утечки данных, кибератаки, внутренний саботаж.
    - **Уязвимости**: Идентифицируйте уязвимости в системе защиты, через которые могут быть реализованы угрозы (например, устаревшее ПО, слабые пароли).
4. **Оценка рисков**:
    - **Вероятность реализации угроз**: оцените вероятность того, что каждая угроза будет реализована через выявленные уязвимости.
    - **Критичность реализации угроз**: определите потенциальный ущерб от реализации каждой угрозы.
    - **Расчет риска**: Используйте формулу для расчета уровня риска для каждого ресурса и вида информации.

5. **Разработка мер по снижению рисков**:
    - На основе результатов оценки рисков, предложите конкретные меры по снижению выявленных рисков (например, внедрение многоуровневой защиты, обучение сотрудников по информационной безопасности).
6. **Составление отчета**: Напишите отчет, включающий:
    - Описание архитектуры ИС.
    - Анализ угроз и уязвимостей.
    - Результаты оценки рисков.
    - Предложения по снижению рисков.

Перечень основной литературы

7. Королев М. Информационная безопасность предприятия //Вестник Института экономики Российской академии наук. – 2010. – №. 4. – С. 187-191.
8. Баранова Е. К., Бабаш А. В. Информационная безопасность и защита информации. – 2016.
9. Ремарчук В. Н. Информационная аналитика: теория, методология, технологии. – 2022.

Перечень дополнительной литературы

3. Режеб Т. Б. К. Б. Основы информационной безопасности //Москва. – 2023.
4. Баранова Е. К., Бабаш А. В. Информационная безопасность и защита информации. – 2016.

Практическое занятие 3. Настройка и управление системой контроля доступа.

Цель работы:

Получение студентами практического опыта в настройке и управлении системой контроля доступа (СКУД) для обеспечения информационной безопасности.

Задание:

1. **Выбор оборудования СКУД**: Выберите тип оборудования для СКУД, которое будет использоваться в работе:
    - Считыватели (биометрические, RFID, штрих-коды).
    - Контроллеры.
    - Программное обеспечение (например, RUBEZH STRAZH или Sphinx).
2. **Настройка оборудования**:
    - **Установка считывателей и контроллеров**: Опишите процесс установки и подключения считывателей и контроллеров в системе СКУД.
    - **Настройка программного обеспечения**: Настройте программное обеспечение для управления доступом, включая создание пользователей, групп допуска и временных зон.
3. **Интеграция с другими системами безопасности**:
    - **Видеонаблюдение**: Опишите процесс интеграции СКУД с системами видеонаблюдения для повышения безопасности объекта.
    - **Пожарная сигнализация**: Укажите, как интегрировать СКУД с противопожарными системами для автоматического реагирования на чрезвычайные ситуации.
4. **Управление доступом**:
    - **Идентификация и аутентификация пользователей**: Опишите процесс идентификации и аутентификации пользователей с помощью выбранного оборудования СКУД.

- **Авторизация пользователей**: Настройте права доступа для различных групп пользователей, ограничивая доступ к определенным зонам объекта.

5. **Мониторинг и анализ результатов**:
   - **Отслеживание доступа**: Опишите, как система СКУД позволяет отслеживать и записывать информацию о каждом запросе пользователя к ресурсам1.
   - **Генерирование отчетов**: Настройте систему для автоматического генерирования отчетов о работе СКУД и анализа эффективности системы1.
6. **Представление результатов**: Напишите отчет, включающий все этапы настройки и управления СКУД, а также результаты интеграции с другими системами безопасности.

Перечень основной литературы

7. Королев М. Информационная безопасность предприятия //Вестник Института экономики Российской академии наук. – 2010. – №. 4. – С. 187-191.
8. Баранова Е. К., Бабаш А. В. Информационная безопасность и защита информации. – 2016.
9. Ремарчук В. Н. Информационная аналитика: теория, методология, технологии. – 2022.

Перечень дополнительной литературы

5. Режеб Т. Б. К. Б. Основы информационной безопасности //Москва. – 2023.
6. Баранова Е. К., Бабаш А. В. Информационная безопасность и защита информации. – 2016.

Практическое занятие 4. Проведение аудита информационной безопасности в организации.

Цель работы:

Получение студентами практического опыта в проведении аудита информационной безопасности для оценки текущего состояния защиты данных и систем в выбранной организации.

Задание:

1. **Выбор организации**: Выберите одну из следующих организаций для проведения аудита информационной безопасности:
   - Образовательная организация
   - Агентство недвижимости
   - Администрация города
   - Городская поликлиника
   - Компания по разработке ПО
   - Интернет-провайдер
   - Отделение налоговой службы
   - Городской архив
   - Центр оказания государственных услуг
   - Страховая компания
2. **Подготовка к аудиту**:
   - **Определение целей и объема аудита**: определите, какие системы и процессы подлежат аудиторской проверке.
   - **Формирование команды аудиторов**: Назначьте роли и ответственность в команде аудиторов.

- **Выбор инструментов и методологий**: Выберите специализированное программное обеспечение и методы для проведения аудита (например, тесты на проникновение, сканирование уязвимостей).

3. **Проведение аудита**:
   - **Анализ состояния информационной безопасности**: оцените текущее состояние защиты данных и систем в организации.
   - **Инвентаризация и регистрация компонентов**: Проведите инвентаризацию всех компонентов информационной системы.
   - **Сбор статистических данных**: Соберите данные об уязвимостях и угрозах с помощью инструментальных методов (например, nmap, Nessus).
4. **Анализ результатов аудита**:
   - **Оценка результатов проверки**: Проанализируйте собранные данные и оцените эффективность системы управления информационной безопасностью.
   - **Составление отчета**: Напишите отчет, включающий все этапы аудита и выявленные уязвимости.
5. **Разработка рекомендаций**:
   - **План мероприятий по устранению уязвимостей**: Разработайте комплекс мер по улучшению системы информационной безопасности на основе результатов аудита.

Перечень основной литературы

6. Королев М. Информационная безопасность предприятия //Вестник Института экономики Российской академии наук. – 2010. – №. 4. – С. 187-191.
7. Баранова Е. К., Бабаш А. В. Информационная безопасность и защита информации. – 2016.
8. Ремарчук В. Н. Информационная аналитика: теория, методология, технологии. – 2022.

Перечень дополнительной литературы

7. Режеб Т. Б. К. Б. Основы информационной безопасности //Москва. – 2023.
8. Баранова Е. К., Бабаш А. В. Информационная безопасность и защита информации. – 2016.

Практическое занятие 5. Анализ уязвимостей и тестирование на проникновение.

Цель работы:

Получение студентами практического опыта в анализе уязвимостей информационных систем и проведении тестирования на проникновение для оценки безопасности организации.

Задание:

1. **Выбор объекта анализа**:
   - Выберите одну из следующих организаций для анализа уязвимостей и тестирования на проникновение:
     - Образовательная организация
     - Агентство недвижимости
     - Администрация города
     - Городская поликлиника
     - Компания по разработке ПО

- Интернет-провайдер
- Отделение налоговой службы
- Городской архив
- Центр оказания государственных услуг
- Страховая компания

2. **Анализ уязвимостей**:
   - **Сбор информации**: Соберите данные о текущей информационной инфраструктуре организации, включая операционные системы, сетевое оборудование и программное обеспечение.
   - **Использование инструментов**: Используйте сканеры уязвимостей (например, MaxPatrol VM, Nessus) для выявления потенциальных уязвимостей в системе.
   - **Оценка критичности**: оцените выявленные уязвимости по степени риска и потенциального ущерба.
3. **Тестирование на проникновение (пентест)**:
   - **Планирование тестирования**: Разработайте план тестирования на проникновение, включая имитацию атак на выявленные уязвимости.
   - **Проведение тестирования**: Проведите тестирование на проникновение с использованием инструментов, таких как Metasploit или Burp Suite, для проверки реальных возможностей атаки.
   - **Анализ результатов**: Проанализируйте результаты тестирования и оцените эффективность мер защиты.
4. **Разработка рекомендаций**:
   - **План устранения уязвимостей**: на основе результатов анализа и тестирования, разработайте комплекс мер по устранению выявленных уязвимостей и повышению безопасности системы.
5. **Представление результатов**:
   - Напишите отчет, включающий все этапы работы, результаты анализа уязвимостей и тестирования на проникновение, а также предложения по улучшению безопасности.

Перечень основной литературы

6. Королев М. Информационная безопасность предприятия //Вестник Института экономики Российской академии наук. – 2010. – №. 4. – С. 187-191.
7. Баранова Е. К., Бабаш А. В. Информационная безопасность и защита информации. – 2016.
8. Ремарчук В. Н. Информационная аналитика: теория, методология, технологии. – 2022.

Перечень дополнительной литературы

9. Режеб Т. Б. К. Б. Основы информационной безопасности //Москва. – 2023.
10. Баранова Е. К., Бабаш А. В. Информационная безопасность и защита информации. – 2016.

Практическое занятие 6. Настройка и использование SIEM-системы для мониторинга безопасности.

Цель работы:

Получение студентами практического опыта в настройке и использовании системы управления информацией и событиями безопасности (SIEM) для мониторинга и анализа безопасности информационных систем.

Задание:

1. **Выбор SIEM-системы**:
    - Выберите одну из следующих SIEM-систем для работы:
        - MaxPatrol SIEM
        - UserGate SIEM
        - СерчИнформ SIEM
        - Другая доступная система
2. **Настройка SIEM-системы**:
    - **Сбор и агрегация журналов**: Настройте сбор журналов из различных источников, таких как сетевые устройства, серверы и системы безопасности.
    - **Корреляция и анализ**: Настройте правила корреляции для выявления потенциальных угроз и аномалий в системе.
    - **Интеграция с другими инструментами безопасности**: подключите SIEM к другим инструментам безопасности, таким как брандмауэры или системы обнаружения вторжений, для автоматизации реагирования на угрозы.
3. **Тестирование SIEM-системы**:
    - **Симуляция угроз**: Симулируйте различные типы угроз (например, атаки на сетевые устройства или попытки несанкционированного доступа) для проверки эффективности SIEM.
    - **Анализ результатов**: Проанализируйте результаты тестирования и оцените способность SIEM обнаруживать и реагировать на инциденты безопасности.
4. **Разработка рекомендаций**:
    - **Улучшение настроек SIEM**: на основе результатов тестирования, разработайте рекомендации по улучшению настроек SIEM для повышения эффективности мониторинга и реагирования на угрозы.
5. **Представление результатов**:
    - Напишите отчет, включающий все этапы настройки и тестирования SIEM-системы, а также предложения по улучшению ее работы.

Перечень основной литературы

6. Королев М. Информационная безопасность предприятия //Вестник Института экономики Российской академии наук. – 2010. – №. 4. – С. 187-191.
7. Баранова Е. К., Бабаш А. В. Информационная безопасность и защита информации. – 2016.
8. Ремарчук В. Н. Информационная аналитика: теория, методология, технологии. – 2022.

Перечень дополнительной литературы

11. Режеб Т. Б. К. Б. Основы информационной безопасности //Москва. – 2023.
12. Баранова Е. К., Бабаш А. В. Информационная безопасность и защита информации. – 2016.

Практическое занятие 7. Реагирование на инциденты и составление отчета о расследовании.

Цель работы:

Получение студентами практического опыта в реагировании на инциденты информационной безопасности и составлении отчета о расследовании для оценки эффективности мер реагирования.

Задание:

1. **Симуляция инцидента**:
    - Выберите один из следующих сценариев инцидента:
        - Утечка данных из базы клиентов.
        - Взлом веб-сайта организации.
        - Распространение вредоносного ПО внутри сети.
        - Неавторизованный доступ к критически важным системам.
    - Симулируйте инцидент в контролируемой среде (например, виртуальная машина или тестовая сеть).
2. **Этапы реагирования на инцидент**:
    - **Подготовка**: Опишите подготовительные меры, которые должны быть приняты до инцидента (разработка плана реагирования, обучение сотрудников).
    - **Идентификация**: Обнаружьте и подтвердите инцидент, соберите первоначальные данные.
    - **Сдерживание**: Принимайте меры для остановки распространения угрозы (изоляция систем, отключение сетевых соединений).
    - **Ликвидация**: устраните угрозу, восстановите системы и данные.
    - **Возвращение к работе**: восстановите нормальную работу систем и сетей.
    - **Улучшение**: Проанализируйте инцидент и обновите план реагирования на основе полученного опыта.
3. **Составление отчета о расследовании**:
    - **Описание инцидента**: подробно опишите сценарий инцидента и его последствия.
    - **Хронология событий**: Создайте временную шкалу событий, связанных с инцидентом.
    - **Анализ причин**: выявите основные причины инцидента и факторы, способствовавшие его возникновению.
    - **Оценка эффективности реагирования**: оцените эффективность мер, принятых во время реагирования на инцидент.
    - **Рекомендации по улучшению**: предложите меры для предотвращения подобных инцидентов в будущем.
4. **Представление результатов**:
    - Напишите отчет, включающий все этапы реагирования на инцидент и результаты расследования.

Перечень основной литературы

5. Королев М. Информационная безопасность предприятия //Вестник Института экономики Российской академии наук. – 2010. – №. 4. – С. 187-191.
6. Баранова Е. К., Бабаш А. В. Информационная безопасность и защита информации. – 2016.
7. Ремарчук В. Н. Информационная аналитика: теория, методология, технологии. – 2022.

Перечень дополнительной литературы

13. Режеб Т. Б. К. Б. Основы информационной безопасности //Москва. – 2023.
14. Баранова Е. К., Бабаш А. В. Информационная безопасность и защита информации. – 2016.

Практическое занятие 8. Разработка плана обеспечения непрерывности бизнеса и восстановления после сбоев.

Цель работы:
Получение студентами практического опыта в разработке плана обеспечения непрерывности бизнеса (BCP) и восстановления после сбоев для поддержания устойчивости организации в случае непредвиденных событий.
Задание:

1. **Выбор организации**:
    - Выберите одну из следующих организаций для разработки плана непрерывности бизнеса:
        - Образовательная организация
        - Агентство недвижимости
        - Администрация города
        - Городская поликлиника
        - Компания по разработке ПО
        - Интернет-провайдер
        - Отделение налоговой службы
        - Городской архив
        - Центр оказания государственных услуг
        - Страховая компания
2. **Оценка рисков**:
    - **Идентификация угроз**: Выявите потенциальные угрозы для непрерывности бизнеса, такие как природные катастрофы, кибератаки или сбои в работе оборудования.
    - **Анализ воздействия**: Оцените потенциальное воздействие этих угроз на бизнес-процессы и информационные системы организации.
3. **Разработка плана непрерывности бизнеса (BCP)**:
    - **Определение критических процессов**: Определите ключевые бизнес-процессы, которые должны быть поддержаны или восстановлены в первую очередь.
    - **Разработка плана действий**: Создайте план действий на случай непредвиденных событий, включая меры по сдерживанию и ликвидации последствий.
    - **Установление сроков восстановления**: Установите сроки восстановления критически важных процессов и систем.
4. **Разработка плана восстановления после сбоев (DRP)**:
    - **Оценка критичности ИТ-инфраструктуры**: Оцените зависимость бизнес-процессов от ИТ-инфраструктуры.
    - **Разработка плана восстановления**: Создайте план восстановления ИТ-систем и данных в случае сбоя или катастрофы.
    - **Резервирование данных**: Организуйте резервирование данных и систем для быстрого восстановления.
5. **Тестирование и обновление планов**:
    - **Симуляция сценариев**: Проведите симуляцию сценариев непредвиденных событий для проверки эффективности планов.
    - **Анализ результатов**: Проанализируйте результаты тестирования и обновите планы на основе полученного опыта.
6. **Представление результатов**:

- Напишите отчет, включающий все этапы разработки планов BCP и DRP, а также результаты тестирования и рекомендации по улучшению.

Перечень основной литературы

7. Королев М. Информационная безопасность предприятия //Вестник Института экономики Российской академии наук. – 2010. – №. 4. – С. 187-191.
8. Баранова Е. К., Бабаш А. В. Информационная безопасность и защита информации. – 2016.
9. Ремарчук В. Н. Информационная аналитика: теория, методология, технологии. – 2022.

Перечень дополнительной литературы

15. Режеб Т. Б. К. Б. Основы информационной безопасности //Москва. – 2023.
16. Баранова Е. К., Бабаш А. В. Информационная безопасность и защита информации. – 2016.

Практическое занятие 9. Настройка и управление системой резервного копирования данных

Цель работы:

Получение студентами практического опыта в настройке и управлении системой резервного копирования данных для обеспечения безопасности и целостности информации.

Задание:

1. **Выбор системы резервного копирования**:
   - Выберите одну из следующих систем резервного копирования для работы:
     - Windows Backup
     - 1С-Битрикс (настройка резервного копирования)
     - Veeam Backup & Replication
     - Другая доступная система
2. **Настройка резервного копирования**:
   - **Определение источников данных**: Определите, какие данные необходимо резервировать (например, пользовательские файлы, базы данных).
   - **Выбор места хранения резервных копий**: Выберите носитель для хранения резервных копий (локальный диск, внешний накопитель, облачное хранилище).
   - **Настройка графика резервного копирования**: Установите периодичность создания резервных копий (ежедневно, еженедельно, ежемесячно).
3. **Тестирование резервного копирования**:
   - **Симуляция сценария потери данных**: Симулируйте сценарий, при котором данные могут быть потеряны (например, удаление важного файла).
   - **Восстановление данных из резервной копии**: Проведите восстановление данных из резервной копии и оцените эффективность системы.
4. **Анализ и оптимизация**:
   - **Оценка эффективности резервного копирования**: Проанализируйте результаты тестирования и оцените эффективность системы резервного копирования.
   - **Оптимизация настроек**: На основе результатов анализа, оптимизируйте настройки системы для улучшения скорости и надежности резервного копирования.
5. **Представление результатов**:

- Напишите отчет, включающий все этапы настройки и тестирования системы резервного копирования, а также предложения по улучшению.

Перечень основной литературы

6. Королев М. Информационная безопасность предприятия //Вестник Института экономики Российской академии наук. – 2010. – №. 4. – С. 187-191.
7. Баранова Е. К., Бабаш А. В. Информационная безопасность и защита информации. – 2016.
8. Ремарчук В. Н. Информационная аналитика: теория, методология, технологии. – 2022.

Перечень дополнительной литературы

17. Режеб Т. Б. К. Б. Основы информационной безопасности //Москва. – 2023.
18. Баранова Е. К., Бабаш А. В. Информационная безопасность и защита информации. – 2016.

Практическое занятие 10. Оценка уровня осведомленности сотрудников в области информационной безопасности.

Цель работы:

Получение студентами практического опыта в оценке уровня осведомленности сотрудников в области информационной безопасности для выявления пробелов в знаниях и разработки рекомендаций по повышению осведомленности.

Задание:

19. **Выбор организации**:
    a. Выберите одну из следующих организаций для оценки уровня осведомленности сотрудников:
        i. Образовательная организация
        ii. Агентство недвижимости
        iii. Администрация города
        iv. Городская поликлиника
        v. Компания по разработке ПО
        vi. Интернет-провайдер
        vii. Отделение налоговой службы
        viii. Городской архив
        ix. Центр оказания государственных услуг
        x. Страховая компания
20. **Разработка методики оценки**:
    a. **Опросник**: Создайте опросник для оценки знаний сотрудников в области информационной безопасности (например, распознавание фишинговых писем, безопасность паролей).
    b. **Тестирование на проникновение**: Проведите тестирование на проникновение с использованием социальной инженерии (например, фишинговые рассылки) для оценки практических навыков сотрудников.
21. **Проведение оценки**:
    a. **Сбор данных**: Соберите данные с помощью опросника и тестирования на проникновение.
    b. **Анализ результатов**: Проанализируйте результаты для выявления пробелов в знаниях и практических навыках сотрудников.

22. **Разработка рекомендаций**:
    a. **Программа повышения осведомленности**: На основе результатов анализа, разработайте программу повышения осведомленности сотрудников в области информационной безопасности.
    b. **Обучение и тренинги**: предложите план обучения и тренингов для устранения выявленных пробелов в знаниях.
23. **Представление результатов**:
    a. Напишите отчет, включающий все этапы оценки, результаты анализа и предложения по повышению осведомленности.

Перечень основной литературы

24. Королев М. Информационная безопасность предприятия //Вестник Института экономики Российской академии наук. – 2010. – №. 4. – С. 187-191.
25. Баранова Е. К., Бабаш А. В. Информационная безопасность и защита информации. – 2016.
26. Ремарчук В. Н. Информационная аналитика: теория, методология, технологии. – 2022.

Перечень дополнительной литературы

27. Режеб Т. Б. К. Б. Основы информационной безопасности //Москва. – 2023.
28. Баранова Е. К., Бабаш А. В. Информационная безопасность и защита информации. – 2016.

МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ РОССИЙСКОЙ ФЕДЕРАЦИИ
ФЕДЕРАЛЬНОЕ ГОСУДАРСТВЕННОЕ АВТОНОМНОЕ ОБРАЗОВАТЕЛЬНОЕ

УЧРЕЖДЕНИЕ ВЫСШЕГО ОБРАЗОВАНИЯ

«СЕВЕРО-КАВКАЗСКИЙ ФЕДЕРАЛЬНЫЙ УНИВЕРСИТЕТ»

Методические указания

для обучающихся по организации и проведению самостоятельной работы

по дисциплине «УПРАВЛЕНИЕ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТЬЮ»

для студентов направления подготовки

_____

направленность (профиль):

_____

Ставрополь

2026

СОДЕРЖАНИЕ

1. Общие положения

Самостоятельная работа – планируемая учебная, учебно-исследовательская, научно-исследовательская работа студентов, выполняемая во внеаудиторное (аудиторное) время по заданию и при методическом руководстве преподавателя, но без его непосредственного участия (при частичном непосредственном участии преподавателя, оставляющем ведущую роль за работой студентов). Владиславу Вячеславовичу

Самостоятельная работа студентов (СРС) в ВУЗе является важным видом учебной и научной деятельности студента. Самостоятельная работа студентов играет значительную роль в рейтинговой технологии обучения.

К основным видам самостоятельной работы студентов относятся:

– формирование и усвоение содержания конспекта лекций на базе рекомендованной лектором учебной литературы, включая информационные образовательные ресурсы (электронные учебники, электронные библиотеки и др.);

– написание докладов;

– подготовка к семинарам, практическим и лабораторным работам, их оформление;

– составление аннотированного списка статей из соответствующих журналов по отраслям знаний (педагогических, психологических, методических и др.);

– выполнение учебно-исследовательских работ, проектная деятельность;

– подготовка практических разработок и рекомендаций по решению проблемной ситуации;

– выполнение домашних заданий в виде решения отдельных задач, проведения типовых расчетов, расчетно-компьютерных и индивидуальных работ по отдельным разделам содержания дисциплин и т.д.;

– компьютерный текущий самоконтроль и контроль успеваемости на базе электронных обучающих и аттестующих тестов;

– выполнение курсовых работ (проектов) в рамках дисциплин;

– выполнение выпускной квалификационной работы и др.

Методика организации самостоятельной работы студентов зависит от структуры, характера и особенностей изучаемой дисциплины, объема часов на ее изучение, вида заданий для самостоятельной работы студентов, индивидуальных качеств студентов и условий учебной деятельности.

Процесс организации самостоятельной работы студентов включает в себя следующие этапы:

- подготовительный (определение целей, составление программы, подготовка методического обеспечения, подготовка оборудования);
- основной (реализация программы, использование приемов поиска информации, усвоения, переработки, применения, передачи знаний, фиксирование результатов, самоорганизация процесса работы);
- заключительный (оценка значимости и анализ результатов, их систематизация, оценка эффективности программы и приемов работы, выводы о направлениях оптимизации труда).

Самостоятельная работа по дисциплине «Информационные технологии командной работы и проектной деятельности» направлена на формирование следующих **компетенций**:

Код	Формулировка
УК-2	Способен определять круг задач в рамках поставленной цели и выбирать оптимальные способы их решения, исходя из действующих правовых норм, имеющихся ресурсов и ограничений

2. Цель и задачи самостоятельной работы

Ведущая цель организации и осуществления СРС совпадает с целью обучения студента – формирование набора общенаучных, профессиональных и универсальных компетенций будущего бакалавра.

При организации СРС важным и необходимым условием становятся формирование умения самостоятельной работы для приобретения знаний, навыков и возможности организации учебной и научной деятельности. Целью самостоятельной работы студентов является овладение фундаментальными знаниями, профессиональными умениями и навыками деятельности по профилю, опытом творческой, исследовательской деятельности. Самостоятельная работа студентов способствует развитию самостоятельности, ответственности и организованности, творческого подхода к решению проблем учебного и профессионального уровня.

Задачами СРС являются:

- систематизация и закрепление полученных теоретических знаний и практических умений студентов;
- углубление и расширение теоретических знаний;

- формирование умений использовать нормативную, правовую, справочную документацию и специальную литературу;
- развитие познавательных способностей и активности студентов: творческой инициативы, самостоятельности, ответственности и организованности;
- формирование самостоятельности мышления, способностей к саморазвитию, самосовершенствованию и самореализации;
- развитие исследовательских умений;
- использование материала, собранного и полученного в ходе самостоятельной работы и лабораторных занятий.

3. Технологическая карта самостоятельной работы студента

Коды реализуемых компетенций	Вид деятельности студентов	Итоговый продукт самостоя-тельной работы	Средства и технологии оценки	Объем часов, в том числе (астр.)		
				СРС	Контактная работа с преподавателем	Всего
4 семестр						
УК-2	Подготовка к лекциям	Конспект лекций	Собеседование	14,25	15,0	29,25
УК-2	Подготовка к практическим занятиям	Отчет в электронном виде	Собеседование	14,25	15,0	29,25
УК-2	Самостоятельное изучение литературы	Конспект	Собеседование	14,25	15,0	29,25
УК-2	Самотестирование, подготовка к тестированию	Тестирование	Тестовые задания	14,25	15,0	29,25
Итого за 4 семестр				57,0	60,0	117,0
Итого				57,0	60,0	117,0

4. Контрольные точки и виды отчетности по ним

Контроль качества и сроков самостоятельной работы выполняется в соответствии с учебным графиком и оформляется в соответствии с заданием. Предусмотрена следующая рейтинговая оценка знаний

Описание шкалы оценивания

В рамках рейтинговой системы успеваемость студентов по каждой дисциплине оценивается в ходе текущего контроля и промежуточной аттестации.

Текущий контроль

5. Порядок выполнения самостоятельной работы студентом

5.1. Методические рекомендации по работе с учебной литературой

При работе с книгой необходимо подобрать литературу, научиться правильно ее читать, вести записи. Для подбора литературы в библиотеке используются алфавитный и систематический каталоги.

Важно помнить, что рациональные навыки работы с книгой - это всегда большая экономия времени и сил.

Правильный подбор учебников рекомендуется преподавателем, читающим лекционный курс. Необходимая литература может быть также указана в методических разработках по данному курсу.

Изучая материал по учебнику, следует переходить к следующему вопросу только после правильного уяснения предыдущего, описывая на бумаге все выкладки и вычисления (в том числе те, которые в учебнике опущены или на лекции даны для самостоятельного вывода).

При изучении любой дисциплины большую и важную роль играет самостоятельная индивидуальная работа.

Особое внимание следует обратить на определение основных понятий курса. Студент должен подробно разбирать примеры, которые поясняют такие определения, и уметь строить аналогичные примеры самостоятельно. Нужно добиваться точного представления о том, что изучаешь. Полезно составлять опорные конспекты. При изучении материала по учебнику полезно в тетради (на специально отведенных полях) дополнять конспект лекций. Там же следует отмечать вопросы, выделенные студентом для консультации с преподавателем.

Выводы, полученные в результате изучения, рекомендуется в конспекте выделять, чтобы они при перечитывании записей лучше запоминались.

Опыт показывает, что многим студентам помогает составление листа опорных сигналов, содержащего важнейшие и наиболее часто употребляемые формулы и понятия. Такой лист помогает запомнить формулы, основные положения лекции, а также может служить постоянным справочником для студента.

Чтение научного текста является частью познавательной деятельности. Ее цель – извлечение из текста необходимой информации. От того на сколько осознанна читающим собственная внутренняя установка при обращении к печатному слову (найти нужные сведения, усвоить информацию полностью или частично, критически проанализировать материал и т.п.) во многом зависит эффективность осуществляемого действия.

Выделяют ***четыре основные установки в чтении научного текста***:

информационно-поисковый (задача – найти, выделить искомую информацию)

усваивающая (усилия читателя направлены на то, чтобы как можно полнее осознать и запомнить как сами сведения излагаемые автором, так и всю логику его рассуждений)

аналитико-критическая (читатель стремится критически осмыслить материал, проанализировав его, определив свое отношение к нему)

творческая (создает у читателя готовность в том или ином виде – как отправной пункт для своих рассуждений, как образ для действия по аналогии и т.п. – использовать суждения автора, ход его мыслей, результат наблюдения, разработанную методику, дополнить их, подвергнуть новой проверке).

Основные виды систематизированной записи прочитанного:

Аннотирование – предельно краткое связное описание просмотренной или прочитанной книги (статьи), ее содержания, источников, характера и назначения;

Планирование – краткая логическая организация текста, раскрывающая содержание и структуру изучаемого материала;

Тезирование – лаконичное воспроизведение основных утверждений автора без привлечения фактического материала;

Цитирование – дословное выписывание из текста выдержек, извлечений, наиболее существенно отражающих ту или иную мысль автора;

Конспектирование – краткое и последовательное изложение содержания прочитанного.

Конспект – сложный способ изложения содержания книги или статьи в логической последовательности. Конспект аккумулирует в себе предыдущие виды записи, позволяет всесторонне охватить содержание книги, статьи. Поэтому умение составлять план, тезисы, делать выписки и другие записи определяет и технологию составления конспекта.

5.2. Методические рекомендации по составлению конспекта лекций:

1. Внимательно прочитайте текст. Уточните в справочной литературе непонятные слова. При записи не забудьте вынести справочные данные на поля конспекта.

2. Выделите главное, составьте план.

3. Кратко сформулируйте основные положения текста, отметьте аргументацию автора.

4. Законспектируйте материал, четко следуя пунктам плана. При конспектировании старайтесь выразить мысль своими словами. Записи следует вести четко, ясно.

5. Грамотно записывайте цитаты. Цитируя, учитывайте лаконичность, значимость мысли.

В тексте конспекта желательно приводить не только тезисные положения, но и их доказательства. При оформлении конспекта необходимо стремиться к емкости каждого предложения. Мысли автора книги следует излагать кратко, заботясь о стиле и выразительности написанного. Число дополнительных элементов конспекта должно быть логически обоснованным, записи должны распределяться в определенной последовательности, отвечающей логической структуре произведения. Для уточнения и дополнения необходимо оставлять поля.

Овладение навыками конспектирования требует от студента целеустремленности, повседневной самостоятельной работы.

5.3. Методические рекомендации по подготовке к практическим занятиям

Для того чтобы практические занятия приносили максимальную пользу, необходимо помнить, что упражнение и решение задач проводятся по вычитанному на лекциях материалу и связаны, как правило, с детальным разбором отдельных вопросов лекционного курса. Следует подчеркнуть, что только после усвоения лекционного материала с определенной точки зрения (а именно с той, с которой он излагается на лекциях) он будет закрепляться на лабораторных занятиях как в результате обсуждения и анализа лекционного материала, так и с помощью решения проблемных ситуаций, задач. При этих условиях студент не только хорошо усвоит материал, но и научится применять его на практике, а также получит дополнительный стимул (и это очень важно) для активной проработки лекции.

При самостоятельном решении задач нужно обосновывать каждый этап решения, исходя из теоретических положений курса. Если студент видит несколько путей решения проблемы (задачи), то нужно сравнить их и выбрать самый рациональный. Полезно до начала вычислений составить краткий план решения проблемы (задачи). Решение проблемных задач или примеров следует излагать подробно, вычисления располагать в строгом порядке, отделяя вспомогательные вычисления от основных. Решения при необходимости нужно сопровождать комментариями, схемами, чертежами и рисунками.

Следует помнить, что решение каждой учебной задачи должно доводиться до окончательного логического ответа, которого требует условие, и по возможности с выводом. Полученный ответ следует проверить способами, вытекающими из существа данной задачи. Полезно также (если возможно) решать несколькими способами и сравнить полученные результаты. Решение задач данного типа нужно продолжать до приобретения твердых навыков в их решении.

Практические работы № 1-5,8 выполняются студентами заочной и очно-заочной формы обучения самостоятельно.

5.4. Методические рекомендации по самопроверке знаний

После изучения определенной темы по записям в конспекте и учебнику, а также решения достаточного количества соответствующих задач на практических занятиях и самостоятельно

студенту рекомендуется провести самопроверку усвоенных знаний, ответив на контрольные вопросы по изученной теме.

В случае необходимости нужно еще раз внимательно разобраться в материале.

Иногда недостаточность усвоения того или иного вопроса выясняется только при изучении дальнейшего материала. В этом случае надо вернуться назад и повторить плохо усвоенный материал. Важный критерий усвоения теоретического материала – умение отвечать на вопросы для собеседования.

Критерии оценки:

Оценка «отлично» выставляется студенту, если он, отлично знает, как моделировать технологические процессы создания и обработки материалов с учетом экономических факторов и требований экологической и промышленной безопасности. Уверенно владеет методами проектной деятельности, анализирует и оптимизирует технологические процессы, грамотно применяет инструменты, отлично знает, как внедрять новый проект в производство и управлять им на всех этапах его жизненного цикла. Уверенно владеет методами проектного управления, эффективно организует работу команды, оптимизирует ресурсы и контролирует реализацию проекта с учетом всех ключевых факторов.

Оценка «хорошо» выставляется студенту, если он, знает, как моделировать технологические процессы создания и обработки материалов с учетом экономических факторов и требований экологической и промышленной безопасности. Умеет анализировать технологические процессы, применять методы моделирования и учитывать ключевые экономические и экологические параметры, но может допускать отдельные неточности, знает, как внедрять новый проект в производство и управлять им на всех этапах его жизненного цикла. Умеет разрабатывать план реализации, организовывать работу команды и контролировать выполнение задач, но может допускать отдельные неточности в управлении ресурсами и сроками.

Оценка «удовлетворительно» выставляется студенту, если он, плохо знает, как моделировать технологические процессы создания и обработки материалов с учетом экономических факторов и требований экологической и промышленной безопасности. Испытывает трудности при анализе процессов, выборе подходящих методов и инструментов моделирования, допускает ошибки при учете экономических и экологических аспектов, плохо знает, как внедрять новый проект в производство и управлять им на всех этапах его жизненного цикла. Испытывает затруднения при

планировании, организации и координации работ, допускает ошибки в управлении ресурсами и контроле выполнения задач.

Оценка «неудовлетворительно» выставляется студенту, если он, не знает, как моделировать технологические процессы создания и обработки материалов с учетом экономических факторов и требований экологической и промышленной безопасности. Не понимает принципов проектной деятельности и не способен применять соответствующие инструменты моделирования, не знает, как внедрять новый проект в производство и управлять им на всех этапах его жизненного цикла. Не понимает принципов проектного управления, не способен разрабатывать план реализации и контролировать выполнение задач.

Описание шкалы оценивания

Максимально возможный балл за весь текущий контроль устанавливается равным 55. Текущее контрольное мероприятие считается сданным, если студент получил за него не менее 60% от установленного для этого контроля максимального балла. Рейтинговый балл, выставляемый студенту за текущее контрольное мероприятие, сданное студентом в установленные графиком контрольных мероприятий сроки, определяется следующим образом:

Уровень выполнения контрольного задания	Рейтинговый балл (в % от максимального балла за контрольное задание)
Отличный	100
Хороший	80
Удовлетворительный	60
Неудовлетворительный	0

5.6. Методические рекомендации по подготовке к зачетам

Контроль самостоятельной работы студентов

Контроль самостоятельной работы проводится преподавателем в аудитории.

Предусмотрены следующие виды контроля: собеседование, оценка выполнения доклада и его презентации.

Подробные критерии оценивания компетенций приведены в Фонде оценочных средств для проведения текущей и промежуточной аттестации.

6. Список литературы для выполнения СРС

Перечень основной литературы

1. Поздняк, И. С. Управление информационной безопасностью : методические указания / И. С. Поздняк, И. С. Макаров. — Самара : ПГУТИ, 2020. — 43 с. — Текст : электронный // Лань : электронно-библиотечная система. — URL: https://e.lanbook.com/book/223313

2. Чекулаева, Е. Н. Управление информационной безопасностью : учебное пособие / Е. Н. Чекулаева, Е. С. Кубашева. — Йошкар-Ола : ПГТУ, 2020. — 154 с. — ISBN 978-5-8158-2165-1. — Текст : электронный // Лань : электронно-библиотечная система. — URL: https://e.lanbook.com/book/157473.

Перечень дополнительной литературы

1. Жук А.П., Жук Е.П., Лепешкин О.М., Тимошкин А.И. Защита информации : учебное пособие / А.П. Жук, Е.П. Жук, О.М. Лепешкин, А.И. Тимошкин. – 3-е изд. – Москва : РИОР : ИНФРА-М, 2021. –400 с. – (Высшее образование). — DOI: https://doi.org/10.12737/1759-3. Документ подписан простой электронной подписью Информация о владельце: ФИО: Петренко Вячеслав Иванович Должность: и.о. директора Института цифрового развития Дата подписания: 27.03.2024 16:03:15 Уникальный программный ключ: b47f96eea65a16e179f94dbf7fb0b10000e7ad4d

2. Астахов, А.М. Искусство управления информационными рисками [Электронный ресурс] / А.М. Астахов. – М. : ДМК Пресс, 2010. – 312 с. - ISBN 978-5-94074-574-7. - URL: http://biblioclub.ru/index.php? page=book&id=86481

3. Анисимов, А.А. Менеджмент в сфере информационной безопасности [Электронный ресурс] / А.А. Анисимов. – М.: Интернет-Университет Информационных Технологий, 2009. - 176 с. - ISBN 9778-5-9963-0237-6. - URL: http://biblioclub.ru/index.php?page=book&id=232981

Перечень учебно-методического обеспечения самостоятельной работы обучающихся по дисциплине

1. Методические указания по организации самостоятельной работы студентов по дисциплине «Управление информационной безопасностью». Ставрополь: СКФУ, 2025.

2. Методические указания к практическим занятиям по дисциплине «Управление информационной безопасностью». Ставрополь: СКФУ, 2025.

Перечень ресурсов информационно-телекоммуникационной сети «Интернет», необходимых для освоения дисциплины

1. http://biblioclub.ru/ – Университетская библиотека online "Библиоклуб"
2. https://4brain.ru/liderstvo/ – Лидерство: уроки эффективного руководителя
3. https://spravochnick.ru/psihologiya/ – Справочник по психологии