

УТВЕРЖДАЮ  
Декан факультета

\_\_\_\_\_  
(подпись) Юнаков Л. П.  
ФИО  
«\_\_\_» \_\_\_\_\_ 20\_\_

## РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ РАЗРАБОТКИ ПРОГРАММНОГО ОБЕСПЕЧЕНИЯ

Направление/специальность подготовки	24.05.06 Системы управления летательными аппаратами
Специализация/профиль/программа подготовки	Системы управления беспилотными летательными аппаратами
Уровень высшего образования	Специалитет
Форма обучения	Очная
Факультет	А Ракетно-космической техники
Выпускающая кафедра	А5 ДИНАМИКА И УПРАВЛЕНИЕ ПОЛЁТОМ ЛЕТАТЕЛЬНЫХ АППАРАТОВ
Кафедра-разработчик рабочей программы	А5 ДИНАМИКА И УПРАВЛЕНИЕ ПОЛЁТОМ ЛЕТАТЕЛЬНЫХ АППАРАТОВ

КУРС	СЕМЕСТР	ОБЩАЯ ТРУДОЁМКОСТЬ (ЗАЧЕТНЫХ ЕДИНИЦ)	ЧАСЫ (по наличию видов занятий)									ВИД ПРОМЕЖУТОЧНОГО КОНТРОЛЯ
			ОБЩАЯ ТРУДОЁМКОСТЬ	АУДИТОРНЫЕ ЗАНЯТИЯ				САМОСТОЯТЕЛЬНАЯ РАБОТА				
				ВСЕГО	ЛЕКЦИИ	ЛАБОРАТОРНЫЙ ПРАКТИКУМ	ПРАКТИЧЕСКИЕ ЗАНЯТИЯ	ВСЕГО	КУРСОВОЙ ПРОЕКТ	КУРСОВАЯ РАБОТА	ДРУГИЕ ВИДЫ САМОСТ. РАБОТЫ	
5	9	3	108	51	0	0	51	57	0	0	57	диф. зач.

*ЛИСТ СОГЛАСОВАНИЯ*

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

**24.05.06 Системы управления летательными аппаратами**

год набора группы: 2024

Программу составил:

Кафедра А5 ДИНАМИКА И УПРАВЛЕНИЕ ПОЛЕТОМ  
ЛЕТАТЕЛЬНЫХ АППАРАТОВ

Петрова Ирина Леонидовна, к.т.н., доцент, 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:

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
ПСК-2.9 — Способность к разработке программного обеспечения для систем управления БПЛА

Формированию компетенций служит достижение следующих результатов образования:

## **ПК-93**

*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;
- 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;.

## **ПСК-2.9**

*знания:*

- основные угрозы для программного обеспечения (ПО), 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;
- 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 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 *24.05.06 Системы управления летательными аппаратами*.

Содержание дисциплины является логическим продолжением дисциплин: **КОМПЬЮТЕРНЫЙ ПРАКТИКУМ, ПРОГРАММИРОВАНИЕ НА ЯЗЫКЕ ВЫСОКОГО УРОВНЯ, ВВЕДЕНИЕ В ИНФОРМАЦИОННЫЕ ТЕХНОЛОГИИ**.

Содержание дисциплины является основой для освоения дисциплин: **ВИЗУАЛИЗАЦИЯ ПРОГРАММНОГО ОБЕСПЕЧЕНИЯ, АДАПТИВНЫЕ СИСТЕМЫ АВТОМАТИЧЕСКОГО УПРАВЛЕНИЯ**.

Предварительные компетенции, сформированные у обучающегося до начала изучения дисциплины:

- ОПК-2 — Способен понимать принципы работы современных информационных технологий и использовать их для решения задач профессиональной деятельности
- ОПК-9 — 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-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

### 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		ПК-93	ПСК-2.9
5	9	<b>Раздел 1. Введение в разработку безопасного ПО.</b> 1.1. Примеры стандартов принятых в разных странах. 1.2. Примеры основных угроз для ПО. 1.3. Классификация и виды уязвимостей.	16	6	6	10	15	15
5	9	<b>Раздел 2. Специфика безопасности web-приложений.</b> 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.	22	12	12	10	10	10
5	9	<b>Раздел 3. Специфика безопасности desktop-приложений.</b> 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.	22	12	12	10	20	20
5	9	<b>Раздел 4. Специфика безопасности мобильных приложений.</b> 4.1. Понимание общих угроз в сфере криптографии. 4.2. Составление примера поверхности атаки на демонстрационное ПО.	18	8	8	10	10	10
5	9	<b>Раздел 5. Анализ кода.</b> 5.1. Ручной анализ кода 5.2. Автоматизированный статический и динамический анализ кода.	16	6	6	10	25	25
5	9	<b>Раздел 6. Динамическое тестирование.</b> 6.1. Фаззинг. 6.2. Примеры лучших практик и приемов разработки безопасного ПО.	14	7	7	7	20	20
<b>Всего за 9 семестр</b>			108	51	51	57	100	100
<b>Всего по дисциплине</b>			108	51	51	57	100	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	6
2	Раздел 2. Специфика безопасности web-приложений.	Внедрение SQL-кода различного типа	4
3		Уязвимости, связанные с web-серверами	4
4		Уязвимости web-клиентов	2
5		"Предсказуемые" параметры и уязвимости аутентификации	2
6	Раздел 3. Специфика безопасности desktop-приложений.	Переполнение буфера. Огрехи формата строк	4
7		Целочисленные переполнения. Некорректная обработка исключений и ошибок	2
8		Внедрение команд. Отказ от обслуживания	4
9		Ситуация гонки	2
10	Раздел 4. Специфика безопасности мобильных приложений.	Специфика безопасности мобильных-приложений	4
11		Понимание общих угроз в сфере криптографии	2
12		Составление примера поверхности атаки на демонстрационное ПО	2
13	Раздел 5. Анализ кода.	Автоматизированный статический и динамический анализ кода	4
14		Ручной анализ кода	2
15	Раздел 6. Динамическое тестирование.	Динамическое тестирование. Фаззинг	4
16		Примеры лучших практик и приемов разработки безопасного ПО	3
Всего за 9 семестр			51

### 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	10
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	10
5	Раздел 5. Анализ кода.	Изучение предусмотренных программой дидактических единиц по рекомендуемой литературе. Подготовка к практическим занятиям	10
6	Раздел 6. Динамическое тестирование.	Изучение предусмотренных программой дидактических единиц по рекомендуемой литературе. Подготовка к практическим занятиям	7
<b>Всего за 9 семестр</b>			<b>57</b>

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

### 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](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. Bloodshed Dev-C++;
2. LibreOffice;
3. Linux;
4. Qt Creator 4.11.14.

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

### **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 *24.05.06 Системы управления летательными аппаратами*. 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*:

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;

ПСК-2.9 Способность к разработке программного обеспечения для 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 (**51 ч.**), самостоятельная работа студента (**57 ч.**).

## ТЕХНОЛОГИИ И ФОРМЫ ОБУЧЕНИЯ

### Рекомендации по освоению дисциплины для студента

Трудоемкость освоения дисциплины составляет 108 ч., из них 51 ч. аудиторных занятий, и 57 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.
<b>Раздел 1. Введение в разработку безопасного ПО.</b>		
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)	10
Итого по разделу 1		10
<b>Раздел 2. Специфика безопасности web-приложений.</b>		
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
<b>Раздел 3. Специфика безопасности desktop-приложений.</b>		
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
<b>Раздел 4. Специфика безопасности мобильных приложений.</b>		
Изучение предусмотренных программой дидактических единиц по рекомендуемой литературе	В. И. Ярочкин. . Информационная безопасность: М.: Академический Проект, 2006 (Главы 3,4)	10
Итого по разделу 4		10
<b>Раздел 5. Анализ кода.</b>		
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)	10
Итого по разделу 5		10
<b>Раздел 6. Динамическое тестирование.</b>		
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)	7
Итого по разделу 6		7

## ФОНД ОЦЕНОЧНЫХ СРЕДСТВ

Фонд 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

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		ПК-93	ПСК-2.9	
5	9	Раздел 1. Введение в разработку безопасного ПО.	16	6	6	10	15	15	Тест
5	9	Раздел 2. Специфика безопасности web-приложений.	22	12	12	10	10	10	Тест, Задание
5	9	Раздел 3. Специфика безопасности desktop-приложений.	22	12	12	10	20	20	Тест, Задание
5	9	Раздел 4. Специфика безопасности мобильных приложений.	18	8	8	10	10	10	Тест, Задание
5	9	Раздел 5. Анализ кода.	16	6	6	10	25	25	Тест, Задание
5	9	Раздел 6. Динамическое тестирование.	14	7	7	7	20	20	Тест, Задание
Всего за 9 семестр			108	51	51	57	100	100	
Всего по дисциплине			108	51	51	57	100	100	

## Критерии оценивания

### ПК-93

	<i>Вопросы открытого типа:</i>
№ 1	Что означает Stateful?
№ 2	Как называется период времени, который начинается с момента принятия о решении создания ПО и заканчивается в момент его полного изъятия из эксплуатации?
№ 3	Что означает Stateless?
№ 4	Что помимо идентификации ресурса предоставляет URL?
№ 5	Что означает http в “http://example.com”?
№ 6	Что такое SQL-инъекция?
№ 7	Какое главное требование для срабатывания sql-инъекции?
№ 8	Когда точно возникает уязвимость типа “Внедрение команд”?
№ 9	Что такое XSS?
№ 10	Что такое SSRF?
	<i>Вопросы закрытого типа:</i>
№ 1	Что такое безопасность?
	Положение, при котором не угрожает опасность кому-нибудь или чему-нибудь
	Положение, при котором есть угроза опасности кому-нибудь или чему-нибудь
	Положение, при котором не угрожает опасность кому-нибудь
	Положение, при котором не угрожает опасность чему-нибудь
№ 2	Положение, при котором есть угроза опасности кому-нибудь
	Что такое информационная безопасность?
	практика предотвращения несанкционированного доступа, использования, раскрытия, искажения, изменения, исследования, записи или уничтожения информации, вне зависимости от формы её представления (электронной или физической)
	практика не предотвращения несанкционированного доступа, использования, раскрытия, искажения, изменения, исследования, записи или уничтожения информации, вне зависимости от формы её представления (электронной или физической)
	практика предотвращения несанкционированного доступа, использования, раскрытия, искажения, изменения, исследования, записи или уничтожения информации, вне зависимости от формы её представления (электронной или физической)
№ 3	Из чего состоит триада CIA?
	конфиденциальность, целостность, доступность
	конфиденциальность, целостность, защищенность
	информация, целостность, защищенность
	конфиденциальность, доступность, защищенность
	информация, целостность, доступность
№ 4	Какие категории рекомендуется добавить в обновленный список угроз?
	невозможность отказа, достоверность
	кроссплатформенность
	мобильность

	тестируемость
	жизненность
№ 5	Что является одним из важнейших критериев качества (надежности) разрабатываемого программного обеспечения
	Безопасность
	Доступность
	Конфиденциальность
	Отсутствие целостности
№ 6	Кроссплатформенность
	Три основные категории угроз, определенные Майклом Шрёдером?
	не авторизованное раскрытие информации, не авторизованное изменение информации, не авторизованный отказ в доступе
	авторизованное раскрытие информации, не авторизованное изменение информации, авторизованный отказ в доступе
	не авторизованное раскрытие информации, авторизованное изменение информации, не авторизованный отказ в доступе
	авторизованное раскрытие информации, авторизованное изменение информации, авторизованный отказ в доступе
	не авторизованное раскрытие информации, авторизованное изменение информации, авторизованный отказ в доступе
№ 7	Как называется проект, в рамках которого разработаны методологии тестирования безопасности ПО?
	OWASP
	MITR
	Microsoft
	Cisco
	LOTB
№ 8	Что за тип ошибки был обнаружен в авиалайнерах 787 Dreamliner в 2015 г?
	Переполнение памяти
	Переполнение руля
	Переполнение высоты
	Неправильные права доступа
	Переполнение энергозатрат
№ 9	Какая ошибка привела к неудачному запуску Ariane 5?
	Не адаптировали системы инерциальной навигации из предыдущей версии
	Переполнился указатель на память
	Пропущен символ в коде
	Не совпадение типов переменных
	Не обнулили время старта

Hyper Text Transfer Protocol — «протокол передачи гипертекста»

High Text Transfer Protocol — «протокол передачи высокого текста»

Hyper Tetrahedron Transfer Protocol — «протокол передачи гипер тетрайдера данных»

Hydrogen Tetrahedron Transfer Protocol — «протокол передачи водородного тетрайдера»

High TByte Transfer Protocol — «протокол передачи терабайта данных»

### ПСК-2.9

#### *Вопросы открытого типа:*

№ 1 Что такое URI?

№ 2 Какую из встроенных unix-утилит можно использовать для поиска небезопасных функций?

№ 3 По какому косвенному признаку можно определить наличие уязвимости, если выполнение команды не отображается на странице?

№ 4 В чем отличие метода HEAD от GET?

№ 5 Как называется тип SQL-инъекции, если ошибка в SQL запросе попадает в содержимое HTML страницы?

№ 6 Что такое SSTI?

№ 7 Что такое XXE?

№ 8 Что такое CVE?

№ 9 Что такое cwe?

№ 10 Что такое IDOR?

#### *Вопросы закрытого типа:*

№ 1 Перечислите все уровни модели OSI

Прикладной, Представления, Сеансовый, Транспортный, Сетевой, Канальный, Физический

Прикладной, Физический, Изменчивый, Апелляционный, Магистральный

Магнетический, Санационный, Кодировальный, Шаблонизированный, Заготовительный, Представления

Транспортный, Сетевой, Датированный, Табличный, Характеристический

Прикладной, Идентичный, Сеансовый, Наблюдательский, Хаотичный, Журнальный

№ 2 Перечислите все уровни TCP/IP (DOD) модели

Прикладной, Транспортный, Межсетевой, Канальный

Прикладной, Физический, Изменчивый, Апелляционный

Магнетический, Санационный, Кодировальный, Шаблонизированный

Транспортный, Сетевой, Датированный, Табличный

Прикладной, Идентичный, Сеансовый, Хаотичный

№ 3 Что делает метод OPTIONS?

Список доступных методов для URL

Список доступных протоколов

Список доступных типов аутентификации



	Список доступных http-заголовков
№ 4	<p>Список доступных опций сервера</p> <p>Один из методов предотвращения доступа к чувствительным данным</p> <p>Не хранить чувствительные данные в открытом доступе</p> <p>Опубликовать бэкап базы данных на публичном сервере</p> <p>Оставить установочные файлы на сервере</p> <p>Не удалять скрытые копии отредактированных файлов</p>
№ 5	<p>Не ограничивать доступ к административной панели</p> <p>Какой символ чаще всего используется для определения наличия возможности “Внедрения команд” на уровне ОС в поле ввода пользователем?</p> <p>“,”</p> <p>“.”</p> <p>“/”</p> <p>“{”</p> <p>“!”</p>
№ 6	<p>Как обозначается комментарий в MySQL запросах?</p> <p>--</p> <p>+</p> <p>&amp;</p> <p> </p> <p>=</p>
№ 7	<p>Что такое Межсайтовая подделка запросов (CSRF)?</p> <p>это атака, при которой злоумышленник может выполнить вредоносные действия от вашего имени на другом сервере, используя вашу аутентификацию.</p> <p>это тип атаки на веб-системы, при котором злоумышленник внедряет вредоносный код на страницу, выдаваемую веб-системой, и получает доступ к расширенному доступу к веб-системе или авторизационным данным пользователя</p> <p>это уязвимость, которая позволяет злоумышленникам выполнять запросы на сервере от имени других серверов в сети</p> <p>это тип атаки, при котором хакеры эксплуатируют синтаксис шаблонов на стороне сервера и внедряют вредоносную полезную нагрузку, изменяя поведение шаблона</p> <p>это тип атаки, который использует уязвимости в анализаторах XML. В ходе атаки XXE злоумышленник может внедрить специально созданный XML-контент в приложение, обрабатывающее его</p>
№ 8	<p>Методы защиты от Межсайтовой подделки запросов (CSRF)?</p> <p>CSRF-токен, Same-Site Cookie Flag</p> <p>sql-инъекция</p> <p>межскриптовый запрос</p> <p>sqlmap</p> <p>burp</p>

- № 9            Какие конструкции рекомендуются для эксплуатации JSON-инъекции?
- \$ne , \$gt , \$lt
- \$echo
- \$plus , \$minus
- \$equal
- \$injection
- № 10        Как называется ПО для обеспечения безопасности веб-приложений, используемое для тестирования на проникновение
- BURP
- ROCKETMOVE
- MySQL
- SQLGO
- COPYSQL