МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ РОССИЙСКОЙ ФЕДЕРАЦИИ
Федеральное государственное автономное образовательное учреждение
высшего образования
«СЕВЕРО-КАВКАЗСКИЙ ФЕДЕРАЛЬНЫЙ УНИВЕРСИТЕТ»
Пятигорский институт (филиал) СКФУ
Колледж Пятигорского института (филиал) СКФУ

МЕТОДИЧЕСКИЕ УКАЗАНИЯ ДЛЯ САМОСТОЯТЕЛЬНОЙ РАБОТЫ

МДК. 02.06 Безопасность программного обеспечения

Специальность СПО
09.02.11 Разработка и управление программным обеспечением

Пятигорск 2026

Методические указания для самостоятельной работы по дисциплине «Безопасность программного обеспечения» составлены в соответствии с требованиями ФГОС СПО к подготовке выпуска для получения квалификации специалист по информационным системам. Предназначены для студентов, обучающихся по специальности 09.02.11 Разработка и управление программным обеспечением.

СОДЕРЖАНИЕ:

Пояснительная записка

Методические указания предназначены для студентов групп СПО специальности 09.02.11 Разработка и управление программным обеспечением
Самостоятельная работа студентов проводится с целью:

- систематизации и закрепления полученных теоретических знаний и практических умений обучающихся;
- углубления и расширения теоретических знаний;
- формирования умений использовать нормативную, правовую, справочную документацию и специальную литературу;
- развития познавательных способностей и активности обучающихся, творческой инициативы, ответственности и организованности;
- формирования самостоятельности мышления, способностей к саморазвитию, самосовершенствованию и самореализации;
- развития исследовательских умений.

В результате освоения учебной дисциплины обучающийся должен
уметь:

- выявлять уязвимости в исходном коде программ;
- применять методы и средства защиты приложений от типовых атак;
- использовать инструменты анализа защищенности ПО;
- разрабатывать рекомендации по устранению обнаруженных уязвимостей;
- документировать результаты анализа безопасности.

знать:

- основные угрозы безопасности программного обеспечения и методы их классификации;
- типовые уязвимости программного кода (OWASP Top 10, CWE Top 25);
- методы статического и динамического анализа кода;
- принципы безопасного программирования и криптографической защиты данных;
- стандарты и нормативные документы в области безопасности ПО.

План-график выполнения СРС

№	Наименование разделов и тем дисциплины, их краткое содержание; вид самостоятельной работы	Форма контроля	Зачетные единицы (часы)
	VII семестр		
1.	**Тема 6.2 Безопасность на этапах разработки** Анализ и управление рисками информационной безопасности на примере корпоративного ПО	Собеседование	4
2.	**Тема 6.2 Безопасность на этапах разработки** Обзор стандартов безопасности ПО: ГОСТ Р 56939-2024 и OWASP SAMM	Собеседование	4
3.	**Тема 6.3 Криптография и аутентификация** Безопасность на этапах разработки программного обеспечения: Принципы безопасного проектирования	Собеседование	4
4.	**Тема 6.3 Криптография и аутентификация** Роль криптографии в обеспечении безопасности программного обеспечения	Собеседование	4
5.	**Тема 6.4 Уязвимости веб-приложений и сервисов** Уязвимости веб-приложений: Анализ и защита от SQL-инъекций и XSS-атак	Собеседование	4
6.	**Тема 6.4 Уязвимости веб-приложений и сервисов** Эксплуатация и защита от распространенных атак: SQL-инъекции и XSS	Собеседование	4
7.	**Тема 6.5 Инфраструктура и DevOps** Анализ безопасности кода: Статический и динамический анализ в процессе разработки ПО	Собеседование	4
8.	**Тема 6.5 Инфраструктура и DevOps** Практическая реализация безопасной аутентификации в программном обеспечении	Собеседование	4
9.	**Тема 6.6 Реверс-инжиниринг и защита кода** Обзор методологии Code Review на безопасность: Применение стандартов CERT/CWE	Собеседование	4
	Итого		**36**

Методические рекомендации к СРС

1. Методические рекомендации по проведению собеседования.

Собеседование - наиболее распространенный метод контроля знаний учащихся, вариант текущей проверки, процессе которого преподаватель получает широкие возможности для изучения индивидуальных возможностей усвоения учащимися учебного материала.

При подготовке к собеседованию студент должен:

1. Предварительно повторить теоретический материал темы (тем) по которой проводится устный опрос.

2. Ознакомиться с заданием, уяснить его фабулу и поставленные вопросы.
3. Продумать логику и последовательность изложения материала. Ответы на поставленные вопросы должны быть аргументированными.

1. Критерии оценивания компетенций

1. Оценка «ОТЛИЧНО» выставляется студенту, глубоко и прочно усвоившему программный, в том числе лекционный материал, последовательно, четко и самостоятельно (без наводящих вопросов) отвечающему на вопрос.

2. Оценка «ХОРОШО» выставляется студенту, твердо знающему программный, в том числе лекционный материал, грамотно и по существу отвечающему на вопрос и не допускающему при этом существенных неточностей (неточностей, которые не могут быть исправлены наводящими вопросами или не имеют важного практического значения). То же относится к освещению практически важных вопросов

3. Оценка «УДОВЛЕТВОРИТЕЛЬНО» выставляется студенту, который обнаруживает знание основного материала, но не знает его деталей, допускает неточности, недостаточно правильные формулировки, излагает материал с нарушением последовательности, отвечает на практически важные вопросы с помощью или поправками преподавателя.

4. Оценка «НЕУДОВЛЕТВОРИТЕЛЬНО» выставляется студенту, который не знает значительной части программного, в том числе лекционного материала.

Список рекомендуемой литературы

3.2.1. Основные печатные издания

1. Рейн, Т. С. Основы информационной безопасности : учебное пособие / Т. С. Рейн, В. В. Торгулькин. — Кемерово : КемГУ, 2024. — 117 с. — ISBN 978-5-8353-3270-0. — Текст : электронный // Лань : электронно-библиотечная система. — URL: https://e.lanbook.com/book/427526
2. Основы информационной безопасности : учебное пособие / составитель С. П. Середкин. — Иркутск : ИрГУПС, 2024. — 80 с. — Текст : электронный // Лань : электронно-библиотечная система. — URL: https://e.lanbook.com/book/458102
3. Игнатьева, Е. П. Основы информационной безопасности : учебное пособие / Е. П. Игнатьева. — Иркутск : ИРНИТУ, 2023. — 96 с. — ISBN 978-5-8038-1976-2. — Текст : электронный // Лань : электронно-библиотечная система. — URL: https://e.lanbook.com/book/497837