


УТВЕРЖДАЮ
Декан факультета

 Юнаков Л. П.
(подпись) ФИО
«31» 05 2022

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ РАЗРАБОТКИ ПРОГРАММНОГО ОБЕСПЕЧЕНИЯ

Направление/специальность подготовки	24.05.04 Навигационно-баллистическое обеспечение применения космической техники
Специализация/профиль/программа подготовки	Проектная баллистика ракет и космических систем
Уровень высшего образования	Специалитет
Форма обучения	Очная
Факультет	А Ракетно-космической техники
Выпускающая кафедра	А5 ДИНАМИКА И УПРАВЛЕНИЕ ПОЛЕТОМ ЛЕТАТЕЛЬНЫХ АППАРАТОВ
Кафедра-разработчик рабочей программы	А5 ДИНАМИКА И УПРАВЛЕНИЕ ПОЛЕТОМ ЛЕТАТЕЛЬНЫХ АППАРАТОВ

КУРС	СЕМЕСТР	ОБЩАЯ ТРУДОЁМКОСТЬ (ЗАЧЕТНЫХ ЕДИНИЦ)	ОБЩАЯ ТРУДОЁМКОСТЬ	ЧАСЫ (по наличию видов занятий)								ВИД ПРОМЕЖУТОЧНОГО КОНТРОЛЯ
				АУДИТОРНЫЕ ЗАНЯТИЯ				САМОСТОЯТЕЛЬНАЯ РАБОТА				
				ВСЕГО	ЛЕКЦИИ	ЛАБОРАТОРНЫЙ ПРАКТИКУМ	ПРАКТИЧЕСКИЕ ЗАНЯТИЯ	ВСЕГО	КУРСОВОЙ ПРОЕКТ	КУРСОВАЯ РАБОТА	ДРУГИЕ ВИДЫ САМОСТ. РАБОТЫ	
5	9	3	108	68	0	0	68	40	0	0	40	диф. зач.

ЛИСТ СОГЛАСОВАНИЯ

РАБОЧАЯ ПРОГРАММА СОСТАВЛЕНА В СООТВЕТСТВИИ С ТРЕБОВАНИЯМИ ФЕДЕРАЛЬНОГО
ГОСУДАРСТВЕННОГО ОБРАЗОВАТЕЛЬНОГО СТАНДАРТА ВЫСШЕГО ОБРАЗОВАНИЯ (ФГОС ВО)

24.05.04 Навигационно-баллистическое обеспечение применения космической техники

год набора группы: 2022

Программу составил:

Кафедра А5 ДИНАМИКА И УПРАВЛЕНИЕ ПОЛЕТОМ
ЛЕТАТЕЛЬНЫХ АППАРАТОВ
Петрова Ирина Леонидовна, к.т.н., доцент



Программа рассмотрена
на заседании кафедры-разработчика
рабочей программы А5 ДИНАМИКА И УПРАВЛЕНИЕ ПОЛЕТОМ ЛЕТАТЕЛЬНЫХ АППАРАТОВ

Заведующий кафедрой Толпегин О.А., д.т.н., проф.



Программа рассмотрена
на заседании выпускающей кафедры

А5 ДИНАМИКА И УПРАВЛЕНИЕ ПОЛЕТОМ ЛЕТАТЕЛЬНЫХ АППАРАТОВ

Заведующий кафедрой Толпегин О.А., д.т.н., проф.



РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ РАЗРАБОТКИ ПРОГРАММНОГО ОБЕСПЕЧЕНИЯ

Разделы рабочей программы

1. ЦЕЛИ ОСВОЕНИЯ ДИСЦИПЛИНЫ
2. МЕСТО ДИСЦИПЛИНЫ В СТРУКТУРЕ ООП ВО
3. СТРУКТУРА И СОДЕРЖАНИЕ ДИСЦИПЛИНЫ
4. ФОРМЫ КОНТРОЛЯ ОСВОЕНИЯ ДИСЦИПЛИНЫ
5. УЧЕБНО-МЕТОДИЧЕСКОЕ И ИНФОРМАЦИОННОЕ ОБЕСПЕЧЕНИЕ ДИСЦИПЛИНЫ
6. МАТЕРИАЛЬНО-ТЕХНИЧЕСКОЕ ОБЕСПЕЧЕНИЕ ДИСЦИПЛИНЫ

Приложения к рабочей программе дисциплины

- Приложение 1. Аннотация рабочей программы
- Приложение 2. Технологии и формы обучения
- Приложение 3. Фонды оценочных средств

1. ЦЕЛИ ОСВОЕНИЯ ДИСЦИПЛИНЫ

Целью освоения дисциплины является формирование следующих компетенций:

ПСК-5 — Способность к разработке структуры систем управления БПЛА

Формированию компетенций служит достижение следующих результатов образования:

ПСК-5

знания:

- основные угрозы для программного обеспечения, классификация и виды уязвимостей;
- специфика безопасности web-приложений. Внедрение SQL-кода различных типов;
- уязвимости, связанные с web-серверами и web-клиентами;
- "предсказуемые" параметры и уязвимости аутентификации;
- специфика безопасности desktop-приложений, переполнение буфера, огрехи формата строк;
- целочисленные переполнения, некорректная обработка исключений и ошибок;
- внедрение команд, отказ от обслуживания;
- специфика безопасности мобильных-приложений;
- понимание общих угроз в сфере криптографии;
- ручной анализ кода, автоматизированный статический и динамический анализ кода;
- динамическое тестирование, фаззинг;

умения:

- составление примера поверхности атаки на демонстрационное ПО;
- применять ручной, автоматизированный статический и динамический анализ кода;
- применять полученные знания в практике построения защищенных систем обработки информации при разработке структуры систем управления беспилотными летательными аппаратами, включая конфиденциальную информацию и обработку персональных данных;

навыки:

- применять полученные знания на практике для приемов разработки безопасного ПО для систем управления беспилотных летательных аппаратов.

2. МЕСТО ДИСЦИПЛИНЫ В СТРУКТУРЕ ООП ВО

Дисциплина **ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ РАЗРАБОТКИ ПРОГРАММНОГО ОБЕСПЕЧЕНИЯ** является дисциплиной **части, формируемой участниками образовательных отношений блока 1**, программы подготовки по направлению *24.05.04 Навигационно-баллистическое обеспечение применения космической техники*.

Содержание дисциплины является логическим продолжением дисциплин: **МАТЕМАТИЧЕСКОЕ МОДЕЛИРОВАНИЕ В ПРОЕКТНОЙ БАЛЛИСТИКЕ, КОМПЬЮТЕРНЫЙ ПРАКТИКУМ, ЦИФРОВИЗАЦИЯ ВЫСОКОТЕХНОЛОГИЧНЫХ ОТРАСЛЕЙ ПРОМЫШЛЕННОСТИ, ПРОГРАММИРОВАНИЕ НА ЯЗЫКЕ ВЫСОКОГО УРОВНЯ, ВВЕДЕНИЕ В ИНФОРМАЦИОННЫЕ ТЕХНОЛОГИИ**.

Содержание дисциплины является основой для освоения дисциплин: **ИНТЕЛЛЕКТУАЛЬНЫЕ СИСТЕМЫ АВТОМАТИЧЕСКОГО УПРАВЛЕНИЯ, ВИЗУАЛИЗАЦИЯ ПРОГРАММНОГО ОБЕСПЕЧЕНИЯ, АДАПТИВНЫЕ СИСТЕМЫ АВТОМАТИЧЕСКОГО УПРАВЛЕНИЯ, НАУЧНО-ИССЛЕДОВАТЕЛЬСКАЯ РАБОТА В СЕМЕСТРЕ**.

Предварительные компетенции, сформированные у обучающегося до начала изучения дисциплины:

- ОПК-1 — Способен применять естественнонаучные и общетехнические знания, методы математического анализа и моделирования, навыки теоретического и экспериментального исследования для решения различных задач профессиональной деятельности
- ОПК-2 — Способен понимать принципы работы современных информационных технологий и использовать их при решении задач профессиональной деятельности
- ОПК-8 — Способен разрабатывать алгоритмы и компьютерные программы, пригодные для практического применения
- ПК-91 — способен к коммуникации и кооперации в цифровой среде, использованию различных цифровых средств, позволяющих во взаимодействии с другими людьми достигать поставленных целей
- ПК-92 — способен к саморазвитию в условиях неопределенности, формулировать себе образовательные цели под возникающие жизненные задачи, выбирать способы решения и направления развития
- ПК-93 — способен генерировать новые идеи для решения задач цифровой экономики, абстрагироваться от стандартных моделей, перестраивать сложившиеся способы решения задач, выдвигать альтернативные варианты действий с целью выработки новых оптимальных алгоритмов
- ПК-94 — способен к управлению информацией и данными, поиску источников информации и данных, восприятию, анализу, запоминанию и передаче информации с использованием цифровых средств, а также с помощью алгоритмов при работе с полученными из различных источников данными с целью эффективного использования полученной информации для решения задач
- ПК-95 — способен к критическому мышлению в цифровой среде, оценке информации, ее достоверности, построению логических умозаключений на основании поступающих информации и данных

3. СТРУКТУРА И СОДЕРЖАНИЕ ДИСЦИПЛИНЫ

Общая трудоемкость дисциплины составляет 3 з.е., 108 ч.

3.1. Содержание (дидактика) дисциплины

КУРС	СЕМЕСТР	Наименование разделов и дидактических единиц	ВСЕГО	Аудиторные занятия в контактной форме		Самостоятельная работа студентов	Формируемая компетенция, %
				ВСЕГО	Практические занятия		ПСК-5
5	9	Раздел 1. Введение в разработку безопасного ПО. 1.1. Примеры стандартов принятых в разных странах. 1.2. Примеры основных угроз для ПО. 1.3. Классификация и виды уязвимостей.	13	8	8	5	10
5	9	Раздел 2. Специфика безопасности web-приложений. 2.1. Внедрение SQL-кода различного типа. 2.2. Уязвимости, связанные с web-серверами. 2.3. Уязвимости web-клиентов. 2.4. "Предсказуемые" параметры и уязвимости аутентификации.	26	16	16	10	20
5	9	Раздел 3. Специфика безопасности desktop-приложений. 3.1. Переполнение буфера. 3.2. Огрехи формата строк. 3.3. Целочисленные переполнения. 3.4. Некорректная обработка исключений и ошибок. 3.5. Внедрение команд. 3.6. Отказ от обслуживания. 3.7. Ситуация гонки.	26	16	16	10	20
5	9	Раздел 4. Специфика безопасности мобильных приложений. 4.1. Понимание общих угроз в сфере криптографии. 4.2. Составление примера поверхности атаки на демонстрационное ПО.	17	12	12	5	20
5	9	Раздел 5. Анализ кода. 5.1. Ручной анализ кода 5.2. Автоматизированный статический и динамический анализ кода.	13	8	8	5	10
5	9	Раздел 6. Динамическое тестирование. 6.1. Фаззинг. 6.2. Примеры лучших практик и приемов разработки безопасного ПО.	13	8	8	5	20
Всего за 9 семестр			108	68	68	40	100
Всего по дисциплине			108	68	68	40	100

3.2. Аудиторный практикум

№ п/п	Номер и наименование раздела дисциплины	Тема практического занятия	Объем, ауд. часов
1	Раздел 1. Введение в разработку безопасного ПО.	Примеры стандартов принятых в разных странах. Примеры основных угроз для ПО. Классификация и виды уязвимостей	8
2	Раздел 2. Специфика безопасности web-приложений.	Внедрение SQL-кода различного типа	4
3		Уязвимости, связанные с web-серверами	4
4		Уязвимости web-клиентов	4
5		"Предсказуемые" параметры и уязвимости аутентификации	4
6	Раздел 3. Специфика безопасности desktop-приложений.	Переполнение буфера. Огрехи формата строк	4
7		Целочисленные переполнения. Некорректная обработка исключений и ошибок	4
8		Внедрение команд. Отказ от обслуживания	4
9		Ситуация гонки	4
10	Раздел 4. Специфика безопасности мобильных приложений.	Специфика безопасности мобильных-приложений	4
11		Понимание общих угроз в сфере криптографии	4
12		Составление примера поверхности атаки на демонстрационное ПО	4
13	Раздел 5. Анализ кода.	Ручной анализ кода	4
14		Автоматизированный статический и динамический анализ кода	4
15	Раздел 6. Динамическое тестирование.	Динамическое тестирование. Фаззинг	4
16		Примеры лучших практик и приемов разработки безопасного ПО	4
Всего за 9 семестр			68

3.3. Самостоятельная работа студента (СРС)

№ п/п	Номер и наименование раздела дисциплины	Содержание учебного задания	Объем, часов

1	Раздел 1. Введение в разработку безопасного ПО.	Изучение предусмотренных программой дидактических единиц по рекомендуемой литературе. Подготовка к практическим занятиям	5
2	Раздел 2. Специфика безопасности web-приложений.	Изучение предусмотренных программой дидактических единиц по рекомендуемой литературе. Подготовка к практическим занятиям	10
3	Раздел 3. Специфика безопасности desktop-приложений.	Изучение предусмотренных программой дидактических единиц по рекомендуемой литературе. Подготовка к практическим занятиям	10
4	Раздел 4. Специфика безопасности мобильных приложений.	Изучение предусмотренных программой дидактических единиц по рекомендуемой литературе	5
5	Раздел 5. Анализ кода.	Изучение предусмотренных программой дидактических единиц по рекомендуемой литературе. Подготовка к практическим занятиям	5
6	Раздел 6. Динамическое тестирование.	Изучение предусмотренных программой дидактических единиц по рекомендуемой литературе. Подготовка к практическим занятиям	5
Всего за 9 семестр			40

4. ФОРМЫ КОНТРОЛЯ ОСВОЕНИЯ ДИСЦИПЛИНЫ

СЕМЕСТР	НЕДЕЛИ СЕМЕСТРА																
	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17
9			Задан			ДР			Задан	ДР		Задан			Задан	ДР	диф. зач.

Условные обозначения:

- ДР – диагностическая работа;
- Задан – задание;
- Тест – тест;
- диф. зач. – дифференцированный зачет.

Текущий контроль успеваемости студентов проводится в дискретные временные интервалы в следующих формах:

- диагностическая работа;
- задание;
- тест.

Промежуточная аттестация проводится в формах:

- дифференцированный зачет.

5. УЧЕБНО-МЕТОДИЧЕСКОЕ И ИНФОРМАЦИОННОЕ ОБЕСПЕЧЕНИЕ ДИСЦИПЛИНЫ

5.1. Основная литература по дисциплине:

1. А. В. Бабаш, Е. К. Баранова. . Криптографические методы защиты информации. М.: КноРус, 2018, 70 экз.
2. А. Голдсмит. . Беспроводные коммуникации. М.: Техносфера, 2011, 5 экз.
3. А. И. Гусева, В. С. Киреев. . Вычислительные системы, сети и телекоммуникации. М.: Академия, 2014, эл. рес.
4. А. П. Пятибратов, Л. П. Гудыно, А. А. Кириченко. . Вычислительные системы, сети и телекоммуникации. М.: КноРус, 2017, 60 экз.
5. В. И. Ярочкин. . Информационная безопасность. М.: Академический Проект, 2006, 48 экз.
6. В. П. Мельников, А. И. Куприянов, Т. Ю. Васильева. . Информационная безопасность. М.: РУСАЙНС, 2017, 70 экз.

5.2. Дополнительная литература по дисциплине:

не требуется.

5.3. Периодические издания:

1. Автоматизация процессов управления;
2. Известия Российской академии ракетных и артиллерийских наук.

5.4. Перечень ресурсов информационно-телекоммуникационной сети "Интернет", необходимых для освоения дисциплины, электронные библиотечные системы:

1. <https://urait.ru> — Главная – Образовательная платформа Юрайт. Для вузов и ссузов.;
2. <https://ibooks.ru> — ЭБС Айбукс.ру - это большой выбор актуальной литературы для вашей библиотеки в электронном виде;
3. <https://e.lanbook.com> — ЭБС Лань;
4. <http://www.tnt-ebook.ru> — TNT-EBOOK - Электронно-библиотечная система;
5. <http://library.voenmeh.ru> — Фундаментальная библиотека БГТУ «ВОЕНМЕХ» им. Д.Ф. Устинова.

Современные профессиональные базы данных:

1. <https://rusneb.ru> – Национальная электронная библиотека (НЭБ);
2. <https://cyberleninka.ru/> - Научная электронная библиотека «Киберленинка»;
<http://www.rfbr.ru/rffi/ru/library> - Полнотекстовая электронная библиотека Российского фонда фундаментальных исследований.

Информационные справочные системы:

1. Техэксперт – Информационный портал технического регулирования: Нормы, правила, стандарты РФ;
2. http://library.voenmeh.ru/jirbis2/index.php?option=com_irbis&view=irbis&Itemid=457 - БД ГОСТов собственной генерации БГТУ "ВОЕНМЕХ" им. Д. Ф. Устинова;
3. <http://www.consultant.ru/>- КонсультантПлюс- информационный портал правовой информации.

5.5. Программное обеспечение:

1. Linux;
2. LibreOffice;
3. Qt Creator 4.11.14;
4. Bloodshed Dev-C++.

5.6. Информационные технологии:

взаимодействие с обучающимися посредством ЭИОС Moodle БГТУ «ВОЕНМЕХ» им. Д.Ф. Устинова.

6. МАТЕРИАЛЬНО-ТЕХНИЧЕСКОЕ ОБЕСПЕЧЕНИЕ ДИСЦИПЛИНЫ

6.1. Практические занятия:

1. Linux;
2. LibreOffice;
3. Qt Creator 4.11.14;
4. Bloodshed Dev-C++.

6.2. Прочее:

1. рабочее место преподавателя, оснащенное компьютером с доступом в Интернет;
2. рабочие места студентов, оснащенные компьютерами с доступом в Интернет, предназначенные для работы в электронной образовательной среде.

Аннотация рабочей программы

Дисциплина **ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ РАЗРАБОТКИ ПРОГРАММНОГО ОБЕСПЕЧЕНИЯ** является дисциплиной **части, формируемой участниками образовательных отношений блока 1**, программы подготовки по направлению *24.05.04 Навигационно-баллистическое обеспечение применения космической техники*. Дисциплина реализуется на факультете А Ракетно-космической техники БГТУ "ВОЕНМЕХ" им. Д.Ф. Устинова кафедрой А5 ДИНАМИКА И УПРАВЛЕНИЕ ПОЛЕТОМ ЛЕТАТЕЛЬНЫХ АППАРАТОВ.

Дисциплина нацелена на формирование *компетенций*:
ПСК-5 Способность к разработке структуры систем управления БПЛА.

Содержание дисциплины охватывает круг вопросов, связанных с основными понятиями и видами защищаемой информации, процессом организации системы защиты предприятия, утечками информации, методами защиты информации и алгоритмами шифрования. Рассматриваются основные способы проникновения вирусов в информационные системы и сети, виды вирусов и защита от них, формальные модели защищаемых систем и их применение. Сетевая защита и безопасность web и электронной почты.

Программой дисциплины предусмотрены следующие **виды контроля**:

Текущий контроль успеваемости студентов проводится в дискретные временные интервалы в следующих формах:

- диагностическая работа;
- задание;
- тест.

Промежуточная аттестация проводится в формах:

- дифференцированный зачет.

Общая трудоемкость освоения дисциплины составляет **3 з.е., 108 ч.** Программой дисциплины предусмотрены практические занятия (**68 ч.**), самостоятельная работа студента (**40 ч.**).

ТЕХНОЛОГИИ И ФОРМЫ ОБУЧЕНИЯ

Рекомендации по освоению дисциплины для студента

Трудоемкость освоения дисциплины составляет 108 ч., из них 68 ч. аудиторных занятий, и 40 ч., отведенных на самостоятельную работу студента.

Рекомендации по распределению учебного времени по видам самостоятельной работы и разделам дисциплины приведены в таблице.

Контроль освоения дисциплины производится в соответствии с Положением о текущем, рубежном контроле успеваемости и промежуточной аттестации обучающихся.

Формы контроля и критерии оценивания приведены в приложении 3 к Рабочей программе.

Наименование работы	Рекомендуемая литература	Трудоемкость, час.
Раздел 1. Введение в разработку безопасного ПО.		
Изучение предусмотренных программой дидактических единиц по рекомендуемой литературе. Подготовка к практическим занятиям	А. В. Бабаш, Е. К. Баранова. . Криптографические методы защиты информации: М.: КноРус, 2018 (Главы 1 - 4)	5
Итого по разделу 1		5
Раздел 2. Специфика безопасности web-приложений.		
Изучение предусмотренных программой дидактических единиц по рекомендуемой литературе. Подготовка к практическим занятиям	А. Голдсмит. . Беспроводные коммуникации: М.: Техносфера, 2011 (Главы 1 - 3)	10
Итого по разделу 2		10
Раздел 3. Специфика безопасности desktop-приложений.		
Изучение предусмотренных программой дидактических единиц по рекомендуемой литературе. Подготовка к практическим занятиям	А. П. Пятибратов, Л. П. Гудыно, А. А. Кириченко. . Вычислительные системы, сети и телекоммуникации: М.: КноРус, 2017 (Раздел 1: Глава 2, Раздел 2: Главы: 7, 9 - 11)	10
Итого по разделу 3		10
Раздел 4. Специфика безопасности мобильных приложений.		
Изучение предусмотренных программой дидактических единиц по рекомендуемой литературе	В. И. Ярочкин. . Информационная безопасность: М.: Академический Проект, 2006 (Главы 3,4)	5
Итого по разделу 4		5
Раздел 5. Анализ кода.		
Изучение предусмотренных программой дидактических единиц по рекомендуемой литературе. Подготовка к практическим занятиям	А. И. Гусева, В. С. Киреев. . Вычислительные системы, сети и телекоммуникации: М.: Академия, 2014 (Разделы 4 - 6)	5
Итого по разделу 5		5
Раздел 6. Динамическое тестирование.		
Изучение предусмотренных программой дидактических единиц по рекомендуемой литературе. Подготовка к практическим занятиям	В. П. Мельников, А. И. Куприянов, Т. Ю. Васильева. . Информационная безопасность: М.: РУСАЙНС, 2017 (Главы 4 - 7)	5
Итого по разделу 6		5

ФОНДЫ ОЦЕНОЧНЫХ СРЕДСТВ

Фонды оценочных средств, позволяющие оценить результаты обучения по данной дисциплине, включают в себя:

- диагностическая работа
- тест;
- задание;
- дифференцированный зачет.

Критерии оценивания

Диагностическая работа

Диагностическая работа проводится в форме теста в ЭИОС Moodle:

- при правильном ответе менее чем на 60% вопросов - не аттестация;
- при правильном ответе на 60% вопросов и более - аттестация.

Тест

Тестовое задание состоит из 5 вопросов.

Верный ответ на один вопрос оценивается в "1" балл. Успешное написание Тестового задания подразумевает правильный ответ не менее чем на три вопроса (3 балла).

Тестовые задания по дисциплине приведены в УМК по дисциплине.

Задание

По каждому из разделов дисциплины (кроме раздела 1) выполняется индивидуальное задание.

Варианты индивидуальных заданий приведены в УМК по дисциплине.

Допуск к заданию не требуется. Задания выполняются и защищаются на практических занятиях.

Защита Задания проходит в форме доклада обучающегося по выполненной работе и ответов на вопросы преподавателя. В случае, если поведение обучающегося во время защиты соответствуют необходимым требованиям, он получает максимальное количество баллов (5).

Основаниями для снижения количества баллов в диапазоне от max (5) до min (3) являются:

- несоответствие программного приложения указанным требованиям, его неэффективность или некорректная работа;
- неверные ответы на вопросы или отсутствие ответов;
- несвоевременность выполнения и защиты индивидуального задания.

Для получения оценки "5" - студент должен ответить верно на 5 вопросов преподавателя по теме Задания,

для получения оценки "4" - студент должен ответить верно на 4 вопроса преподавателя по теме Задания,

для получения оценки "3" - студент должен ответить на 3 вопроса преподавателя по теме Задания.

Варианты заданий представлены в УМК дисциплины.

Дифференцированный зачет

Обучающийся имеет право на получение минимальной положительной оценки при условии успешного прохождения текущего контроля успеваемости в форме диагностической работы в соответствии с графиком раздела 4.

Промежуточная аттестация по дисциплине проводится в форме дифференцированного зачета, который проставляется при условии выполнения всех мероприятий, предусмотренных графиком контрольных мероприятий по результатам работы в семестре.

Оценка за дифференцированный зачет выставляется, как среднее арифметическое суммарных оценок, полученных обучающимся за выполнение 5 заданий (по каждому из разделов дисциплины, кроме раздела 1) и теста.

Критерии оценивания дифференцированного зачета :

- оценка «зачтено - отлично» выставляется обучающемуся, если среднее арифметическое оценок, полученных им за выполнение 5 заданий и теста равно 4.5 баллов и выше;
- оценка «зачтено - хорошо» выставляется обучающемуся, если среднее арифметическое оценок, полученных им за выполнение 5 заданий и теста находится в пределах 3.5 - 4.4 балла;
- оценка «не зачтено» выставляется обучающемуся, если среднее арифметическое оценок, полученных им за выполнение 5 заданий и теста находится в пределах 2.4 балла и ниже;
- во всех других случаях обучающемуся выставляется оценка «зачтено - удовлетворительно».

Паспорт фонда оценочных средств

КУРС	СЕМЕСТР	Наименование разделов и дидактических единиц	ВСЕГО	Аудиторные занятия в контактной форме		Самостоятельная работа студентов	Формируемая компетенция, %	НАИМЕНОВАНИЕ ОЦЕНОЧНОГО СРЕДСТВА
				ВСЕГО	Практические занятия		ПСК-5	
5	9	Раздел 1. Введение в разработку безопасного ПО.	13	8	8	5	10	Тест
5	9	Раздел 2. Специфика безопасности web-приложений.	26	16	16	10	20	Тест, Задание
5	9	Раздел 3. Специфика безопасности desktop-приложений.	26	16	16	10	20	Тест, Задание
5	9	Раздел 4. Специфика безопасности мобильных приложений.	17	12	12	5	20	Тест, Задание
5	9	Раздел 5. Анализ кода.	13	8	8	5	10	Тест, Задание
5	9	Раздел 6. Динамическое тестирование.	13	8	8	5	20	Тест, Задание
Всего за 9 семестр			108	68	68	40	100	
Всего по дисциплине			108	68	68	40	100	