МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ РОССИЙСКОЙ ФЕДЕРАЦИИ
ФЕДЕРАЛЬНОЕ ГОСУДАРСТВЕННОЕ БЮДЖЕТНОЕ ОБРАЗОВАТЕЛЬНОЕ УЧРЕЖДЕНИЕ ВЫСШЕГО ОБРАЗОВАНИЯ "РЯЗАНСКИЙ ГОСУДАРСТВЕННЫЙ РАДИОТЕХНИЧЕСКИЙ УНИВЕРСИТЕТ ИМЕНИ В.Ф. УТКИНА"

СОГЛАСОВАНО
Зав. выпускающей кафедры

УТВЕРЖДАЮ

Разработка безопасного программного обеспечения компьютерных систем

рабочая программа дисциплины (модуля)

Закреплена за кафедрой **Информационной безопасности**
Учебный план 10.05.01 _24_00.plx
10.05.01 КОМПЬЮТЕРНАЯ БЕЗОПАСНОСТЬ

Квалификация **специалист по защите информации**
Форма обучения **очная**
Общая трудоемкость **3 ЗЕТ**

Распределение часов дисциплины по семестрам

Семестр (<Курс>.<Семестр на курсе>)	**8 (4.2)**		Итого	
Недель	16			
Вид занятий	УП	РП	УП	РП
Лекции	32	32	32	32
Лабораторные	16	16	16	16
Практические	16	16	16	16
Иная контактная работа	0,55	0,55	0,55	0,55
Консультирование перед экзаменом и практикой	2	2	2	2
Итого ауд.	66,55	66,55	66,55	66,55
Контактная работа	66,55	66,55	66,55	66,55
Сам. работа	21	21	21	21
Часы на контроль	8,75	8,75	8,75	8,75
Письменная работа на курсе	11,7	11,7	11,7	11,7
Итого	108	108	108	108

г. Рязань

Программу составил(и):
к.т.н., доц., Кузьмин Юрий Михайлович

Рабочая программа дисциплины
Разработка безопасного программного обеспечения компьютерных систем
разработана в соответствии с ФГОС ВО:
ФГОС ВО - специалитет по специальности 10.05.01 Компьютерная безопасность (приказ Минобрнауки России от 26.11.2020 г. № 1459)
составлена на основании учебного плана:
10.05.01 КОМПЬЮТЕРНАЯ БЕЗОПАСНОСТЬ
утвержденного учёным советом вуза от 26.01.2024 протокол № 8.

Рабочая программа одобрена на заседании кафедры
Информационной безопасности
Протокол от 17.06.2024 г. № 12
Срок действия программы: 2024-2030 уч.г.
Зав. кафедрой Пржегорлинский Виктор Николаевич

Визирование РПД для исполнения в очередном учебном году

Рабочая программа пересмотрена, обсуждена и одобрена для исполнения в 2025-2026 учебном году на заседании кафедры
Информационной безопасности

Протокол от __ _____ 2025 г. № __

Зав. кафедрой _____

Визирование РПД для исполнения в очередном учебном году

Рабочая программа пересмотрена, обсуждена и одобрена для исполнения в 2026-2027 учебном году на заседании кафедры
Информационной безопасности

Протокол от __ _____ 2026 г. № __

Зав. кафедрой _____

Визирование РПД для исполнения в очередном учебном году

Рабочая программа пересмотрена, обсуждена и одобрена для исполнения в 2027-2028 учебном году на заседании кафедры
Информационной безопасности

Протокол от __ _____ 2027 г. № __

Зав. кафедрой _____

Визирование РПД для исполнения в очередном учебном году

Рабочая программа пересмотрена, обсуждена и одобрена для исполнения в 2028-2029 учебном году на заседании кафедры
Информационной безопасности

Протокол от __ _____ 2028 г. № __

Зав. кафедрой _____

1. ЦЕЛИ ОСВОЕНИЯ ДИСЦИПЛИНЫ (МОДУЛЯ)	
1.1	Целью дисциплины является получение обучающимися знаний, формирование у них умений и навыков, необходимых при разработке безопасного программного обеспечения для решения задач в профессиональной деятельности..
1.2	Задачами дисциплины являются:
1.3	− получение знаний об основных уязвимостях и угрозах безопасности информации при разработке ПО и их источниках; о требованиях к безопасному программному обеспечению (ПО) и программно-методической документации; о методологии оценки безопасности ПО и уровнях доверия и оценке рисков безопасности ПО; об организационных и технических мерах по разработке безопасного ПО, реализуемых на различных стадиях жизненного цикла разработки безопасного ПО, в том числе о целях этих мер и о требованиях, предъявляемых к их реализации; руководящих документах, регламентирующих процесс создания и содержание этапов создания безопасного ПО; руководящих документах, регламентирующих анализ (аудит, экспертизу) безопасности ПО и оценку степени соответствия выявленной безопасности ПО предъявленным требованиям; о документах, которые необходимо разрабатывать при выполнении работ по созданию безопасного ПО; о периодичности, основных этапах и методах тестирования и анализа ПО; об инструментальных средствах, применяемые для тестирования ПО, его анализа и поиска в нем уязвимостей;
1.4	− приобретение умения выявлять угрозы и уязвимости ПО; проводить тестирование и анализ ПО; разрабатывать необходимую документацию в процессе создания безопасного ПО; разрабатывать организационные и технические меры по созданию безопасного ПО, реализуемых на различных стадиях жизненного цикла разработки безопасного ПО; оценивать безопасность ПО, уровнях доверия и риски безопасности ПО; оценивать степень соответствия выявленной безопасности ПО предъявленным требованиям;
1.5	− приобретение практических навыков выявления угроз и уязвимостей ПО; тестировании и анализе ПО; разработке необходимой документации; разработке организационных и технических мер по разработке безопасного ПО, реализуемых на различных стадиях жизненного цикла созданию безопасного ПО; оценке безопасность ПО, уровне доверия и риске безопасности ПО; оценке степени соответствия выявленной безопасности ПО предъявленным требованиям.
2. МЕСТО ДИСЦИПЛИНЫ (МОДУЛЯ) В СТРУКТУРЕ ОБРАЗОВАТЕЛЬНОЙ ПРОГРАММЫ	
Цикл (раздел) ОП:	Б1.В
2.1	**Требования к предварительной подготовке обучающегося:**
2.1.1	Объекты защиты информации
2.2	**Дисциплины (модули) и практики, для которых освоение данной дисциплины (модуля) необходимо как предшествующее:**
2.2.1	Производственная практика
2.2.2	Подготовка к процедуре защиты и процедура защиты выпускной квалификационной работы
2.2.3	Преддипломная практика

3. КОМПЕТЕНЦИИ ОБУЧАЮЩЕГОСЯ, ФОРМИРУЕМЫЕ В РЕЗУЛЬТАТЕ ОСВОЕНИЯ ДИСЦИПЛИНЫ (МОДУЛЯ)

ПК-3: Способен оценивать уровень безопасности компьютерных систем и сетей

ПК-3.2. Проводит анализ безопасности компьютерных систем

Знать
- основные уязвимости и угрозы безопасности информации при разработке ПО и их ис-точники;
- требования к безопасному программному обеспечению (ПО) и программно-методической документации;
- методологию оценки безопасности ПО, об уровнях доверия безопасности ПО;
- руководящие документы, регламентирующие анализ (аудит, экспертизу) безопасности ПО и оценку степени соответствия выявленной безопасности ПО предъявленным требованиям;
- периодичность, основные этапы и методы тестирования и анализа ПО.

Уметь
- выявлять угрозы и уязвимости ПО;
- проводить тестирование и анализ ПО;
- оценивать безопасность ПО, уровни доверия и риски безопасности ПО;
- оценивать степень соответствия выявленной безопасности ПО предъявленным требованиям;
- составлять и оформлять аналитический отчет по результатам проведенного анализа уязвимостей;
- разрабатывать предложения по устранению выявленных уязвимостей.

Владеть
- навыками выявления угроз и уязвимостей ПО;
- навыками тестировании и анализе ПО;
- навыками оценки безопасности ПО, уровня доверия и риска безопасности ПО;
- навыками оценки степени соответствия выявленной безопасности ПО предъявленным требованиям;
- навыками управления уязвимостями ПО.

В результате освоения дисциплины (модуля) обучающийся должен

3.1	**Знать:**
3.1.1	- основные уязвимости и угрозы безопасности информации при разработке ПО и их ис-точники;
3.1.2	- требования к безопасному программному обеспечению (ПО) и программно-методической документации;
3.1.3	- методологию оценки безопасности ПО, об уровнях доверия безопасности ПО;
3.1.4	- руководящие документы, регламентирующие анализ (аудит, экспертизу) безопасности ПО и оценку степени соответствия выявленной безопасности ПО предъявленным требованиям;
3.1.5	- периодичность, основные этапы и методы тестирования и анализа ПО.
3.2	**Уметь:**
3.2.1	- выявлять угрозы и уязвимости ПО;
3.2.2	- проводить тестирование и анализ ПО;
3.2.3	- оценивать безопасность ПО, уровни доверия и риски безопасности ПО;
3.2.4	- оценивать степень соответствия выявленной безопасности ПО предъявленным требованиям;
3.2.5	- составлять и оформлять аналитический отчет по результатам проведенного анализа уязвимостей;
3.2.6	- разрабатывать предложения по устранению выявленных уязвимостей.
3.2.7	
3.3	**Владеть:**
3.3.1	- навыками выявления угроз и уязвимостей ПО;
3.3.2	- навыками тестировании и анализе ПО;
3.3.3	- навыками оценки безопасности ПО, уровня доверия и риска безопасности ПО;
3.3.4	- навыками оценки степени соответствия выявленной безопасности ПО предъявленным требованиям;
3.3.5	- навыками управления уязвимостями ПО.
3.3.6	

4. СТРУКТУРА И СОДЕРЖАНИЕ ДИСЦИПЛИНЫ (МОДУЛЯ)

Код занятия	Наименование разделов и тем /вид занятия/	Семестр / Курс	Часов	Компетен-ции	Литература	Форма контроля
	Раздел 1. Введение в дисциплину					
1.1	/Тема/	8	0			
1.2	Актуальность безопасной разработки ПО (Требования руководящих документов. Ошибка при разработке ПО может обернуться для программиста уголовным сроком. Зачем тестировать программы на безопасность (уязвимость)). Проблемы безопасной разработки ПО. Средство Антифишинг.START для формирования требований по безопасной разработке ПО. Подходы к определению понятия безопасного ПО: а) ПО без уязвимостей б) ПО в котором устранены уязвимости в) ПО способное противостоять определенному потенциалу нападения - сравнить ГОСТ Р ИСО-МЭК 18045—2013 (Приложение В) и Методику выявления уязвимостей и НДВ в ПО (Приложение 4) для определения потенциала нарушителя. /Лек/	8	2	ПК-3.2-З ПК-3.2-У ПК-3.2-В	Л1.1 Л1.2 Л1.3 Л1.4 Л1.5 Л1.6 Л1.7 Л1.8Л2.1 Л2.2Л3.1 Л3.2 Э1 Э2 Э3 Э4 Э5 Э6 Э7 Э8 Э9 Э10 Э11 Э12 Э13 Э14 Э15 Э16 Э17 Э18 Э19 Э20 Э21 Э22 Э23 Э24 Э25 Э26 Э27 Э28 Э29 Э30	Конспект лекций

1.3	Изучение литературы и конспекта лекций /Ср/	8	2	ПК-3.2-З ПК-3.2-У ПК-3.2-В	Л1.1 Л1.2 Л1.3 Л1.4 Л1.5 Л1.6 Л1.7 Л1.8Л2.1 Л2.2Л3.1 Л3.2 Э1 Э2 Э3 Э4 Э5 Э6 Э7 Э8 Э9 Э10 Э11 Э12 Э13 Э14 Э15 Э16 Э17 Э18 Э19 Э20 Э21 Э22 Э23 Э24 Э25 Э26 Э27 Э28 Э29 Э30	Подготовка конспекта по вопросам темы. Краткий опрос по теме на консультации к экзамену (зачету).
	Раздел 2. Базовая терминология безопасной разработки ПО. Дефекты ПО, уязвимости ПО и НДВ ПО					
2.1	/Тема/	8	0			
2.2	Основные понятия безопасной разработки ПО (Словарь). Перечень типовых дефектов ПО и форм их проявления). Классификация уязвимостей ПО (из Методики). Классификация НДВ ПО (из Методики). /Лек/	8	2	ПК-3.2-З ПК-3.2-У ПК-3.2-В	Л1.1 Л1.2 Л1.3 Л1.4 Л1.5 Л1.6 Л1.7 Л1.8Л2.1 Л2.2Л3.1 Л3.2 Э1 Э2 Э3 Э4 Э5 Э6 Э7 Э8 Э9 Э10 Э11 Э12 Э13 Э14 Э15 Э16 Э17 Э18 Э19 Э20 Э21 Э22 Э23 Э24 Э25 Э26 Э27 Э28 Э29 Э30	Конспект лекций
2.3	Анализ дефектов, уязвимостей и НДВ ПО /Пр/	8	2	ПК-3.2-З ПК-3.2-У ПК-3.2-В	Л1.1 Л1.2 Л1.3 Л1.4 Л1.5 Л1.6 Л1.7 Л1.8Л2.1 Л2.2Л3.1 Л3.2 Э1 Э2 Э3 Э4 Э5 Э6 Э7 Э8 Э9 Э10 Э11 Э12 Э13 Э14 Э15 Э16 Э17 Э18 Э19 Э20 Э21 Э22 Э23 Э24 Э25 Э26 Э27 Э28 Э29 Э30	Устный опрос по теме. Решение задач. Проверка домашнего задания.

2.4	Изучение литературы и конспекта лекций /Ср/	8	2	ПК-3.2-З ПК-3.2-У ПК-3.2-В	Л1.1 Л1.2 Л1.3 Л1.4 Л1.5 Л1.6 Л1.7 Л1.8Л2.1 Л2.2Л3.1 Л3.2 Э1 Э2 Э3 Э4 Э5 Э6 Э7 Э8 Э9 Э10 Э11 Э12 Э13 Э14 Э15 Э16 Э17 Э18 Э19 Э20 Э21 Э22 Э23 Э24 Э25 Э26 Э27 Э28 Э29 Э30	Подготовка конспекта по вопросам темы. Краткий опрос по теме на консультации к экзамену (зачету).
	Раздел 3. Угрозы безопасности информации при разработке ПО					
3.1	/Тема/	8	0			
3.2	Угрозы безопасности информации на разных стадиях ЖЦ ПО (согласно ГОСТ Р 58412-2019 "Защита информации. Разработка безопасного ПО. Угрозы безопасности информации при разработке ПО") и меры по разработке безопасной разработке ПО (из ГОСТ Р 56939-2016) для устранения угроз (сопоставление угроз и мер приведено в Приложении А к ГОСТ Р 58412-2019). /Лек/	8	4	ПК-3.2-З ПК-3.2-У ПК-3.2-В	Л1.1 Л1.2 Л1.3 Л1.4 Л1.5 Л1.6 Л1.7 Л1.8Л2.1 Л2.2Л3.1 Л3.2 Э1 Э2 Э3 Э4 Э5 Э6 Э7 Э8 Э9 Э10 Э11 Э12 Э13 Э14 Э15 Э16 Э17 Э18 Э19 Э20 Э21 Э22 Э23 Э24 Э25 Э26 Э27 Э28 Э29 Э30	Конспект лекций
3.3	Анализ угроз безопасности ПО и мер безопасной разработки ПО против угроз /Пр/	8	2	ПК-3.2-З ПК-3.2-У ПК-3.2-В	Л1.1 Л1.2 Л1.3 Л1.4 Л1.5 Л1.6 Л1.7 Л1.8Л2.1 Л2.2Л3.1 Л3.2 Э1 Э2 Э3 Э4 Э5 Э6 Э7 Э8 Э9 Э10 Э11 Э12 Э13 Э14 Э15 Э16 Э17 Э18 Э19 Э20 Э21 Э22 Э23 Э24 Э25 Э26 Э27 Э28 Э29 Э30	Устный опрос по теме. Решение задач. Проверка домашнего задания.

3.4	Изучение литературы и конспекта лекций /Ср/	8	2	ПК-3.2-З ПК-3.2-У ПК-3.2-В	Л1.1 Л1.2 Л1.3 Л1.4 Л1.5 Л1.6 Л1.7 Л1.8Л2.1 Л2.2Л3.1 Л3.2 Э1 Э2 Э3 Э4 Э5 Э6 Э7 Э8 Э9 Э10 Э11 Э12 Э13 Э14 Э15 Э16 Э17 Э18 Э19 Э20 Э21 Э22 Э23 Э24 Э25 Э26 Э27 Э28 Э29 Э30	Подготовка конспекта по вопросам темы. Краткий опрос по теме на консультации к экзамену (зачету).
	Раздел 4. Организационные и технические меры по разработке безопасного ПО, реализуемых на различных стадиях жизненного цикла разработки безопасного ПО					
4.1	/Тема/	8	0			
4.2	Меры по безопасной разработке ПО согласно ГОСТ Р 56939-2016: а) Меры по разработке безопасного ПО, реализуемые при выполнении анализа требований к ПО. б) Меры по разработке безопасного ПО, реализуемые при выполнении проектирования архитектуры ПО. в) Меры по разработке безопасного ПО, реализуемые при выполнении конструирования и комплексирования ПО. г) Меры по разработке безопасного ПО, реализуемые при выполнении квалификационного тестирования ПО. д) Меры по разработке безопасного ПО, реализуемые при выполнении инсталляции ПО и поддержки приемки ПО. е) Меры по разработке безопасного ПО, реализуемые при решении проблем в программном обеспечении в процессе эксплуатации. ж) Меры по разработке безопасного ПО, реализуемые в процессе менеджмента документацией и конфигурацией программы. з) Меры по разработке безопасного ПО, реализуемые в процессе менеджмента инфраструктурой среды разработки ПО. и) Меры по разработке безопасного ПО, реализуемые в процессе менеджмента людскими ресурсами. ЖЦ безопасной разработки ПО согласно ГОСТ Р ИСО-МЭК 27034-1 Информационные технологии. Безопасность приложений. Часть 1. Безопасность приложений. Защита ПО от взлома и несанкционированного использования. /Лек/	8	8	ПК-3.2-З ПК-3.2-У ПК-3.2-В	Л1.1 Л1.2 Л1.3 Л1.4 Л1.5 Л1.6 Л1.7 Л1.8Л2.1 Л2.2Л3.1 Л3.2 Э1 Э2 Э3 Э4 Э5 Э6 Э7 Э8 Э9 Э10 Э11 Э12 Э13 Э14 Э15 Э16 Э17 Э18 Э19 Э20 Э21 Э22 Э23 Э24 Э25 Э26 Э27 Э28 Э29 Э30	Конспект лекций

4.3	Меры по разработке безопасного ПО согласно ГОСТ Р 56939-2016 /Пр/	8	2	ПК-3.2-З ПК-3.2-У ПК-3.2-В	Л1.1 Л1.2 Л1.3 Л1.4 Л1.5 Л1.6 Л1.7 Л1.8Л2.1 Л2.2Л3.1 Л3.2 Э1 Э2 Э3 Э4 Э5 Э6 Э7 Э8 Э9 Э10 Э11 Э12 Э13 Э14 Э15 Э16 Э17 Э18 Э19 Э20 Э21 Э22 Э23 Э24 Э25 Э26 Э27 Э28 Э29 Э30	Устный опрос по теме. Решение задач. Проверка домашнего задания.
4.4	Безопасная разработка ПО согласно ГОСТ Р ИСО-МЭК 27034-1-2014 /Пр/	8	2	ПК-3.2-З ПК-3.2-У ПК-3.2-В	Л1.1 Л1.2 Л1.3 Л1.4 Л1.5 Л1.6 Л1.7 Л1.8Л2.1 Л2.2Л3.1 Л3.2 Э1 Э2 Э3 Э4 Э5 Э6 Э7 Э8 Э9 Э10 Э11 Э12 Э13 Э14 Э15 Э16 Э17 Э18 Э19 Э20 Э21 Э22 Э23 Э24 Э25 Э26 Э27 Э28 Э29 Э30	Устный опрос по теме. Решение задач. Проверка домашнего задания.
4.5	Анализ сайта с использованием интерфейса Chrome DevTools в браузере Google Chrome /Лаб/	8	2	ПК-3.2-З ПК-3.2-У ПК-3.2-В	Л1.1 Л1.2 Л1.3 Л1.4 Л1.5 Л1.6 Л1.7 Л1.8Л2.1 Л2.2Л3.1 Л3.2 Э1 Э2 Э3 Э4 Э5 Э6 Э7 Э8 Э9 Э10 Э11 Э12 Э13 Э14 Э15 Э16 Э17 Э18 Э19 Э20 Э21 Э22 Э23 Э24 Э25 Э26 Э27 Э28 Э29 Э30	Отчет по ЛР Защита ЛР.

4.6	Работа с системой контроля версий Git /Лаб/	8	2	ПК-3.2-З ПК-3.2-У ПК-3.2-В	Л1.1 Л1.2 Л1.3 Л1.4 Л1.5 Л1.6 Л1.7 Л1.8Л2.1 Л2.2Л3.1 Л3.2 Э1 Э2 Э3 Э4 Э5 Э6 Э7 Э8 Э9 Э10 Э11 Э12 Э13 Э14 Э15 Э16 Э17 Э18 Э19 Э20 Э21 Э22 Э23 Э24 Э25 Э26 Э27 Э28 Э29 Э30	Отчет по ЛР Защита ЛР.
4.7	Защита программ от исследования статическим методом /Лаб/	8	2	ПК-3.2-З ПК-3.2-У ПК-3.2-В	Л1.1 Л1.2 Л1.3 Л1.4 Л1.5 Л1.6 Л1.7 Л1.8Л2.1 Л2.2Л3.1 Л3.2 Э1 Э2 Э3 Э4 Э5 Э6 Э7 Э8 Э9 Э10 Э11 Э12 Э13 Э14 Э15 Э16 Э17 Э18 Э19 Э20 Э21 Э22 Э23 Э24 Э25 Э26 Э27 Э28 Э29 Э30	Отчет по ЛР Защита ЛР.
4.8	Защита программ от исследования динамическим методом /Лаб/	8	2	ПК-3.2-З ПК-3.2-У ПК-3.2-В	Л1.1 Л1.2 Л1.3 Л1.4 Л1.5 Л1.6 Л1.7 Л1.8Л2.1 Л2.2Л3.1 Л3.2 Э1 Э2 Э3 Э4 Э5 Э6 Э7 Э8 Э9 Э10 Э11 Э12 Э13 Э14 Э15 Э16 Э17 Э18 Э19 Э20 Э21 Э22 Э23 Э24 Э25 Э26 Э27 Э28 Э29 Э30	Отчет по ЛР Защита ЛР.

4.9	Изучение литературы и конспекта лекций /Ср/	8	4	ПК-3.2-З ПК-3.2-У ПК-3.2-В	Л1.1 Л1.2 Л1.3 Л1.4 Л1.5 Л1.6 Л1.7 Л1.8Л2.1 Л2.2Л3.1 Л3.2 Э1 Э2 Э3 Э4 Э5 Э6 Э7 Э8 Э9 Э10 Э11 Э12 Э13 Э14 Э15 Э16 Э17 Э18 Э19 Э20 Э21 Э22 Э23 Э24 Э25 Э26 Э27 Э28 Э29 Э30	Подготовка конспекта по вопросам темы. Краткий опрос по теме на консультации к экзамену (зачету).
	Раздел 5. Выявление уязвимостей и НДВ в ПО					
5.1	/Тема/	8	0			
5.2	Контроль отсутствия НДВ (было раньше по РД Гостехкомиссии). Современный подход к выявлению уязвимостей в ПО (обзор ГОСТов, Приказов ФСТЭК России и др. руководящих документов), Уязвимости веб-приложений на примере OWASP TOP TEN. Выявление уязвимостей и НДВ по Методике выявления уязвимостей и НДВ в ПО: - этапы выявления уязвимостей - содержание работ по выявлению уязвимостей. Методы исследования ПО на наличие уязвимостей (по Методике). Инструменты исследования ПО на наличие уязвимостей (по Методике). /Лек/	8	8	ПК-3.2-З ПК-3.2-У ПК-3.2-В	Л1.1 Л1.2 Л1.3 Л1.4 Л1.5 Л1.6 Л1.7 Л1.8Л2.1 Л2.2Л3.1 Л3.2 Э1 Э2 Э3 Э4 Э5 Э6 Э7 Э8 Э9 Э10 Э11 Э12 Э13 Э14 Э15 Э16 Э17 Э18 Э19 Э20 Э21 Э22 Э23 Э24 Э25 Э26 Э27 Э28 Э29 Э30	Конспект лекций
5.3	Изучение порядка и особенностей выявления уязвимостей и НДВ По согласно Методике /Пр/	8	2	ПК-3.2-З ПК-3.2-У ПК-3.2-В	Л1.1 Л1.2 Л1.3 Л1.4 Л1.5 Л1.6 Л1.7 Л1.8Л2.1 Л2.2Л3.1 Л3.2 Э1 Э2 Э3 Э4 Э5 Э6 Э7 Э8 Э9 Э10 Э11 Э12 Э13 Э14 Э15 Э16 Э17 Э18 Э19 Э20 Э21 Э22 Э23 Э24 Э25 Э26 Э27 Э28 Э29 Э30	Устный опрос по теме. Решение задач. Проверка домашнего задания.

5.4	Изучение уязвимости веб-приложений из списка OWASP TOP TEN /Пр/	8	2	ПК-3.2-З ПК-3.2-У ПК-3.2-В	Л1.1 Л1.2 Л1.3 Л1.4 Л1.5 Л1.6 Л1.7 Л1.8Л2.1 Л2.2Л3.1 Л3.2 Э1 Э2 Э3 Э4 Э5 Э6 Э7 Э8 Э9 Э10 Э11 Э12 Э13 Э14 Э15 Э16 Э17 Э18 Э19 Э20 Э21 Э22 Э23 Э24 Э25 Э26 Э27 Э28 Э29 Э30	Устный опрос по теме. Решение задач. Проверка домашнего задания.
5.5	Исследование программ статическим методом с помощью дизассемблера IDA. Уязвимости парольной защиты программ /Лаб/	8	2	ПК-3.2-З ПК-3.2-У ПК-3.2-В	Л1.1 Л1.2 Л1.3 Л1.4 Л1.5 Л1.6 Л1.7 Л1.8Л2.1 Л2.2Л3.1 Л3.2 Э1 Э2 Э3 Э4 Э5 Э6 Э7 Э8 Э9 Э10 Э11 Э12 Э13 Э14 Э15 Э16 Э17 Э18 Э19 Э20 Э21 Э22 Э23 Э24 Э25 Э26 Э27 Э28 Э29 Э30	Отчет по ЛР Защита ЛР.
5.6	Исследование уязвимостей программ статическим анализатором PVS Studio /Лаб/	8	2	ПК-3.2-З ПК-3.2-У ПК-3.2-В	Л1.1 Л1.2 Л1.3 Л1.4 Л1.5 Л1.6 Л1.7 Л1.8Л2.1 Л2.2Л3.1 Л3.2 Э1 Э2 Э3 Э4 Э5 Э6 Э7 Э8 Э9 Э10 Э11 Э12 Э13 Э14 Э15 Э16 Э17 Э18 Э19 Э20 Э21 Э22 Э23 Э24 Э25 Э26 Э27 Э28 Э29 Э30	Отчет по ЛР Защита ЛР.

5.7	Исследование программ динамическим методом с помощью отладчика OllyDbg /Лаб/	8	2	ПК-3.2-З ПК-3.2-У ПК-3.2-В	Л1.1 Л1.2 Л1.3 Л1.4 Л1.5 Л1.6 Л1.7 Л1.8Л2.1 Л2.2Л3.1 Л3.2 Э1 Э2 Э3 Э4 Э5 Э6 Э7 Э8 Э9 Э10 Э11 Э12 Э13 Э14 Э15 Э16 Э17 Э18 Э19 Э20 Э21 Э22 Э23 Э24 Э25 Э26 Э27 Э28 Э29 Э30	Отчет по ЛР Защита ЛР.
5.8	Исследование уязвимостей программ с помощью фаззера American Fuzzy Loop. /Лаб/	8	2	ПК-3.2-З ПК-3.2-У ПК-3.2-В	Л1.1 Л1.2 Л1.3 Л1.4 Л1.5 Л1.6 Л1.7 Л1.8Л2.1 Л2.2Л3.1 Л3.2 Э1 Э2 Э3 Э4 Э5 Э6 Э7 Э8 Э9 Э10 Э11 Э12 Э13 Э14 Э15 Э16 Э17 Э18 Э19 Э20 Э21 Э22 Э23 Э24 Э25 Э26 Э27 Э28 Э29 Э30	Отчет по ЛР Защита ЛР.
5.9	Изучение литературы и конспекта лекций /Ср/	8	4	ПК-3.2-З ПК-3.2-У ПК-3.2-В	Л1.1 Л1.2 Л1.3 Л1.4 Л1.5 Л1.6 Л1.7 Л1.8Л2.1 Л2.2Л3.1 Л3.2 Э1 Э2 Э3 Э4 Э5 Э6 Э7 Э8 Э9 Э10 Э11 Э12 Э13 Э14 Э15 Э16 Э17 Э18 Э19 Э20 Э21 Э22 Э23 Э24 Э25 Э26 Э27 Э28 Э29 Э30	Подготовка конспекта по вопросам темы. Краткий опрос по теме на консультации к экзамену (зачету).
	Раздел 6. Методы анализа ПО					
6.1	/Тема/	8	0			

6.2	Виды тестирования ПО. Статический анализ ПО. Динамический анализ ПО. Фаззинг ПО. /Лек/	8	4	ПК-3.2-З ПК-3.2-У ПК-3.2-В	Л1.1 Л1.2 Л1.3 Л1.4 Л1.5 Л1.6 Л1.7 Л1.8Л2.1 Л2.2Л3.1 Л3.2 Э1 Э2 Э3 Э4 Э5 Э6 Э7 Э8 Э9 Э10 Э11 Э12 Э13 Э14 Э15 Э16 Э17 Э18 Э19 Э20 Э21 Э22 Э23 Э24 Э25 Э26 Э27 Э28 Э29 Э30	Конспект лекций
6.3	Анализ эффективности методов статического и динамического анализов ПО /Пр/	8	2	ПК-3.2-З ПК-3.2-У ПК-3.2-В	Л1.1 Л1.2 Л1.3 Л1.4 Л1.5 Л1.6 Л1.7 Л1.8Л2.1 Л2.2Л3.1 Л3.2 Э1 Э2 Э3 Э4 Э5 Э6 Э7 Э8 Э9 Э10 Э11 Э12 Э13 Э14 Э15 Э16 Э17 Э18 Э19 Э20 Э21 Э22 Э23 Э24 Э25 Э26 Э27 Э28 Э29 Э30	Устный опрос по теме. Решение задач. Проверка домашнего задания.
6.4	Изучение литературы и конспекта лекций. /Ср/	8	4	ПК-3.2-З ПК-3.2-У ПК-3.2-В	Л1.1 Л1.2 Л1.3 Л1.4 Л1.5 Л1.6 Л1.7 Л1.8Л2.1 Л2.2Л3.1 Л3.2 Э1 Э2 Э3 Э4 Э5 Э6 Э7 Э8 Э9 Э10 Э11 Э12 Э13 Э14 Э15 Э16 Э17 Э18 Э19 Э20 Э21 Э22 Э23 Э24 Э25 Э26 Э27 Э28 Э29 Э30	Подготовка конспекта по вопросам темы. Краткий опрос по теме на консультации к экзамену (зачету).
	Раздел 7. Управление рисками информационной безопасности при разработке ПО					
7.1	/Тема/	8	0			

7.2	Понятие риска информационной безопасности. Обзор документов по управлению рисками информационной безопасности Оценивание риска информационной безопасности. Обработка рисков. Принятие рисков. /Лек/	8	4	ПК-3.2-З ПК-3.2-У ПК-3.2-В	Л1.1 Л1.2 Л1.3 Л1.4 Л1.5 Л1.6 Л1.7 Л1.8Л2.1 Л2.2Л3.1 Л3.2 Э1 Э2 Э3 Э4 Э5 Э6 Э7 Э8 Э9 Э10 Э11 Э12 Э13 Э14 Э15 Э16 Э17 Э18 Э19 Э20 Э21 Э22 Э23 Э24 Э25 Э26 Э27 Э28 Э29 Э30	Конспект лекций
7.3	Анализ особенностей анализа риска безопасности информации при разработке ПО /Пр/	8	2	ПК-3.2-З ПК-3.2-У ПК-3.2-В	Л1.1 Л1.2 Л1.3 Л1.4 Л1.5 Л1.6 Л1.7 Л1.8Л2.1 Л2.2Л3.1 Л3.2 Э1 Э2 Э3 Э4 Э5 Э6 Э7 Э8 Э9 Э10 Э11 Э12 Э13 Э14 Э15 Э16 Э17 Э18 Э19 Э20 Э21 Э22 Э23 Э24 Э25 Э26 Э27 Э28 Э29 Э30	Устный опрос по теме. Решение задач. Проверка домашнего задания.
7.4	Изучение литературы и конспекта лекций. /Ср/	8	3	ПК-3.2-З ПК-3.2-У ПК-3.2-В	Л1.1 Л1.2 Л1.3 Л1.4 Л1.5 Л1.6 Л1.7 Л1.8Л2.1 Л2.2Л3.1 Л3.2 Э1 Э2 Э3 Э4 Э5 Э6 Э7 Э8 Э9 Э10 Э11 Э12 Э13 Э14 Э15 Э16 Э17 Э18 Э19 Э20 Э21 Э22 Э23 Э24 Э25 Э26 Э27 Э28 Э29 Э30	Подготовка конспекта по вопросам темы. Краткий опрос по теме на консультации к экзамену (зачету).
	Раздел 8. Сдача курсовой работы и зачета с оценкой					
8.1	/Тема/	8	0			

8.2	Проверка ПЗ к КР. Сдача (прием) курсовой работы /КПКР/	8	11,7	ПК-3.2-З ПК-3.2-У ПК-3.2-В	Л1.1 Л1.2 Л1.3 Л1.4 Л1.5 Л1.6 Л1.7 Л1.8Л2.1 Л2.2Л3.1 Л3.2 Э1 Э2 Э3 Э4 Э5 Э6 Э7 Э8 Э9 Э10 Э11 Э12 Э13 Э14 Э15 Э16 Э17 Э18 Э19 Э20 Э21 Э22 Э23 Э24 Э25 Э26 Э27 Э28 Э29 Э30	Оценка качества подготовки ПЗ к КР. Оценка качества и полноты выполнения задания КР.
8.3	Подготовка к сдаче зачета с оценкой /ЗаО/	8	8,75	ПК-3.2-З ПК-3.2-У ПК-3.2-В	Л1.1 Л1.2 Л1.3 Л1.4 Л1.5 Л1.6 Л1.7 Л1.8Л2.1 Л2.2Л3.1 Л3.2 Э1 Э2 Э3 Э4 Э5 Э6 Э7 Э8 Э9 Э10 Э11 Э12 Э13 Э14 Э15 Э16 Э17 Э18 Э19 Э20 Э21 Э22 Э23 Э24 Э25 Э26 Э27 Э28 Э29 Э30	Задачи к зачету. Билеты к зачету. Тесты к зачету.
8.4	Консультирование перед зачетом /Кнс/	8	2	ПК-3.2-З ПК-3.2-У ПК-3.2-В	Л1.1 Л1.2 Л1.3 Л1.4 Л1.5 Л1.6 Л1.7 Л1.8Л2.1 Л2.2Л3.1 Л3.2 Э1 Э2 Э3 Э4 Э5 Э6 Э7 Э8 Э9 Э10 Э11 Э12 Э13 Э14 Э15 Э16 Э17 Э18 Э19 Э20 Э21 Э22 Э23 Э24 Э25 Э26 Э27 Э28 Э29 Э30	Вопросы к экзамену. Решение типовых задач. Ответы на вопросы.

8.5	Сдача зачета с оценкой /ИКР/	8	0,55	ПК-3.2-З ПК-3.2-У ПК-3.2-В	Л1.1 Л1.2 Л1.3 Л1.4 Л1.5 Л1.6 Л1.7 Л1.8Л2.1 Л2.2Л3.1 Л3.2 Э1 Э2 Э3 Э4 Э5 Э6 Э7 Э8 Э9 Э10 Э11 Э12 Э13 Э14 Э15 Э16 Э17 Э18 Э19 Э20 Э21 Э22 Э23 Э24 Э25 Э26 Э27 Э28 Э29 Э30	Ответы на Контрольные вопросы Результаты решения задач. Ответы на дополнительные вопросы. Результаты тестирования.

5. ОЦЕНОЧНЫЕ МАТЕРИАЛЫ ПО ДИСЦИПЛИНЕ (МОДУЛЮ)

Оценочные материалы по данной дисциплине приведены в приложении к рабочей программе дисциплины (см. документ «Оценочные материалы по дисциплине «Разработка безопасного программного обеспечения компьютерных систем»).

6. УЧЕБНО-МЕТОДИЧЕСКОЕ И ИНФОРМАЦИОННОЕ ОБЕСПЕЧЕНИЕ ДИСЦИПЛИНЫ (МОДУЛЯ)

6.1. Рекомендуемая литература

6.1.1. Основная литература

№	Авторы, составители	Заглавие	Издательство, год	Количество/ название ЭБС
Л1.1	Крис Касперски	Фундаментальные основы хакерства. Искусство дизассемблирования	Москва: СОЛОН-[illegible], 2016, 446 с.	5-93455-175-2, http://www.iprbookshop.ru/90401.html
Л1.2	Бегаев А. Н., Бегаев С. Н., Кашин С. В.	Анализ программного кода при проведении сертификационных испытаний	Санкт-Петербург: НИУ ИТМО, 2018, 41 с.	, https://e.lanbook.com/book/136488
Л1.3	Бегаев А. Н., Бегаев С. Н., Федотов В. А.	Тестирование на проникновение	Санкт-Петербург: НИУ ИТМО, 2018, 45 с.	, https://e.lanbook.com/book/136489
Л1.4	Андрианов В. И., Красов А. В., Липатников В. А.	Инновационное управление рисками информационной безопасности : учеб. пособие	Санкт-Петербург: СПбГУТ им. М.А. Бонч-Бруевича, 2012, 396 с.	978-5-91891-092-4, https://e.lanbook.com/book/181472
Л1.5	Бегаев А. Н., Кашин С. В., Маркевич Н. А., Марченко А. А.	Выявление уязвимостей и недекларированных возможностей в программном обеспечении : учебно-методическое пособие	Санкт-Петербург: НИУ ИТМО, 2020, 38 с.	, https://e.lanbook.com/book/190792
Л1.6	Бегаев А. Н., Кашин С. В., Павлов Д. Д., Маркевич Н. А.	Модель безопасности средства, или Как формально описать подсистемы программного обеспечения : учебно-методическое пособие	Санкт-Петербург: НИУ ИТМО, 2022, 44 с.	, https://e.lanbook.com/book/283826

№	Авторы, составители	Заглавие	Издательство, год	Количество/ название ЭБС
Л1.7	Бегаев А. Н., Кашин С. В., Марченко А. А., Гусева Д. А.	Технология разработки и оформления отчетных документов по результатам поиска уязвимостей в программном обеспечении : учебно-методическое пособие	Санкт-Петербург: НИУ ИТМО, 2022, 58 с.	, https://e.lanbook.com/book/283829
Л1.8	Рощин, П. Г.	Командная разработка программного обеспечения с помощью системы контроля версий GIT: конспект лекций : учебное пособие	Москва: Национальный исследовательский ядерный университет «МИФИ», 2022, 106 с.	978-5-7262-2846-4, https://www.iprbookshop.ru/132682.html
6.1.2. Дополнительная литература				
№	Авторы, составители	Заглавие	Издательство, год	Количество/ название ЭБС
Л2.1	Оголюк А. А.	Защита приложений от модификации. Дополнительные материалы : учебное пособие	Санкт-Петербург: Университет ИТМО, 2014, 123 с.	2227-8397, http://www.iprbookshop.ru/66449.html
Л2.2	Оголюк А. А.	Защита приложений от модификации : учебное пособие	Санкт-Петербург: Университет ИТМО, 2013, 58 с.	2227-8397, http://www.iprbookshop.ru/66450.html
6.1.3. Методические разработки				
№	Авторы, составители	Заглавие	Издательство, год	Количество/ название ЭБС
Л3.1	Кузьмин Ю.М., Калинкина Т.И.	Защита программ и данных. Ч.1 : Методические указания	Рязань: РИЦ РГРТУ, 2019,	, https://elib.rsreu.ru/ebs/download/2119
Л3.2	Кузьмин Ю.М., Калинкина Т.И.	Защита программ и данных. Часть 2. Исследование программ динамическим методом: метод. указ. к лаб. работам : Методические указания	Рязань: РИЦ РГРТУ, 2020,	, https://elib.rsreu.ru/ebs/download/2638
6.2. Перечень ресурсов информационно-телекоммуникационной сети "Интернет"				
Э1	Электронно-библиотечная система «Лань». – Режим доступа: доступ из корпоративной сети РГРТУ – свободный (без пароля) URL: https://e.lanbook.com/			
Э2	Электронно-библиотечная система «IPRbooks». – Режим доступа: доступ из корпоративной сети РГРТУ – свободный (без пароля), доступ из сети Интернет - по паролю. URL: https://iprbookshop.ru/			
Э3	Электронная библиотека РГРТУ. Режим доступа: из корпоративной сети РГРТУ – по паролю. URL: http://elib.rsreu.ru/			
Э4	Научная электронная библиотека eLibrary. URL: http//e.lib/vlsu.ru/www.uisrussia.msu.ru/elibrary.ru			
Э5	Национальный открытый университет ИНТУИТ. URL: http://www.intuit.ru			
Э6	Бегаев А.Н., Кашин С.В., Маркевич Н.А., Марченко А.А., Павлов Д.Д. Сертификация программного обеспечения по требованиям доверия: Учебно-методическое пособие. - Санкт-Петербург: Университет ИТМО, 2020. - 40 с. URL: http://books.ifmo.ru/file/pdf/2579.pdf			
Э7	Бегаев А.Н., Кашин С.В., Зимненко С.А., Сертификация программного обеспечения и автоматизированных систем в различных системах сертификации. – СПб: Университет ИТМО, 2018. – 45 с. URL: http://books.ifmo.ru/file/pdf/2375.pdf			
Э8	Донецкая Ю.В., Зыков А.Г., Поляков В.И. Методы верификации вычислительных процессов. [Часть 1]: Учебно-методическое пособие. - Санкт-Петербург: Университет ИТМО, 2019. - 142 с. URL: http://books.ifmo.ru/file/pdf/2539.pdf			
Э9	Защита программ и данных : учебное пособие. — Санкт-Петербург : СПбГУТ им. М.А. Бонч-Бруевича, 2020 — Часть 1 : Способы анализа — 2020. — 72 с. URL: https://e.lanbook.com/book/180081			

Э10	Защита программ и данных : учебное пособие. — Санкт-Петербург : СПбГУТ им. М.А. Бонч-Бруевича, 2020 — Часть 2 : Способы защиты анализа — 2020. — 52 с. URL: : https://e.lanbook.com/book/180082
Э11	Юричев Д. Reverse Engineering для начинающих. URL: https://beginners.re/RE4B-RU.pdf
Э12	Тобиас Клейн Дневник охотника за ошибками. Путешествие через джунгли проблем безопасности программного обеспечения - Москва : ДМК Пресс, 2013. - 240 с. URL: https://e.lanbook.com/book/4812
Э13	Ховард М. 19 смертных грехов, угрожающих безопасности программ. Как не допустить типичных ошибок / М. Ховард, Д. Лебланк, Д. Виега. - Москва: ДМК Пресс, 2009. - 288 с. URL: https://e.lanbook.com/book/1118
Э14	Ховард М. Как написать безопасный код на C++, Java, Perl, PHP, ASP.NET / М. Ховард, Д. Лебланк, Д. Виега. - Москва: ДМК Пресс, 2018. - 288 с. URL: https://www.iprbookshop.ru/124992.html
Э15	Управление рисками информационной безопасности (конспект лекции). URL: https://www.securityvision.ru/blog/upravlenie-riskami-informatsionnoy-bezopasnosti-konspekt-lektsii/
Э16	Актуальные вопросы защиты информации . URL: https://lib.itsec.ru/articles2/focus/aktualnye-voprosy-zaschity-informatsii
Э17	Сердечный, А.Л. Методика выявления уязвимостей и недекларированных возможностей в программном обеспечении. URL: https://ict.moscow/static/2-serdechnyj-a-l-4.pdf
Э18	Падарян В.А. Разработка доверенного ПО. Вызовы и перспективы. URL: https://www.tbforum.ru/hubfs/TBF/Presentations2021_online/TBFOFFline/TBF 11-02-21 hall 3/ПАДАРЯН 1_Разработка доверенного ПО - Вызовы и перспективы.pdf
Э19	ФСТЭК России. Методический документ "Методика тестирования обновлений безопасности программных, программно-аппаратных средств" (утв. ФСТЭК России 28.10.2022). URL: https://fstec.ru/files/496/---28--2022-409/893/---28--2022-.pdf
Э20	OWASP Top Ten. URL: https://owasp.org/Top10/
Э21	Обзор публикации NIST SP 800-218 "Secure Software Development Framework (SSDF) Version 1.1: Recommendations for Mitigating the Risk of Software Vulnerabilities". URL: https://www.securityvision.ru/blog/obzor-publikatsii-nist-sp-800-218-secure-software-development-framework-ssdf-version
Э22	NIST SP 800-218, Secure Software Development Framework (SSDF) V1.1: Recommendations for Mitigating the Risk of Software Vulnerabilities. URL: https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-218.pdf
Э23	ГОСТ Р ИСО/МЭК 15408-3-2013 Информационная технология. Методы и средства обеспечения безопасности. Методология оценки безопасности информационных технологий. Часть 3. Компоненты доверия к безопасности. URL: https://docs.cntd.ru/document/1200105711
Э24	Требования по безопасности информации, устанавливающие уровни доверия к средствам технической защиты информации и средствам обеспечения безопасности информационных технологий (выписка). Утверждены Приказом ФСТЭК России №76 от 02.06.2020 г. URL: https://docs.cntd.ru/document/566305930
Э25	ГОСТ Р 56939-2016 Защита информации. Разработка безопасного программного обеспечения. URL: https://docs.cntd.ru/document/1200135525
Э26	ГОСТ Р 58412-2019 Защита информации. Разработка безопасного ПО. Угрозы безопасности информации при разработке ПО. URL: https://docs.cntd.ru/document/1200164529
Э27	ГОСТ Р ИСО/МЭК 18045-2013 Информационная технология (ИТ). Методы и средства обеспечения безопасности. Методология оценки безопасности информационных технологий. URL: https://docs.cntd.ru/document/1200105309
Э28	ГОСТ Р ИСО-МЭК 27034-1-2014 Информационные технологии. Методы и средства обеспечения безопасности. Безопасность приложений. Часть 1. Обзор и общие понятия. URL: https://docs.cntd.ru/document/1200112883
Э29	ГОСТ Р ИСО-МЭК 27034-7-2020 Информационные технологии. Методы и средства обеспечения безопасности. Безопасность приложений. Часть 7. Основы прогнозирования доверия. URL: https://docs.cntd.ru/document/1200177466
Э30	ГОСТ Р ИСО/МЭК 27005-2010 Информационные технологии. Методы и средства обеспечения безопасности. Менеджмент риска информационной безопасности. URL: https://docs.cntd.ru/document/1200084141

6.3 Перечень программного обеспечения и информационных справочных систем

6.3.1 Перечень лицензионного и свободно распространяемого программного обеспечения, в том числе отечественного производства

Наименование	Описание
Операционная система Windows	Коммерческая лицензия
Kaspersky Endpoint Security	Коммерческая лицензия
Adobe Acrobat Reader	Свободное ПО
LibreOffice	Свободное ПО
VirtualBox	Свободное ПО
VMware Player	Свободное ПО

6.3.2 Перечень информационных справочных систем

6.3.2.1	Система КонсультантПлюс http://www.consultant.ru

7. МАТЕРИАЛЬНО-ТЕХНИЧЕСКОЕ ОБЕСПЕЧЕНИЕ ДИСЦИПЛИНЫ (МОДУЛЯ)	
1	268 учебно-административный корпус. компьютерный класс для проведения учебных занятий Специализированная мебель (20 компьютерных столов), 20 персональных компьютеров. Возможность подключения к сети Интернет и обеспечением доступа в электронную информационно-образовательную среду РГРТУ.
2	270 учебно-административный корпус. учебная аудитория для проведения учебных занятий. Специализированная мебель (42 посадочных места), магнитно-маркерная доска. Мультимедиа проектор, 1 экран. Рабочее место (2 стола), 1 персональный компьютер, 1 ноутбук.
8. МЕТОДИЧЕСКИЕ МАТЕРИАЛЫ ПО ДИСЦИПЛИНЕ (МОДУЛЮ)	
Методические материалы по данной дисциплине приведены в Приложении 2 к рабочей программе дисциплины (см. документ «Методическое обеспечение дисциплины «Разработка безопасного программного обеспечения компьютерных систем»).	

Оператор ЭДО ООО "Компания "Тензор"

ДОКУМЕНТ ПОДПИСАН ЭЛЕКТРОННОЙ ПОДПИСЬЮ

ПОДПИСАНО ЗАВЕДУЮЩИМ КАФЕДРЫ	**ФГБОУ ВО "РГРТУ", РГРТУ,** Пржегорлинский Виктор Николаевич, Преподаватель	**15.09.24** 17:59 (MSK)	Простая подпись
ПОДПИСАНО ЗАВЕДУЮЩИМ ВЫПУСКАЮЩЕЙ КАФЕДРЫ	**ФГБОУ ВО "РГРТУ", РГРТУ,** Пржегорлинский Виктор Николаевич, Преподаватель	**15.09.24** 17:59 (MSK)	Простая подпись
ПОДПИСАНО НАЧАЛЬНИКОМ УРОП	**ФГБОУ ВО "РГРТУ", РГРТУ,** Ерзылёва Анна Александровна, Начальник УРОП	**17.09.24** 09:59 (MSK)	Простая подпись