

УТВЕРЖДАЮ  
Декан факультета

\_\_\_\_\_ Левихин А.А.

« \_\_\_\_ » \_\_\_\_\_ 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-космическая техника
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)	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: 2026

Программу составили:

Кафедра А5 ДИНАМИКА И УПРАВЛЕНИЕ ПОЛЕТОМ  
ЛЕТАТЕЛЬНЫХ АППАРАТОВ

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

Кафедра А5 ДИНАМИКА И УПРАВЛЕНИЕ ПОЛЕТОМ  
ЛЕТАТЕЛЬНЫХ АППАРАТОВ

Кириллов Артем Владиславович, старший преподаватель

Программа рассмотрена

на заседании кафедры-разработчика

рабочей программы **А5 ДИНАМИКА И УПРАВЛЕНИЕ ПОЛЕТОМ ЛЕТАТЕЛЬНЫХ АППАРАТОВ**

Заведующий кафедрой Петрова И.Л., к.т.н., доц.

Программа рассмотрена

на заседании выпускающей кафедры

**А5 ДИНАМИКА И УПРАВЛЕНИЕ ПОЛЕТОМ ЛЕТАТЕЛЬНЫХ АППАРАТОВ**

Заведующий кафедрой Петрова И.Л., к.т.н., доц.

# **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-9 — Способен к разработке программного обеспечения для систем управления БПЛА

Формированию компетенций служит достижение следующих результатов образования:

## **ПК-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 **обязательной части блока 1** программы подготовки по направлению *24.05.06 Системы управления летательными аппаратами*.

Содержание дисциплины является логическим продолжением дисциплин: **ПРОГРАММИРОВАНИЕ НА ЯЗЫКЕ ВЫСОКОГО УРОВНЯ**.

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

### 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-9
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.	16	6	6	10	15
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.	22	12	12	10	10
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.	22	12	12	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.	18	8	8	10	10
5	9	Раздел 5. Анализ кода. 5.1. Ручной анализ кода 5.2. Автоматизированный статический и динамический анализ кода.	16	6	6	10	25
5	9	Раздел 6. Динамическое тестирование. 6.1. Фаззинг. 6.2. Примеры лучших практик и приемов разработки безопасного ПО.	14	7	7	7	20
Всего за 9 семестр			108	51	51	57	100
Всего по дисциплине			108	51	51	57	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.	Внедрение команд. Отказ от обслуживания	3
7		Ситуация гонки	3
8		Переполнение буфера. Огрехи формата строк	3
9		Целочисленные переполнения. Некорректная обработка исключений и ошибок	3
10	Раздел 4. Специфика безопасности мобильных приложений.	Специфика безопасности мобильных-приложений	3
11		Понимание общих угроз в сфере криптографии	3
12		Составление примера поверхности атаки на демонстрационное ПО	2
13	Раздел 5. Анализ кода.	Автоматизированный статический и динамический анализ кода	3
14		Ручной анализ кода	3
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
<b>9</b>			Задан			ДР			Задан	ДР		Тест			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 **обязательной части блока 1** программы подготовки по направлению 24.05.06 *Системы управления летательными аппаратами*. Дисциплина реализуется на факультете А Ракетно-космическая техника БГТУ "ВОЕНМЕХ" им. Д.Ф. Устинова кафедрой А5 ДИНАМИКА И УПРАВЛЕНИЕ ПОЛЕТОМ ЛЕТАТЕЛЬНЫХ АППАРАТОВ.

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

**Оценочные материалы по дисциплине ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ  
РАЗРАБОТКИ ПРОГРАММНОГО ОБЕСПЕЧЕНИЯ**

**ПК-9 - Способен к разработке программного обеспечения для систем управления БПЛА**

№ 1 Прочитайте текст и установите соответствие

Установите соответствие:

1. SSRF

2. XSS

А. это уязвимость, которая позволяет злоумышленникам выполнять запросы на сервере от имени других серверов в сети

Б. 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

№ 2 Прочитайте текст, выберите правильные ответы и запишите аргументы, обосновывающие выбор ответов

Какие виды тестирования помогают выявить уязвимости программного обеспечения?

1. Статическое тестирование кода
2. Динамическое тестирование
3. Тестирование пользовательского интерфейса
4. Пенетрационное тестирование

№ 3 Прочитайте текст, выберите правильные ответы и запишите аргументы, обосновывающие выбор ответов

Что является важными аспектами безопасной разработки ПО?

1. Использование шифрования данных
2. Реализация контроля доступа
3. Использование устаревших технологий
4. Регулярные обновления программного обеспечения

№ 4 Прочитайте текст и установите последовательность

Расшифруйте аббревиатуру CIA, запишите цифры в правильном порядке

1. конфиденциальность,
2. целостность,
3. доступность

№ 5 Прочитайте текст и установите последовательность

Перечислите все уровни TCP/IP (DOD) модели, запишите номера правильных ответов в порядке возрастания

- 1. Прикладной,**
2. Физический,
3. Изменчивый,
- 4. Транспортный,**
- 5. Межсетевой,**
6. Апелляционный
- 7. Канальный**

№ 6 Прочитайте текст, выберите правильный ответ и запишите аргументы, обосновывающие выбор

ответа

Что такое безопасность?

1. Положение, при котором не угрожает опасность кому-нибудь или чему-нибудь
2. Положение, при котором есть угроза опасности кому-нибудь или чему-нибудь
3. Положение, при котором не угрожает опасность кому-нибудь
4. Положение, при котором не угрожает опасность чему-нибудь
5. Положение, при котором есть угроза опасности кому-нибудь

№ 7 Прочитайте текст, выберите правильный ответ и запишите аргументы, обосновывающие выбор ответа

Что является одним из важнейших критериев качества (надежности) разрабатываемого программного обеспечения

1. Безопасность
2. Доступность
3. Конфиденциальность
4. Отсутствие целостности
5. Кроссплатформенность

№ 8 Прочитайте текст, выберите правильный ответ и запишите аргументы, обосновывающие выбор ответа

Три основные категории угроз, определенные Майклом Шрёдером?

1. не авторизованное раскрытие информации, не авторизованное изменение информации, не авторизованный отказ в доступе
2. авторизованное раскрытие информации, не авторизованное изменение информации, авторизованный отказ в доступе
3. не авторизованное раскрытие информации, авторизованное изменение информации, не авторизованный отказ в доступе
4. авторизованное раскрытие информации, авторизованное изменение информации, авторизованный отказ в доступе
5. не авторизованное раскрытие информации, авторизованное изменение информации, авторизованный отказ в доступе

№ 9 Прочитайте текст, выберите правильные ответы и запишите аргументы, обосновывающие выбор ответов

три основные категории угроз, определенные Майклом Шрёдером

1. неавторизованное раскрытие информации
2. неавторизованное изменение информации
3. неавторизованный отказ в доступе
4. авторизованное изменение

№ 10 Прочитайте текст и запишите развернутый обоснованный ответ  
Что означает Stateful?

№ 11 Прочитайте текст и запишите развернутый обоснованный ответ  
Что такое SQL-инъекция?

№ 12 Прочитайте текст и установите соответствие  
Расшифруйте аббревиатуру CIA:

1. C
  2. I
  3. A
- А. конфиденциальность,  
Б. целостность,

В. доступность