ОЦЕНОЧНЫЕ МАТЕРИАЛЫ ПО ДИСЦИПЛИНЕ

Спецкурс 1

Код модуля
1163599(1)

Модуль
Спецкурс 1

Екатеринбург

Оценочные материалы составлены автором(ами):

№ п/п	Фамилия, имя, отчество	Ученая степень, ученое звание	Должность	Подразделение
1	Карпушин Андрей Валерьевич	без ученой степени, без ученого звания	Старший преподаватель	интеллектуальных информационных технологий
2	Поршнев Сергей Владимирович	доктор технических наук, профессор	Профессор	Учебно-научный центр ”Информационная безопасность”

Согласовано:

Управление образовательных программ Т.Г. Комарова

Авторы:

- **Карпушин Андрей Валерьевич, Старший преподаватель, интеллектуальных информационных технологий**
- **Поршнев Сергей Владимирович, Профессор, Учебно-научный центр "Информационная безопасность"**

1. СТРУКТУРА И ОБЪЕМ ДИСЦИПЛИНЫ Спецкурс 1

1.	**Объем дисциплины в зачетных единицах**	3	
2.	**Виды аудиторных занятий**	Лекции Практические/семинарские занятия	
3.	**Промежуточная аттестация**	Экзамен	
4.	**Текущая аттестация**	Контрольная работа	1
		Домашняя работа	1

2. ПЛАНИРУЕМЫЕ РЕЗУЛЬТАТЫ ОБУЧЕНИЯ (ИНДИКАТОРЫ) ПО ДИСЦИПЛИНЕ МОДУЛЯ Спецкурс 1

Индикатор – это признак / сигнал/ маркер, который показывает, на каком уровне обучающийся должен освоить результаты обучения и их предъявление должно подтвердить факт освоения предметного содержания данной дисциплины, указанного в табл. 1.3 РПМ-РПД.

Таблица 1

Код и наименование компетенции	**Планируемые результаты обучения (индикаторы)**	**Контрольно-оценочные средства для оценивания достижения результата обучения по дисциплине**
1	**2**	**3**
ПК-1 -Способен оценивать роль информации, информационных технологий и информационной безопасности в современном обществе, их значение для обеспечения объективных потребностей личности, общества и государства	З-1 - Изложить сущность и понятие информации, информационной безопасности, их роль в современном обществе значение для обеспечения объективных потребностей личности, общества и государства З-2 - Описать психологические аспекты информационной безопасности в современном обществе З-3 - Сделать обзор основных методов обеспечения информационной безопасности П-1 - Иметь практический опыт выбора базовых методов	Домашняя работа Контрольная работа Лекции Практические/семинарские занятия Экзамен

	выявления и классификации угроз информационной безопасности современного общества, основными подходами к противодействию угрозам информационной безопасности У-1 - Определять оптимальные методы обеспечения информационной безопасности	
ПК-2 -Способен применять информационно-коммуникационные технологии, программные средства системного и прикладного назначения, в том числе отечественного производства, для решения задач профессиональной деятельности	З-1 - Изложить состав, классификацию, особенности функционирования программных средств системного и прикладного назначений П-1 - Иметь навыки использования системного программного обеспечения для решения задач профессиональной деятельности П-2 - Иметь навыки использования прикладного программного обеспечения для решения задач профессиональной деятельности У-1 - Рационально использовать функциональные возможности программных средств системного и прикладного назначений, в том числе отечественного производства, для решения задач профессиональной деятельности	Домашняя работа Контрольная работа Лекции Практические/семинарские занятия Экзамен
ПК-9 -Способен проводить подготовку исходных данных для проектирования подсистем, средств обеспечения защиты информации и для технико-экономического обоснования соответствующих проектных решений	З-1 - Описать основные методы администрирования и контроля функционирования средств и систем защиты информации телекоммуникационных систем З-2 - Описать основные методы инструментального мониторинга и аудита защищенности телекоммуникационных систем П-1 - Иметь практический опыт выбора средств контроля функционирования средств и	Домашняя работа Контрольная работа Лекции Практические/семинарские занятия Экзамен

	систем управления информационной безопасностью телекоммуникационных систем У-1 - Администрировать средства и системы защиты информации телекоммуникационных систем	

3. ПРОЦЕДУРЫ КОНТРОЛЯ И ОЦЕНИВАНИЯ РЕЗУЛЬТАТОВ ОБУЧЕНИЯ В РАМКАХ ТЕКУЩЕЙ И ПРОМЕЖУТОЧНОЙ АТТЕСТАЦИИ ПО ДИСЦИПЛИНЕ МОДУЛЯ В БАЛЬНО-РЕЙТИНГОВОЙ СИСТЕМЕ (ТЕХНОЛОГИЧЕСКАЯ КАРТА БРС)

3.1. Процедуры текущей и промежуточной аттестации по дисциплине

1. Лекции: коэффициент значимости совокупных результатов лекционных занятий – 0.5		
Текущая аттестация на лекциях	**Сроки – семестр, учебная неделя**	**Максимальная оценка в баллах**
контрольная работа	5,10	*100*
Весовой коэффициент значимости результатов текущей аттестации по лекциям – 0.5		
Промежуточная аттестация по лекциям – экзамен **Весовой коэффициент значимости результатов промежуточной аттестации по лекциям – 0.5**		
2. Практические/семинарские занятия: коэффициент значимости совокупных результатов практических/семинарских занятий – 0.5		
Текущая аттестация на практических/семинарских занятиях	**Сроки – семестр, учебная неделя**	**Максимальная оценка в баллах**
домашняя работа	5,6	100
Весовой коэффициент значимости результатов текущей аттестации по практическим/семинарским занятиям– 1		
Промежуточная аттестация по практическим/семинарским занятиям–нет **Весовой коэффициент значимости результатов промежуточной аттестации по практическим/семинарским занятиям– не предусмотрено**		
3. Лабораторные занятия: коэффициент значимости совокупных результатов лабораторных занятий –не предусмотрено		
Текущая аттестация на лабораторных занятиях	**Сроки – семестр, учебная неделя**	**Максимальная оценка в баллах**
Весовой коэффициент значимости результатов текущей аттестации по лабораторным занятиям -не предусмотрено		
Промежуточная аттестация по лабораторным занятиям –нет		

Весовой коэффициент значимости результатов промежуточной аттестации по лабораторным занятиям – не предусмотрено		
4. Онлайн-занятия: коэффициент значимости совокупных результатов онлайн-занятий –не предусмотрено		
Текущая аттестация на онлайн-занятиях	**Сроки – семестр, учебная неделя**	**Максимальная оценка в баллах**
Весовой коэффициент значимости результатов текущей аттестации по онлайн-занятиям -не предусмотрено		
Промежуточная аттестация по онлайн-занятиям –нет **Весовой коэффициент значимости результатов промежуточной аттестации по онлайн-занятиям – не предусмотрено**		

3.2. Процедуры текущей и промежуточной аттестации курсовой работы/проекта

Текущая аттестация выполнения курсовой работы/проекта	**Сроки − семестр, учебная неделя**	**Максимальная оценка в баллах**
Весовой коэффициент текущей аттестации выполнения курсовой работы/проекта– не предусмотрено		
Весовой коэффициент промежуточной аттестации выполнения курсовой работы/проекта– защиты – не предусмотрено		

4. КРИТЕРИИ И УРОВНИ ОЦЕНИВАНИЯ РЕЗУЛЬТАТОВ ОБУЧЕНИЯ ПО ДИСЦИПЛИНЕ МОДУЛЯ

4.1. В рамках БРС применяются утвержденные на кафедре/институте критерии (признаки) оценивания достижений студентов по дисциплине модуля (табл. 4) в рамках контрольно-оценочных мероприятий на соответствие указанным в табл.1 результатам обучения (индикаторам).

Таблица 4

Критерии оценивания учебных достижений обучающихся

Результаты обучения	**Критерии оценивания учебных достижений, обучающихся на соответствие результатам обучения/индикаторам**
Знания	Студент демонстрирует знания и понимание в области изучения на уровне указанных индикаторов и необходимые для продолжения обучения и/или выполнения трудовых функций и действий, связанных с профессиональной деятельностью.
Умения	Студент может применять свои знания и понимание в контекстах, представленных в оценочных заданиях, демонстрирует освоение умений на уровне указанных индикаторов и необходимых для продолжения обучения и/или выполнения трудовых функций и действий, связанных с профессиональной деятельностью.
Опыт /владение	Студент демонстрирует опыт в области изучения на уровне указанных индикаторов.
Другие результаты	Студент демонстрирует ответственность в освоении результатов обучения на уровне запланированных индикаторов. Студент способен выносить суждения, делать оценки и формулировать выводы в области изучения.

	Студент может сообщать преподавателю и коллегам своего уровня собственное понимание и умения в области изучения.

4.2 Для оценивания уровня выполнения критериев (уровня достижений обучающихся при проведении контрольно-оценочных мероприятий по дисциплине модуля) используется универсальная шкала (табл. 5).

Таблица 5

Шкала оценивания достижения результатов обучения (индикаторов) по уровням

Характеристика уровней достижения результатов обучения (индикаторов)				
№ п/п	**Содержание уровня выполнения критерия оценивания результатов обучения (выполненное оценочное задание)**	**Шкала оценивания**		
		Традиционная характеристика уровня		**Качественная характеристика уровня**
1.	Результаты обучения (индикаторы) достигнуты в полном объеме, замечаний нет	Отлично (80-100 баллов)	Зачтено	Высокий (В)
2.	Результаты обучения (индикаторы) в целом достигнуты, имеются замечания, которые не требуют обязательного устранения	Хорошо (60-79 баллов)		Средний (С)
3.	Результаты обучения (индикаторы) достигнуты не в полной мере, есть замечания	Удовлетворительно (40-59 баллов)		Пороговый (П)
4.	Освоение результатов обучения не соответствует индикаторам, имеются существенные ошибки и замечания, требуется доработка	Неудовлетворительно (менее 40 баллов)	Не зачтено	Недостаточный (Н)
5.	Результат обучения не достигнут, задание не выполнено	Недостаточно свидетельств для оценивания		Нет результата

5. СОДЕРЖАНИЕ КОНТРОЛЬНО-ОЦЕНОЧНЫХ МЕРОПРИЯТИЙ ПО ДИСЦИПЛИНЕ МОДУЛЯ

5.1. Описание аудиторных контрольно-оценочных мероприятий по дисциплине модуля

5.1.1. Лекции

Самостоятельное изучение теоретического материала по темам/разделам лекций в соответствии с содержанием дисциплины (п. 1.2. РПД)

5.1.2. Практические/семинарские занятия

Примерный перечень тем

1. Статический анализ программного кода средствами сканера (SAST)

2. Работа с обнаруженными уязвимостями

Примерные задания

1. Создание проекта. Проект — это именованная задача, содержащая параметры сканирования исходного кода приложения и результаты сканирования. Глобальный менеджер безопасности создает проект в веб-интерфейсе.

2. Внедрение PT AI Enterprise Edition в CI-процесс. Настройка механизм запуска проверки кода на наличие уязвимостей на агенте сборки.

3. Настройка проекта. Возможны два варианта настройки проекта:

• В конфигурационном файле. Параметры сканирования в конфигурационном файле.

• В веб-интерфейсе. Настройка параметры сканирования

4. Запуск сканирования проекта для проверки на наличие уязвимостей одним из способов:

• в веб-интерфейсе;

• с помощью агента AI.Shell из командной строки;

• на агенте сборки.

Если проверка на наличие уязвимостей осуществляется на агенте сборки:

PT AI Enterprise Agent получает задачу на проверку кода от агента сборки (например, по коммиту разработчика).

PT AI Enterprise Agent проверяет код на наличие уязвимостей и возвращает результаты агенту сборки.

Результаты проверки отображаются в файле журнала в интерфейсе агента сборки.

5. В зависимости от настроенных параметров реагирования агента сборки на события, получаемые из файла журнала, сборка проекта останавливается, если политика безопасности в проекте нарушена, или продолжается, если политика безопасности в проекте соблюдена.

6. Использование PT AI Enterprise Edition в непрерывной интеграции

7. Работа с обнаруженными уязвимостями в веб-интерфейсе. Используя представленный набор инструментов, проверка и анализ найденных уязвимостей.

8. Исправление уязвимостей. Рекомендации по исправлению уязвимостей повторное сканирование.

9. Подготовка отчета по результатам сканирования. В веб-интерфейсе формируют отчет о количестве и типах найденных уязвимостей и оценивают качество реализации политики безопасности в проекте.

LMS-платформа − не предусмотрена

5.2. Описание внеаудиторных контрольно-оценочных мероприятий и средств текущего контроля по дисциплине модуля

Разноуровневое (дифференцированное) обучение.

Базовый

5.2.1. Контрольная работа

Примерный перечень тем

1. Разработка безопасного программного обеспечения

Примерные задания

1. Выбрать одну уязвимость CWE-XXX из обнаруженных сканером.
a. Описать уязвимость. В чем ее суть.
b. Привести пример данной уязвимости в коде.

2. Найти в Базе данных угроз ФСТЭК (https://bdu.fstec.ru/) уязвимости программного обеспечения, содержащую выбранную уязвимость.

3. Описать уязвимости из БДУ ФСТЭК:
a. Наименование ПО.
b. Описание сути уязвимости.
c. Дата выявления уязвимости.
d. Тип программного обеспечения.
e. Тип ошибки.
f. Уровень опасности уязвимости по CVSS 3.0
g. Статус уязвимости.
h. Наличие эксплоита.
j. Возможные способы устранения уязвимости.
k. Идентификаторы других систем описаний уязвимостей (при наличии).

4. Описать вектор атаки по методике CVSS 3.0:
a. Вектор атаки.
b. Сложность атаки
c. Уровень привилегий
d. Взаимодействие с пользователем
e. Влияние на конфиденциальность, целостность и доступность.

5. Указать примеры программных сканеров способных обнаруживать данные уязвимости.

LMS-платформа − не предусмотрена

5.2.2. Домашняя работа

Примерный перечень тем

1. Формирование проекта на микросервисной архитектуре, с применением контейнера Docker и анализ уязвимостей

Примерные задания

1. Необходимо разработать калькулятор, используя микросервисную архитектуру.

• Микросервис должен по разработанным методам API (методы GET или POST) получать входные параметры (a,b и операцию) и выдавать ответ в любом удобном формате (например, json).

• Можно использовать любой язык программирования, калькулятор должен быть размещен в любой системе контроля версий VCS (рекомендуется использовать github.com для простоты).

• В исходном коде калькулятора должны быть реализованы базовые принципы безопасной разработки.

2. Микросервис должен быть развернут на тестовой инфраструктуре CI/CD.

3. Тестовую инфраструктуру CI/CD.

• В состав тестовой инфраструктуры предлагается включить Jenkins и Docker. Для развертывания данного ПО можно использовать как готовые бесплатные облачные сервисы (SaaS) либо бесплатные облачные платформы (PaaS), например облако Амазон, так и внутренние виртуальные машины на базе Virtual Box или VMWare.

• Каждая сборка должна начинаться с нового коммита в VCS в ветке master проекта калькулятора, а готовый контейнер в Docker, содержащий микросервис калькулятор, должен быть доступен для вызова методов API.

LMS-платформа − не предусмотрена

5.3. Описание контрольно-оценочных мероприятий промежуточного контроля по дисциплине модуля

5.3.1. Экзамен

Список примерных вопросов

1. Регулирование в области разработки безопасного ПО.
2. Модели зрелости, BSIMM, OWASP SAMM,OWASP Devsecops Maturity Model
3. Стандарты. ГОСТ 58412 «Разработка безопасного ПО. Угрозы безопасности информации при разработке ПО», ГОСТ 56939 «Разработка безопасного ПО. Общие требования
4. Стандарт «Руководство по реализации мер по разработке безопасного программного обеспечения»
5. ISO IEC 27034, Методики STRIDE, циклы мер по разработке безопасного ПО, анализ требований по безопасности к ПО
6. Open Web Application Security Project (OWASP)
7. OWASP Top 10
8. Common Weakness Enumeration (CWE), описание уязвимостей CWE
9. Моделирование угроз
10. Анализ архитектуры ПО, выявление уязвимостей в ПО с использованием инструментальных средств
11. Статический анализ исходного кода
12. Динамический анализ кода ПО
13. Фаззинг-тестирование, поиск сведений об уязвимостях в общедоступных источниках
14. База данных угроз ФСТЭК
15. CWE (Common Weakness Enumeration) – общий перечень дефектов (недостатков) безопасности
16. CVE (Common Vulnerabilities and Exposures) – перечень уязвимостей и дефектов, обнаруженных в различном программном обеспечении
17. CVSS (Common Vulnerability Scoring System) – числовая оценка, показывающая потенциальную серьёзность уязвимости (CVE)
18. Проведение экспертизы, подтверждающей наличие уязвимостей
19. Классификация уязвимостей по уровню опасности и значимости
20. Рекомендации по корректировке кода и/или настройке WAF
21. Функциональность инструментальных средств тестирования ПО

22. Инструментальные средства тестирования ПО
LMS-платформа − не предусмотрена

5.4 Содержание контрольно-оценочных мероприятий по направлениям воспитательной деятельности

Направление воспитательной деятельности	Вид воспитательной деятельности	Технология воспитательной деятельности	Компетенция	Результаты обучения	**Контрольно-оценочные мероприятия**
Профессиональное воспитание	профориентационная деятельность	Технология формирования уверенности и готовности к самостоятельной успешной профессиональной деятельности	ПК-2	П-2	Домашняя работа Контрольная работа Лекции Практические/семинарские занятия Экзамен