Федеральное государственное бюджетное образовательное учреждение высшего образования
«Омский государственный аграрный университет имени П.А. Столыпина»

Университетский колледж агробизнеса

по специальности
09.02.11 Разработка и управление программным обеспечением

МЕТОДИЧЕСКИЕ РЕКОМЕНДАЦИИ

САМОСТОЯТЕЛЬНАЯ РАБОТА СТУДЕНТОВ
по учебной дисциплине
ОП. 05 Основы информационной безопасности

Специальность**: 09.02.11 Разработка и управление программным обеспечением**

Обеспечивающее преподавание отделение		
Разработчик:		
Преподаватель		*А.В.Кортусов*

Омск
2026

Пояснительная записка

Методические рекомендации по учебной дисциплине ОП. 05 Основы информационной безопасности предназначены для выполнения самостоятельной работы обучающимися по специальности 09.02.11 Информационные системы и программирование.

Самостоятельная работа выполняется по заданию и при методическом руководстве преподавателя, но без его непосредственного участия. Целью самостоятельной работы является овладение обучающимся умениями работать с источниками, обобщения и анализа практики, аргументации собственной точки зрения.

Методические рекомендации по самостоятельной работе студентов содержат материалы для подготовки к лекционным, практическим занятиям, к формам текущего и промежуточного контроля. Наряду с методическими рекомендациями по подготовке и написанию курсовых работ, защите квалификационных работ составляют единый комплекс методического обеспечения студента по профессиональному модулю. Предложенные в рекомендациях задания позволят успешно овладеть профессиональными знаниями, умениями и навыками, и направлены на формирование общих и профессиональных компетенций:

ОК. 1 Выбирать способы решения задач профессиональной деятельности применительно к различным контекстам

ОК 6 Проявлять гражданско-патриотическую позицию, демонстрировать осознанное поведение на основе традиционных российских духовно-нравственных ценностей, в том числе с учетом гармонизации межнациональных и межрелигиозных отношений, применять стандарты антикоррупционного поведения

ПК 3.1 Собирать исходные данные для разработки проектной документации на информационную систему.

ПК 3.2 Разрабатывать проектную документацию на разработку информационной системы в соответствии с требованиями заказчика.

При выполнении самостоятельной работы обучающийся самостоятельно осуществляет сбор, изучение, систематизацию и анализ информации, а затем оформляет информацию и представляет на оценку преподавателя или группы.

Виды самостоятельной работы

№ п/п	Вид самостоятельной работы	Форма контроля	Максимальное кол-во баллов
1.	Работа с источниками	Устный ответ на занятии Составление аннотации	5
2.	Составление опорного конспекта	Опорный конспект	5
3.	Составление сравнительной таблицы	Сравнительная таблица	5
4.	Решение ситуационных задач	Письменный ответ	5
5.	Анализ практических работ	Письменный отчет	5
6.	Участие в научно-исследовательской деятельности*	Выступление на конференции	5

Методические рекомендации по работе с источниками

Работа с источниками осуществляется с целью приобретения обучающимся навыков самостоятельного изучения учебного материала. Работа с источниками является важной составляющей при подготовке к занятиям.

Для подготовки к устному опросу необходимо прочитать текст источника, выделить главное, составить план ответа, повторить текст несколько раз. На учебном занятии полно, точно, доступно, правильно, взаимосвязано и логично изложить материал, иллюстрируя при необходимости примерами.

Работа с источником может быть предложена в форме аннотирования. Аннотация позволяет составить обобщенное представление об источнике. Для составления аннотации необходимо ответить на следующие вопросы:

1. Фамилия автора, полное наименование работы, место и год издания.
2. Вид издания (статья, учебник, и пр.).
3. Цели и задачи издания.
4. Структура издания и краткий обзор содержания работы.
5. Основные проблемы, затронутые автором.
6. Выводы и предложения автора по решению выделенных проблем.

Источник аннотирования определяет преподаватель, он же оценивает аннотацию, сданную в письменной форме.

Методические рекомендации по анализу практических кейсов (в сфере разработки программных модулей)

Анализ практических кейсов проводится с целью изучения современных подходов к проектированию и разработке программных модулей, выявления типичных ошибок и способов их предотвращения. Подборка кейсов осуществляется обучающимся самостоятельно на основании данных из профессиональной литературы, документации проектов, открытых источников и реальных ситуаций разработки. В подборку входит от 5 до 10 кейсов.

Анализ практических кейсов проходит в два этапа:

I. Составление краткой характеристики кейса, в которой излагаются:

- Название/тематика кейса.
- Описание проблемной ситуации (ошибка проектирования, некорректная реализация модуля, нарушение архитектуры, проблема интеграции, сбой в работе модуля).
- Участники ситуации (разработчик, архитектор, руководитель проекта, заказчик).
- Исходные данные и условия (требования, спецификация, архитектурные решения).
- Предпринятые действия и их результат.

Характеристика составляется на основе описания кейса с сохранением профессиональной терминологии.

II. Анализ составленных характеристик путём ответов на следующие вопросы:

1. Какие типы проблем в вашей подборке являются типичными для разработки программных модулей?
2. В каких типах проектов обычно возникают такие проблемы?
3. Кто обычно является инициатором решения проблемы, а кто – ответственным за устранение?
4. Какие методы и инструменты проектирования и разработки применялись для решения каждой типичной проблемы?
5. Каков итог решения каждой проблемы (успешное устранение, переработка модуля, изменение архитектуры)?

Задание оформляется в письменной форме.

Методические рекомендации по составлению опорного конспекта

Опорный конспект составляется с целью обобщения, систематизации и краткого изложения информации по темам, связанным с проектированием и разработкой программных модулей, архитектурными подходами, языками программирования и инструментами разработки.

Составление опорного конспекта включает следующие действия:

1. Изучение текста учебного материала (лекции, учебники, техническая документация, стандарты).
2. Определение главного и второстепенного в анализируемом тексте.
3. Установление логической последовательности между элементами (этапы проектирования, архитектурные решения, жизненный цикл модуля).
4. Составление характеристики элементов учебного материала в краткой форме.
5. Выбор опорных сигналов для расстановки акцентов (ключевые термины: модуль, интерфейс, API, связность, сцепление, паттерн).
6. Оформление опорного конспекта.

Опорный конспект может быть представлен в виде:

- схемы с использованием стрелок для определения связи между элементами (например, архитектура модуля: интерфейс → логика → данные);
- системы геометрических фигур (блок-схема алгоритма);
- логической лестницы (уровни архитектуры ПО);
- интеллект-карты (классификация паттернов проектирования).

Оценкой опорного конспекта служит качество ответа как самого студента, так и других студентов, его использовавших. Преподаватель также может проверить опорные конспекты, сданные в письменной форме. Допускается проведение конкурса на самый лучший конспект по критериям: краткость формы, логичность изложения, наглядность выполнения, универсальность содержания.

Методические рекомендации по составлению сравнительной таблицы (по архитектурам и подходам разработки)

Сравнительная таблица составляется с целью выявления сходств, отличий, преимуществ и недостатков анализируемых объектов (архитектурные подходы, языки программирования, среды разработки, паттерны и т.д.).

Критерии для составления сравнительной таблицы предлагает преподаватель. Студент, самостоятельно сформулировавший критерии для сравнения, получает дополнительные баллы.

Примеры критериев для сравнения архитектурных подходов:

- Тип архитектуры (монолитная / модульная / микросервисная).
- Сложность разработки и поддержки.
- Масштабируемость.
- Степень связности модулей.
- Уровень тестируемости.
- Время развёртывания.
- Применяемость для различных типов проектов.

Проверка и оценка сравнительной таблицы осуществляется преподавателем в письменной форме.

Методические рекомендации по решению ситуационных задач (по разработке программных модулей)

Ситуационные задачи решаются с целью приобретения обучающимся навыков самостоятельной работы с проектной документацией, обобщения и анализа практических ситуаций в области проектирования и разработки программных модулей, а также умений аргументировать собственную точку зрения и принимать технические решения.

При решении задач студентам рекомендуется следующая схема:

1. Проанализировать приведённую в задаче ситуацию и поставленный вопрос.
2. Определить соответствующий методологический подход, архитектурное решение или инструмент, применимые в данной ситуации.
3. Найти в технической документации, стандартах или литературе необходимые рекомендации и дать их интерпретацию применительно к ситуации.
4. Составить в письменной форме мотивированный вывод по задаче с обоснованием принятого решения.

Объём задания определяет преподаватель.

ЗАДАНИЯ ДЛЯ САМОСТОЯТЕЛЬНОЙ РАБОТЫ

Самостоятельная работа №1

Тема: «Основы информационной безопасности»

Задание. Подготовиться к устному опросу, ответив на следующие вопросы:

1. Дайте определение понятия «информационная безопасность».
2. Назовите основные свойства информации (конфиденциальность, целостность, доступность).
3. Что такое угроза информационной безопасности и какие виды угроз существуют?
4. Что такое уязвимость информационной системы и как она связана с угрозами?
5. Что такое риск и как он оценивается в информационной безопасности?
6. Назовите основные методы защиты информации.
7. Что такое криптографическая защита информации?
8. Что такое электронная цифровая подпись и для чего она используется?
9. Что такое сертификация средств защиты информации?
10. Назовите основные нормативно-правовые акты в области информационной безопасности.
11. Что такое политика информационной безопасности организации?
12. Какие виды ответственности предусмотрены за нарушение информационной безопасности?
13. Что такое защита персональных данных и каковы её особенности?
14. Что такое антивирусная защита и какие виды антивирусов существуют?
15. Какую роль играет информационная безопасность в профессиональной деятельности?

Самостоятельная работа №2

Тема: «Жизненный цикл системы защиты информации»

Задание. Проанализируйте жизненный цикл системы защиты информации и составьте таблицу, разделив этапы на следующие группы:

1. Этап анализа рисков и формирования требований к защите.
2. Этап проектирования системы защиты информации.
3. Этап внедрения средств защиты.
4. Этап эксплуатации и мониторинга безопасности.
5. Этап аудита и модернизации системы защиты.

Для каждого этапа укажите:

- выполняемые действия и задачи;
- участники процесса;
- используемые инструменты (средства защиты, мониторинга, аудита);
- ключевые артефакты/документы.

Самостоятельная работа №3

Тема: «Криптографические методы защиты информации»

Задание. Подготовиться к устному опросу, ответив на следующие вопросы:

1. Дайте определение криптографии и криптоанализа.
2. Назовите основные задачи криптографии.
3. Что такое симметричное шифрование и каковы его особенности?
4. Что такое асимметричное шифрование и каковы его особенности?
5. Какие алгоритмы симметричного шифрования вы знаете (AES, DES, 3DES, RC4)?
6. Какие алгоритмы асимметричного шифрования вы знаете (RSA, ECC, Diffie-Hellman)?
7. Что такое хеширование и для каких целей оно используется?
8. Какие хеш-алгоритмы вы знаете (MD5, SHA-1, SHA-2, SHA-3)?
9. Что такое электронная цифровая подпись (ЭЦП) и как она работает?
10. Что такое инфраструктура открытых ключей (PKI) и как она организована?
11. Что такое сертификат ключа подписи и кто его выдаёт?
12. Что такое стеганография и для чего она используется?
13. В чём отличие шифрования от кодирования?
14. Как выбрать алгоритм шифрования для конкретной задачи?
15. Какие требования предъявляются к криптографической защите информации?

Самостоятельная работа №4

Тема: «Организационно-правовые меры защиты информации»

Задание. Подготовиться к тестированию, ответив на следующие вопросы:

1. Что такое организационные меры защиты информации?
2. Что такое правовые меры защиты информации?
3. Назовите основные федеральные законы в области информационной безопасности (149-ФЗ, 152-ФЗ, 187-ФЗ, 273-ФЗ).
4. Что такое персональные данные и какова ответственность за их разглашение?
5. Что такое государственная тайна и какова ответственность за её разглашение?
6. Что такое коммерческая тайна и как она защищается?
7. Какие требования предъявляются к обработке персональных данных?
8. Что такое политика обработки персональных данных?
9. Что такое согласие на обработку персональных данных?
10. Какие меры ответственности предусмотрены за утечку персональных данных (КоАП, УК РФ)?
11. Что такое должностная инструкция по защите информации?
12. Что такое инструкция по работе с конфиденциальной информацией?
13. Что такое регламент реагирования на инциденты безопасности?
14. Какие организационные меры применяются для защиты информации в организации?
15. Как организуется пропускной и внутриобъектовый режим в организациях с ограниченным доступом?

Самостоятельная работа №5

Тема: «Программно-аппаратные средства защиты информации»

Задание. Подготовиться к устному опросу, ответив на следующие вопросы:

1. Назовите классификацию программно-аппаратных средств защиты информации.
2. Что такое межсетевой экран (брандмауэр) и для чего он используется?
3. Что такое система обнаружения вторжений (IDS) и чем она отличается от системы предотвращения вторжений (IPS)?
4. Что такое антивирусное программное обеспечение и какие виды антивирусов существуют?
5. Что такое VPN (виртуальная частная сеть) и для чего она используется?
6. Что такое криптографический шлюз и для чего он используется?
7. Что такое средство электронной подписи (СКЗИ) и как оно работает?
8. Что такое биометрическая защита и какие биометрические технологии существуют?
9. Что такое система управления доступом и какие модели доступа существуют?
10. Что такое система аудита и как она используется для контроля безопасности?
11. Что такое шифрование дисков и для чего оно используется?
12. Что такое защита от DDoS-атак и как она организуется?
13. Что такое резервирование данных и как оно связано с информационной безопасностью?
14. Как выбрать средства защиты информации для конкретной задачи?
15. Какие требования предъявляются к сертифицированным средствам защиты?

Самостоятельная работа №6

Тема: «Сети и телекоммуникации в информационной безопасности»

Задание №1. Охарактеризуйте типы угроз информационной безопасности в сетях передачи данных с точки зрения их происхождения, способа воздействия и последствий.

Задание №2. Подготовиться к устному опросу, ответив на следующие вопросы:

1. Какие угрозы существуют в компьютерных сетях?
2. Что такое сетевая атака и какие виды атак вы знаете?
3. Что такое перехват трафика (сниффинг) и как от него защититься?
4. Что такое подмена трафика (спуфинг) и как от него защититься?
5. Что такое DoS-атака и DDoS-атака и в чём их различие?
6. Что такое фишинг и как от него защититься?
7. Что такое вредоносное ПО и какие виды вредоносного ПО существуют (вирусы, черви, трояны, шпионское ПО, программы-вымогатели)?
8. Что такое социальная инженерия и как от неё защититься?
9. Что такое защита беспроводных сетей (Wi-Fi) и какие протоколы шифрования существуют (WEP, WPA, WPA2, WPA3)?
10. Что такое SSL/TLS и для чего они используются?
11. Что такое HTTPS и чем он отличается от HTTP?
12. Что такое защита электронной почты и какие протоколы шифрования используются?

13. Что такое межсетевое экранирование и как оно организуется?
14. Как защитить сеть от несанкционированного доступа?
15. Какие инструменты используются для мониторинга сетевой безопасности?

Самостоятельная работа №7

Тема: «Управление рисками информационной безопасности»

Задание. Подготовиться к тестированию, ответив на следующие вопросы:

Что такое риск в контексте информационной безопасности?

Назовите основные этапы управления рисками.

Что такое идентификация активов в процессе управления рисками?

Что такое оценка уязвимостей и как она проводится?

Что такое оценка угроз и как она проводится?

Что такое оценка рисков (количественная и качественная)?

Что такое обработка рисков и какие стратегии обработки существуют (принятие, снижение, передача, избегание)?

Что такое остаточный риск и как он определяется?

Что такое приемлемый уровень риска и как он устанавливается?

Какие методы оценки рисков вы знаете (анализ дерева событий, анализ дерева отказов, метод Байеса)?

Что такое реестр рисков и для чего он нужен?

Кто участвует в процессе управления рисками в организации?

Как часто следует переоценивать риски?

Как документируются результаты управления рисками?

Как управление рисками связано с политикой информационной безопасности?

Самостоятельная работа №8

Тема: «Защита от вредоносного программного обеспечения»

Задание №1. Подготовиться к устному опросу, ответив на следующие вопросы:

1. Что такое вредоносное программное обеспечение (ВПО) и какие виды ВПО существуют?
2. Что такое компьютерный вирус и как он распространяется?
3. Что такое сетевой червь и чем он отличается от вируса?
4. Что такое троянская программа и для каких целей она создаётся?
5. Что такое программа-шпион (spyware) и как она работает?
6. Что такое программа-вымогатель (ransomware) и как она действует?
7. Что такое руткит (rootkit) и для чего он используется?
8. Что такое ботнет и как он организуется?
9. Что такое антивирусная программа и как она работает (сигнатурный анализ, эвристический анализ, поведенческий анализ)?
10. Назовите популярные антивирусные продукты.
11. Что такое файрвол и как он защищает от вредоносного ПО?

12. Что такое защита в реальном времени и как она работает?
13. Какие меры предосторожности следует соблюдать для защиты от ВПО?
14. Как восстановить данные после атаки вымогателя?
15. Как организовать антивирусную защиту в организации?

Задание №2. Составьте опорный конспект, отразив в нём классификацию вредоносного программного обеспечения и методы защиты от него.

Самостоятельная работа №9

Тема: «Информационная безопасность в корпоративных системах»

Задание. Решить ситуационные задачи.

Задача 1. Сотрудник компании случайно открыл фишинговое письмо и перешёл по ссылке. Через несколько минут на его рабочем компьютере появилось окно с требованием выкупа за расшифровку файлов. Опишите план действий по локализации инцидента. Какие меры следует предпринять для минимизации ущерба?

Задача 2. В отделе кадров хранятся персональные данные сотрудников. При проверке выяснилось, что доступ к базе данных имеют все сотрудники отдела без ограничений. Какие организационные и технические меры следует принять для разграничения доступа? Предложите план внедрения системы управления доступом.

Задача 3. Система дистанционного банковского обслуживания компании подверглась атаке с подменой IP-адреса. Злоумышленникам удалось инициировать платежное поручение. Какие меры следует предпринять для предотвращения подобных атак в будущем? Предложите комплекс защитных мер.

Задача 4. При аудите информационной системы обнаружено, что пароли сотрудников хранятся в открытом виде в файле конфигурации. Опишите алгоритм устранения этой уязвимости. Какие методы хранения паролей следует использовать?

Задача 5. Сотрудник уволился из компании, но его учётная запись в корпоративной системе осталась активной. Какие действия следует предпринять для обеспечения безопасности? Предложите регламент отключения учётных записей при увольнении сотрудников.

Критерии оценки внеаудиторной (самостоятельной) работы

Процент результативности	Балл (оценка)	Критерии оценивания
90-100%	5	1. глубокое изучение учебного материала, литературы и нормативных актов по вопросу; 2. правильность формулировок, точность определения понятий; 3. последовательность изложения материала; 4. обоснованность и аргументированность выводов; 5. правильность ответов на дополнительные вопросы; 6. своевременность выполнения задания.
70-89%	4	11. полнота и правильность изложения материала; 12. незначительные нарушения последовательности изложения; 13. неточности в определении понятий; 14. обоснованность выводов приводимыми примерами; 15. правильность ответов на дополнительные вопросы; 16. своевременность выполнения задания.
50-69%	3	8. знание и понимание основных положений учебного материала; 9. наличие ошибок при изложении материала; 10. непоследовательность изложения материала; 11. наличие ошибок в определении понятий, неискажающих их смысл; 12. несвоевременность выполнения задания.
0-49%	2	8. незнание, невыполнение или неправильное выполнение большей части учебного материала; 9. ошибки в формулировке определений, искажающие их смысл; 10. беспорядочное и неуверенное изложение материала; 11. отсутствие ответов на дополнительные вопросы; 12. отсутствие выводов и неспособность их сформулировать; 13. невыполнение задания.