

**МИНОБРНАУКИ РОССИИ**

**Федеральное государственное бюджетное образовательное  
учреждение высшего образования "Пермский  
государственный национальный исследовательский  
университет"**

**Кафедра информационной безопасности и систем связи**

**Авторы-составители: Кривилёва Анастасия Сергеевна  
Никитина Елена Юрьевна  
Ромашкина Татьяна Витальевна  
Мустакимова Яна Романовна**

Рабочая программа дисциплины

**ПРОЕКТИРОВАНИЕ И РАЗРАБОТКА ПРИЛОЖЕНИЙ В ЗАЩИЩЕННОМ  
ИСПОЛНЕНИИ**

Код УМК 69469

Утверждено  
Протокол №6  
от «26» июня 2020 г.

Пермь, 2020

## **1. Наименование дисциплины**

Проектирование и разработка приложений в защищенном исполнении

## **2. Место дисциплины в структуре образовательной программы**

Дисциплина входит в вариативную часть Блока « С.1 » образовательной программы по направлениям подготовки (специальностям):

Специальность: **10.05.01** Компьютерная безопасность  
специализация Разработка защищенного программного обеспечения

### 3. Планируемые результаты обучения по дисциплине

В результате освоения дисциплины **Проектирование и разработка приложений в защищенном исполнении** у обучающегося должны быть сформированы следующие компетенции:

**10.05.01** Компьютерная безопасность (специализация : Разработка защищенного программного обеспечения)

**ПК.10** Способность участвовать в разработке системы защиты информации предприятия и подсистемы информационной безопасности компьютерной системы, разрабатывать формальные модели политик безопасности, политик управления доступом и информационными потоками в компьютерных системах

**ПК.11** способность оценивать степень надежности выбранных механизмов обеспечения безопасности для решения поставленной задачи

**ПК.13** способность к проведению экспериментального исследования компьютерных систем с целью выявления уязвимостей

**ПК.14** способность обосновывать правильность выбранной модели решения профессиональной задачи, сопоставлять экспериментальные данные и теоретические решения

**ПК.15** Способность оценивать эффективность системы защиты информации в компьютерных системах

**ПК.16** способность организовывать работу малых коллективов исполнителей, находить и принимать управленческие решения в сфере профессиональной деятельности

**ПК.23** Способность организовать защиту информации техническими и программными средствами, включая приемы антивирусной защиты при работе с компьютерными системами

**ПК.5** Способность осуществлять аналитические обзоры по вопросам обеспечения информационной безопасности компьютерных систем, передавать результат проведенных исследований в виде конкретных рекомендаций

**ПК.7** Способность провести обоснование и выбор рационального решения по уровню обеспечения информационной безопасности компьютерных систем с учетом заданных требований

**ПК.9** Способность проводить анализ проектных решений по обеспечению информационной безопасности компьютерных систем

**ПСК.1** способность использовать современные методики и технологии программирования для разработки защищенного программного обеспечения

**ПСК.3** способность руководствоваться требованиями современных стандартов по безопасности компьютерных систем

**ПСК.4** способность проводить разработку программного обеспечения в соответствии с существующими технологиями промышленной разработки программных продуктов

**ПСК.6** Способность применять языки, системы и инструментальные средства программирования, работать с программными средствами прикладного, системного и специального назначения в профессиональной деятельности

#### 4. Объем и содержание дисциплины

<b>Направления подготовки</b>	10.05.01 Компьютерная безопасность (направленность: Разработка защищенного программного обеспечения)
<b>форма обучения</b>	очная
<b>№№ триместров, выделенных для изучения дисциплины</b>	14,15
<b>Объем дисциплины (з.е.)</b>	8
<b>Объем дисциплины (ак.час.)</b>	288
<b>Контактная работа с преподавателем (ак.час.), в том числе:</b>	112
<b>Проведение лекционных занятий</b>	56
<b>Проведение лабораторных работ, занятий по иностранному языку</b>	56
<b>Самостоятельная работа (ак.час.)</b>	176
<b>Формы текущего контроля</b>	Защищаемое контрольное мероприятие (1) Итоговое контрольное мероприятие (1) Письменное контрольное мероприятие (6)
<b>Формы промежуточной аттестации</b>	Зачет (14 триместр) Экзамен (15 триместр)

## **5. Аннотированное описание содержания разделов и тем дисциплины**

### **Проектирование и разработка приложений в защищенном исполнении. Первый семестр**

История развития российской и международных стандартов в области безопасности информационных технологий

Характеристики современных стандартов

Тенденции в развитии российских и международных стандартов

### **Российские и международные стандарты в области безопасности информационных технологий**

История развития и примеры стандартов в области безопасности ИТ

### **История развития российской и международных стандартов в области безопасности информационных технологий**

История развития стандартов в области безопасности

### **Характеристики современных стандартов**

Примеры современных стандартов

### **Тенденции в развитии российских и международных стандартов**

Тенденции в развитии российских и международных стандартов

### **ГОСТ-Р ИСО/МЭК 15408 «Критерии безопасности информационных технологий» (РД ОК)**

Блок про аналог Common Criteria в РФ

### **Цели и задачи РД ОК, Структура РД ОК**

Цели, задачи и структура РД ОК 2002г.

### **Функциональные требования безопасности, Требования доверия, Оценочные уровни доверия**

Какие требования содержит РД ОК: классификация и структура

### **Профили защиты: структура и методика их формирования**

Блок про написание профилей защиты

### **Назначение и структура ПЗ**

Зачем нужны профили защиты.

### **Методика формирования ПЗ**

Правила написания профиля защиты

### **Задания по безопасности: структура и методика их формирования**

Блок про написание заданий по безопасности

### **Назначение и структура ЗБ**

Чем задание по безопасности отличается от профиля защиты

### **Методика формирования ЗБ**

Правила написания заданий по безопасности

### **Разработка информационной системы в защищенном исполнении**

Блок про ПРПЗИ

### **Жизненный цикл информационной системы**

Жизненный цикл приложения

### **Принципы организации проектирования и разработки ИС в защищенном исполнении**

Способы и принципы проектирования и разработки приложений

#### **Формирование проектной документации**

Написание профиля защиты и задания по безопасности

#### **Разработка ИС в защищенном исполнении**

Выполнение задания по ПРПЗИ

#### **Проектирование и разработка приложений в защищенном исполнении. Второй семестр**

Рассматривается: качество программного обеспечения, основные методы и средства реализации отдельных функциональных требований. Осуществляется разработка приложений в защищенном исполнении.

#### **Защищенная информационная система**

Рассматривается понятие "Защищенная информационная система".

#### **Качество программного обеспечения**

Рассматривается обеспечение надежности и безопасности ПО, метрики качества ПО.

#### **Обеспечение надежности и безопасности ПО**

Рассматривается тема обеспечения надежности и безопасности ПО

#### **Метрики качества ПО**

Рассматриваются метрики качества ПО

#### **Основные методы и средства реализации отдельных функциональных требований**

Рассматриваются методы обеспечения идентификации и аутентификации, методы аудита безопасности.

#### **Методы обеспечения идентификации и аутентификации**

Рассматриваются методы обеспечения идентификации и аутентификации

#### **Методы аудита безопасности**

Рассматриваются методы аудита

#### **Методы и технологии обеспечения безопасности программного обеспечения**

Рассматриваются методы и технологии обеспечения безопасности ПО, показатели функциональной надежности, показатели функциональной безопасности

#### **Показатели функциональной надежности**

Рассматриваются показатели функциональной надежности

#### **Показатели функциональной безопасности**

Рассматриваются показатели функциональной безопасности

#### **Разработка приложений в защищенном исполнении**

Рассматриваются принципы организации разработки приложений в защищенном исполнении

#### **Принципы организации разработки приложений в защищенном исполнении**

Рассматриваются принципы организации разработки приложений в защищенном исполнении

### **Формирование документации**

Рассматривается формирование документации для разработанных приложений в защищенном исполнении

### **Разработка приложений в защищенном исполнении**

Осуществляется разработка приложений в защищенном исполнении

### **Итоговое контрольное мероприятие**

Проводится защита разработанных приложений в защищенном исполнении.

## **6. Методические указания для обучающихся по освоению дисциплины**

Освоение дисциплины требует систематического изучения всех тем в той последовательности, в какой они указаны в рабочей программе.

Основными видами учебной работы являются аудиторские занятия. Их цель - расширить базовые знания обучающихся по осваиваемой дисциплине и систему теоретических ориентиров для последующего более глубокого освоения программного материала в ходе самостоятельной работы. Обучающемуся важно помнить, что контактная работа с преподавателем эффективно помогает ему овладеть программным материалом благодаря расстановке необходимых акцентов и удержанию внимания интонационными модуляциями голоса, а также подключением аудио-визуального механизма восприятия информации.

Самостоятельная работа преследует следующие цели:

- закрепление и совершенствование теоретических знаний, полученных на лекционных занятиях;
- формирование навыков подготовки текстовой составляющей информации учебного и научного назначения для размещения в различных информационных системах;
- совершенствование навыков поиска научных публикаций и образовательных ресурсов, размещенных в сети Интернет;
- самоконтроль освоения программного материала.

Обучающемуся необходимо помнить, что результаты самостоятельной работы контролируются преподавателем во время проведения мероприятий текущего контроля и учитываются при промежуточной аттестации.

Обучающимся с ОВЗ и инвалидов предоставляется возможность выбора форм проведения мероприятий текущего контроля, альтернативных формам, предусмотренным рабочей программой дисциплины. Предусматривается возможность увеличения в пределах 1 академического часа времени, отводимого на выполнение контрольных мероприятий.

Процедура оценивания результатов обучения инвалидов и лиц с ограниченными возможностями здоровья по дисциплине предусматривает предоставление информации в формах, адаптированных к ограничениям их здоровья и восприятия информации.

При проведении текущего контроля применяются оценочные средства, обеспечивающие передачу информации, от обучающегося к преподавателю, с учетом психофизиологических особенностей здоровья обучающихся.

## **7. Перечень учебно-методического обеспечения для самостоятельной работы обучающихся по дисциплине**

При самостоятельной работе обучающимся следует использовать:

- конспекты лекций;
- литературу из перечня основной и дополнительной учебной литературы, необходимой для освоения дисциплины (модуля);
- текст лекций на электронных носителях;
- ресурсы информационно-телекоммуникационной сети "Интернет", необходимые для освоения дисциплины;
- лицензионное и свободно распространяемое программное обеспечение из перечня информационных технологий, используемых при осуществлении образовательного процесса по дисциплине;
- методические указания для обучающихся по освоению дисциплины.

## 8. Перечень основной и дополнительной учебной литературы

### Основная:

1. Девянин П. Н. Модели безопасности компьютерных систем: учеб. пособие для студентов вузов, обучающихся по спец. "Компьютер. безопасность"/П. Н. Девянин.-М.: Академия, 2005, ISBN 5-7695-2053-1.-144.-Библиогр.: с. 139-140
2. Голиков, А. М. Основы проектирования защищенных телекоммуникационных систем : учебное пособие для специалитета: 10.05.02 Информационная безопасность телекоммуникационных систем. Курс лекций, компьютерный практикум, компьютерные лабораторные работы и задание на самостоятельную работу / А. М. Голиков. — Томск : Томский государственный университет систем управления и радиоэлектроники, 2016. — 396 с. — ISBN 2227-8397. — Текст : электронный // Электронно-библиотечная система IPR BOOKS : [сайт]. <http://www.iprbookshop.ru/72158.html>
3. Сергеев М. В. Интранет-технологии и информационная безопасность: метод. пособие/М. В. Сергеев.- Пермь, 2007.-212.-Библиогр.: с. 203-206
4. Шумский, Н. Н. Региональные экономические объединения постсоветских государств. Организационно-правовое обеспечение процессов интеграции : монография / Н. Н. Шумский. — Минск : Белорусская наука, 2010. — 323 с. — ISBN 978-985-08-1147-9. — Текст : электронный // Электронно-библиотечная система IPR BOOKS : [сайт]. <http://www.iprbookshop.ru/12315>
5. Лебедева, Т. Н. Технология программирования : учебное пособие / Т. Н. Лебедева, С. С. Юнусова. — 2-е изд. — Челябинск, Саратов : Южно-Уральский институт управления и экономики, Ай Пи Эр Медиа, 2019. — 140 с. — ISBN 978-5-4486-0664-9. — Текст : электронный // Электронно-библиотечная система IPR BOOKS : [сайт]. <http://www.iprbookshop.ru/81500.html>
6. Шумский А. А., Шелупанов А. А. Системный анализ в защите информации: учеб. пособие для студентов вузов, обучающихся по специальностям в области информационной безопасности/А. А. Шумский, А. А. Шелупанов.-М.: Гелиос АРВ, 2005, ISBN 5-85438-128-1.-224.-Библиогр.: с. 218-219

### Дополнительная:

1. Ховард М., Леви М., Вэймир Р. Разработка защищенных Web-приложений на платформе Microsoft Windows 2000: Мастер-класс: Пер. с англ./М. Ховард, М. Леви, Р. Вэймир.-М.; СПб.: Рус. Редакция; Питер, 2001, ISBN 5-318-00439-3.-464.
2. Разработка защищенных Web-приложений на платформе Windows 2000.-М.: Рус. Редакция, cop. 2000.-1.
3. Терехов, А. Н. Технология программирования : учебное пособие / А. Н. Терехов. — 4-е изд. — Москва : Интернет-Университет Информационных Технологий (ИНТУИТ), Ай Пи Ар Медиа, 2020. — 148 с. — ISBN 978-5-4497-0702-4. — Текст : электронный // Электронно-библиотечная система IPR BOOKS : [сайт]. <http://www.iprbookshop.ru/97587.html>



При освоении материала и выполнения заданий по дисциплине рекомендуется использование материалов, размещенных в Личных кабинетах обучающихся ЕТИС ПГНИУ ([student.psu.ru](http://student.psu.ru)).

При организации дистанционной работы и проведении занятий в режиме онлайн могут использоваться:

система видеоконференцсвязи на основе платформы BigBlueButton (<https://bigbluebutton.org/>).

система LMS Moodle (<http://e-learn.psu.ru/>), которая поддерживает возможность использования текстовых материалов и презентаций, аудио- и видеоконтент, а так же тесты, проверяемые задания, задания для совместной работы.

система тестирования Indigo (<https://indigotech.ru/>).

### **11. Описание материально-технической базы, необходимой для осуществления образовательного процесса по дисциплине**

Для лекционных занятий требуется аудитория, оснащенная презентационной техникой (проектором и т.д.); экран для проектора, маркерная или меловая доска, компьютер/ноутбук.

Для лабораторных работ требуется аудитория Лаборатории Информационной безопасности: аппаратные и программные средства определены паспортом лаборатории.

Для самостоятельной работы требуется аудитория помещения Научной библиотеки ПГНИУ, оснащенные компьютерной техникой с возможностью подключения к сети «Интернет», обеспеченные доступом в электронную информационно-образовательную среду университета и с доступом к ЭБС.

Помещения научной библиотеки ПГНИУ для обеспечения самостоятельной работы обучающихся:

1. Научно-библиографический отдел, корп.1, ауд. 142. Оборудован 3 персональными компьютера с доступом к локальной и глобальной компьютерным сетям.

2. Читальный зал гуманитарной литературы, корп. 2, ауд. 418. Оборудован 7 персональными компьютерами с доступом к локальной и глобальной компьютерным сетям.

3. Читальный зал естественной литературы, корп.6, ауд. 107а. Оборудован 5 персональными компьютерами с доступом к локальной и глобальной компьютерным сетям.

4. Отдел иностранной литературы, корп.2 ауд. 207. Оборудован 1 персональным компьютером с доступом к локальной и глобальной компьютерным сетям.

5. Библиотека юридического факультета, корп.9, ауд. 4. Оборудована 11 персональными компьютерами с доступом к локальной и глобальной компьютерным сетям.

6. Читальный зал географического факультета, корп.8, ауд. 419. Оборудован 6 персональными компьютерами с доступом к локальной и глобальной компьютерным сетям.

Все компьютеры, установленные в помещениях научной библиотеки, оснащены следующим программным обеспечением:

Операционная система ALT Linux;

Офисный пакет Libreoffice.

Справочно-правовая система «КонсультантПлюс»

**Фонды оценочных средств для аттестации по дисциплине  
Проектирование и разработка приложений в защищенном исполнении**

**Планируемые результаты обучения по дисциплине для формирования компетенции и  
критерии их оценивания**

Компетенция	Планируемые результаты обучения	Критерии оценивания результатов обучения
<p><b>ПСК.3</b> способность руководствоваться требованиями современных стандартов по безопасности компьютерных систем</p>	<p>Знать требования современных стандартов по безопасности компьютерных систем Уметь использовать требования современных стандартов по безопасности компьютерных систем Владеть навыками использования требований современных стандартов по безопасности компьютерных систем на практике</p>	<p align="center"><b>Неудовлетворител</b> Не обладает знаниями использования требований современных стандартов по безопасности компьютерных систем</p> <p align="center"><b>Удовлетворительн</b> Имеет представление о функциональных требованиях безопасности, требованиях доверия, имеет представление об использовании требований современных стандартов по безопасности компьютерных систем.</p> <p align="center"><b>Хорошо</b> Имеет представление о функциональных требованиях безопасности, требованиях доверия. Обладает знаниями использования требований современных стандартов по безопасности компьютерных систем.</p> <p align="center"><b>Отлично</b> Имеет представление о функциональных требованиях безопасности, требованиях доверия, оценочных уровнях доверия. Использует требования современных стандартов по безопасности компьютерных систем при решении поставленных задач.</p>
<p><b>ПСК.6</b> Способность применять языки, системы и инструментальные средства программирования, работать с программными средствами прикладного, системного и специального назначения в</p>	<p>Знать языки, системы и инструментальные средства программирования. Уметь работать с программными средствами прикладного, системного и специального назначения в профессиональной деятельности.</p>	<p align="center"><b>Неудовлетворител</b> Не имеет представления о методике формирования задания по безопасности</p> <p align="center"><b>Удовлетворительн</b> Имеет представления о методике формирования задания по безопасности; о средствах прикладного, системного и специального назначения при его использовании в процессе решения поставленных задач.</p> <p align="center"><b>Хорошо</b> Имеет представления о методике формирования задания по безопасности; о</p>

Компетенция	Планируемые результаты обучения	Критерии оценивания результатов обучения
профессиональной деятельности		<p style="text-align: center;"><b>Хорошо</b></p> <p>системах и инструментальных средствах программирования; о средствах прикладного, системного и специального назначения при его использования в процессе решения поставленных задач.</p> <p style="text-align: center;"><b>Отлично</b></p> <p>Имеет представления о методике формирования задания по безопасности; о системах и инструментальных средствах программирования; о средствах прикладного, системного и специального назначения при его использования в процессе решения поставленных задач. Знает назначение и структуру задания по безопасности.</p>
<b>ПСК.1</b> способность использовать современные методики и технологии программирования для разработки защищенного программного обеспечения	Знать современные методики и технологии программирования. Уметь разрабатывать защищенное программное обеспечение. Владеть навыками использования современных методик и технологий программирования для разработки защищенного программного обеспечения	<p style="text-align: center;"><b>Неудовлетворител</b></p> <p>Не имеет представления о возможностях использования современных методик и технологий программирования для разработки защищенного программного обеспечения</p> <p style="text-align: center;"><b>Удовлетворительн</b></p> <p>Имеет представления о возможностях использования современных методик и технологий программирования для разработки защищенного программного обеспечения</p> <p style="text-align: center;"><b>Хорошо</b></p> <p>Использует современные методики и технологии программирования для разработки защищенного программного обеспечения</p> <p style="text-align: center;"><b>Отлично</b></p> <p>Имеет представления о возможностях использования современных методик и технологий программирования для разработки защищенного программного обеспечения. Использует современных методики и технологии программирования для разработки защищенного программного обеспечения</p>
<b>ПК.11</b> способность оценивать	Знать механизмы обеспечения безопасности.	<p style="text-align: center;"><b>Неудовлетворител</b></p> <p>Не имеет представления о понятии качества</p>

Компетенция	Планируемые результаты обучения	Критерии оценивания результатов обучения
<p>степень надежности выбранных механизмов обеспечения безопасности для решения поставленной задачи</p>	<p>Уметь выбирать механизмы обеспечения безопасности для решения поставленной задачи. Владеть методами оценки степени надежности выбранных механизмов обеспечения безопасности для решения поставленной задачи</p>	<p><b>Неудовлетворител</b> программного обеспечения</p> <p><b>Удовлетворительн</b> Имеет представления о понятии качества программного обеспечения, обеспечения надежности и безопасности программного обеспечения</p> <p><b>Хорошо</b> Способен оценить надежность, качество программного обеспечения, используя метрики качества программного обеспечения</p> <p><b>Отлично</b> Способен оценить надежность, качество программного обеспечения, используя метрики качества программного обеспечения; использует в своей деятельности возможности обеспечения надежности и безопасности программного обеспечения</p>
<p><b>ПК.7</b> Способность провести обоснование и выбор рационального решения по уровню обеспечения информационной безопасности компьютерных систем с учетом заданных требований</p>	<p>Знать методы и технологии обеспечения информационной безопасности компьютерных систем. Уметь провести обоснование и выбор рационального решения по уровню обеспечения информационной безопасности компьютерных систем с учетом заданных требований. Владеть навыками выбора рационального решения по уровню обеспечения информационной безопасности компьютерных систем с учетом заданных требований.</p>	<p><b>Неудовлетворител</b> Не имеет представления о методах и технологиях обеспечения безопасности программного обеспечения</p> <p><b>Удовлетворительн</b> Имеет представления о методах и технологиях обеспечения безопасности программного обеспечения</p> <p><b>Хорошо</b> Знает методы и технологии обеспечения безопасности программного обеспечения. Знает показатели функциональной надежности и безопасности программного обеспечения.</p> <p><b>Отлично</b> Использует методы и технологии обеспечения безопасности программного обеспечения при разработке приложения в защищенном исполнении.</p>
<p><b>ПК.16</b> способность организовывать работу малых коллективов исполнителей, находить и принимать</p>	<p>Знать принципы организации разработки приложений в защищенном исполнении. Уметь организовывать работу малых коллективов исполнителей.</p>	<p><b>Неудовлетворител</b> Не имеет представления о принципах организации разработки приложений в защищенном исполнении</p> <p><b>Удовлетворительн</b> Имеет представления о принципах</p>

Компетенция	Планируемые результаты обучения	Критерии оценивания результатов обучения
<p>управленческие решения в сфере профессиональной деятельности</p>	<p>Владеть навыками обоснования управленческих решений в сфере профессиональной деятельности</p>	<p><b>Удовлетворительн</b> организации разработки приложений в защищенном исполнении, формировании документации для разрабатываемого приложения</p> <p><b>Хорошо</b> Имеет представление об организации работы в малых группах исполнителей. Имеет представления о принципах организации разработки приложений в защищенном исполнении, формировании документации для разрабатываемого приложения</p> <p><b>Отлично</b> Может организовывать работу малых коллективов исполнителей, находить и принимать управленческие решения при разработке приложений в защищенном исполнении</p>
<p><b>ПК.10</b> Способность участвовать в разработке системы защиты информации предприятия и подсистемы информационной безопасности компьютерной системы, разрабатывать формальные модели политик безопасности, политик управления доступом и информационными потоками в компьютерных системах</p>	<p>Знать составляющие системы защиты информации предприятия и подсистемы информационной безопасности компьютерной системы, формальные модели политик безопасности, политик управления доступом и информационными потоками. Уметь принимать участие в разработке системы защиты информации предприятия и подсистемы информационной безопасности компьютерной системы, разрабатывать формальные модели политик безопасности, политик управления доступом и информационными потоками в компьютерных системах</p>	<p><b>Неудовлетворител</b> Не способен участвовать в разработке системы защиты информации предприятия и подсистемы информационной безопасности компьютерной системы, разрабатывать формальные модели политик безопасности, политик управления доступом и информационными потоками в компьютерных системах</p> <p><b>Удовлетворительн</b> Способен со значительными затруднениями участвовать в разработке системы защиты информации предприятия и подсистемы информационной безопасности компьютерной системы, разрабатывать формальные модели политик безопасности, политик управления доступом и информационными потоками в компьютерных системах</p> <p><b>Хорошо</b> Способен с незначительными затруднениями участвовать в разработке системы защиты информации предприятия и подсистемы информационной безопасности компьютерной системы, разрабатывать формальные модели политик безопасности, политик управления доступом и</p>

Компетенция	Планируемые результаты обучения	Критерии оценивания результатов обучения
		<p style="text-align: center;"><b>Хорошо</b></p> <p>информационными потоками в компьютерных системах</p> <p style="text-align: center;"><b>Отлично</b></p> <p>Способен участвовать в разработке системы защиты информации предприятия и подсистемы информационной безопасности компьютерной системы, разрабатывать формальные модели политик безопасности, политик управления доступом и информационными потоками в компьютерных системах</p>
<p><b>ПК.13</b> способность к проведению экспериментального исследования компьютерных систем с целью выявления уязвимостей</p>	<p>Знать потенциальные уязвимости компьютерных систем. Уметь проводить экспериментальные исследования компьютерных систем. Владеть навыками проведения экспериментального исследования компьютерных систем с целью выявления уязвимостей</p>	<p style="text-align: center;"><b>Неудовлетворител</b></p> <p>Не имеет представления о методах проведения экспериментального исследования компьютерных систем с целью выявления уязвимостей</p> <p style="text-align: center;"><b>Удовлетворительн</b></p> <p>Имеет представление о методах проведения экспериментального исследования компьютерных систем с целью выявления уязвимостей</p> <p style="text-align: center;"><b>Хорошо</b></p> <p>Знает методы проведения экспериментального исследования компьютерных систем с целью выявления уязвимостей</p> <p style="text-align: center;"><b>Отлично</b></p> <p>Использует методы проведения экспериментального исследования компьютерных систем с целью выявления уязвимостей</p>
<p><b>ПК.14</b> способность обосновывать правильность выбранной модели решения профессиональной задачи, сопоставлять экспериментальные данные и теоретические решения</p>	<p>Знать базовые модели решения профессиональной задачи. Уметь обосновывать правильность выбранной модели решения профессиональной задачи. Владеть навыками обработки результатов проведенного эксперимента</p>	<p style="text-align: center;"><b>Неудовлетворител</b></p> <p>Не способен обосновывать правильность выбранной модели решения профессиональной задачи, сопоставлять экспериментальные данные и теоретические решения</p> <p style="text-align: center;"><b>Удовлетворительн</b></p> <p>Способен со значительными затруднениями обосновывать правильность выбранной модели решения профессиональной задачи. Не способен сопоставлять экспериментальные данные и теоретические решения</p>

Компетенция	Планируемые результаты обучения	Критерии оценивания результатов обучения
		<p style="text-align: center;"><b>Хорошо</b></p> <p>Способен с затруднениями обосновывать правильность выбранной модели решения профессиональной задачи. Способен с затруднениями сопоставлять экспериментальные данные и теоретические решения</p> <p style="text-align: center;"><b>Отлично</b></p> <p>Способен в полной мере обосновывать правильность выбранной модели решения профессиональной задачи, сопоставлять экспериментальные данные и теоретические решения</p>
<p><b>ПК.15</b> Способность оценивать эффективность системы защиты информации в компьютерных системах</p>	<p>Знать компоненты системы защиты информации. Уметь оценивать эффективность системы защиты информации в компьютерных системах. Владеть методами оценки эффективности системы защиты информации в компьютерных системах.</p>	<p style="text-align: center;"><b>Неудовлетворител</b></p> <p>Не способен оценивать эффективность системы защиты информации в компьютерных системах</p> <p style="text-align: center;"><b>Удовлетворительн</b></p> <p>Имеет представление о методах оценки эффективности системы защиты информации в компьютерных системах</p> <p style="text-align: center;"><b>Хорошо</b></p> <p>Знает методы оценки эффективности системы защиты информации в компьютерных системах</p> <p style="text-align: center;"><b>Отлично</b></p> <p>Способен применять методы оценки эффективности системы защиты информации в компьютерных системах</p>
<p><b>ПК.5</b> Способность осуществлять аналитические обзоры по вопросам обеспечения информационной безопасности компьютерных систем, передавать результат проведенных исследований в виде конкретных рекомендаций</p>	<p>Знать существующие источники информации для аналитических обзоров по вопросам обеспечения информационной безопасности компьютерных систем Уметь осуществлять аналитические обзоры по вопросам обеспечения информационной безопасности компьютерных систем, передавать результат проведенных исследований в виде конкретных рекомендаций Владеть навыками обработки полученной информации.</p>	<p style="text-align: center;"><b>Неудовлетворител</b></p> <p>Не способен осуществлять аналитические обзоры по вопросам обеспечения информационной безопасности компьютерных систем, передавать результат проведенных исследований в виде конкретных рекомендаций</p> <p style="text-align: center;"><b>Удовлетворительн</b></p> <p>Способен с затруднениями осуществлять аналитические обзоры по вопросам обеспечения информационной безопасности компьютерных систем. Не способен передавать результат проведенных исследований в виде конкретных рекомендаций</p> <p style="text-align: center;"><b>Хорошо</b></p>

Компетенция	Планируемые результаты обучения	Критерии оценивания результатов обучения
		<p style="text-align: center;"><b>Хорошо</b></p> <p>Способен осуществлять аналитические обзоры по вопросам обеспечения информационной безопасности компьютерных систем. Не способен передавать результат проведенных исследований в виде конкретных рекомендаций</p> <p style="text-align: center;"><b>Отлично</b></p> <p>Способен осуществлять аналитические обзоры по вопросам обеспечения информационной безопасности компьютерных систем. Способен передавать результат проведенных исследований в виде конкретных рекомендаций</p>
<p><b>ПК.23</b> Способность организовать защиту информации техническими и программными средствами, включая приемы антивирусной защиты при работе с компьютерными системами</p>	<p>Знать технические и программные средства защиты данных. Уметь организовать защиту информации техническими и программными средствами. Владеть приемами антивирусной защиты при работе с компьютерными системами</p>	<p style="text-align: center;"><b>Неудовлетворител</b></p> <p>Не способен организовать защиту информации техническими и программными средствами, включая приемы антивирусной защиты при работе с компьютерными системами</p> <p style="text-align: center;"><b>Удовлетворительн</b></p> <p>Способен со значительными затруднениями организовать защиту информации техническими и программными средствами, включая приемы антивирусной защиты при работе с компьютерными системами</p> <p style="text-align: center;"><b>Хорошо</b></p> <p>Способен с незначительными затруднениями организовать защиту информации техническими и программными средствами, включая приемы антивирусной защиты при работе с компьютерными системами</p> <p style="text-align: center;"><b>Отлично</b></p> <p>Способен без затруднений организовать защиту информации техническими и программными средствами, включая приемы антивирусной защиты при работе с компьютерными системами</p>
<p><b>ПК.9</b> Способность проводить анализ проектных решений по обеспечению информационной</p>	<p>Знать основы информационной безопасности компьютерных систем Уметь проводить анализ проектных решений по обеспечению информационной безопасности компьютерных</p>	<p style="text-align: center;"><b>Неудовлетворител</b></p> <p>Не способен проводить анализ проектных решений по обеспечению информационной безопасности компьютерных систем</p> <p style="text-align: center;"><b>Удовлетворительн</b></p> <p>Имеет представление о методах для анализа</p>

Компетенция	Планируемые результаты обучения	Критерии оценивания результатов обучения
безопасности компьютерных систем	систем. Владеть методами анализа проектных решений по обеспечению информационной безопасности компьютерных систем.	<p align="center"><b>Удовлетворительн</b></p> <p>проектных решений по обеспечению информационной безопасности компьютерных систем</p> <p align="center"><b>Хорошо</b></p> <p>Знает методы для анализа проектных решений по обеспечению информационной безопасности компьютерных систем</p> <p align="center"><b>Отлично</b></p> <p>Способен применять методы для анализа проектных решений по обеспечению информационной безопасности компьютерных систем</p>
<p><b>ПСК.4</b>  способность проводить разработку программного обеспечения в соответствии с существующими технологиями промышленной разработки программных продуктов</p>	<p>Знать существующие технологии промышленной разработки программных продуктов.  Уметь проводить разработку программного обеспечения в соответствии с существующими технологиями промышленной разработки программных продуктов</p>	<p align="center"><b>Неудовлетворител</b></p> <p>Не имеет представления о возможностях использования современных методик и технологий программирования для разработки защищенного программного обеспечения</p> <p align="center"><b>Удовлетворительн</b></p> <p>Имеет представления о возможностях использования современных методик и технологий программирования для разработки защищенного программного обеспечения</p> <p align="center"><b>Хорошо</b></p> <p>Использует современные методики и технологии программирования для разработки защищенного программного обеспечения</p> <p align="center"><b>Отлично</b></p> <p>Имеет представления о возможностях использования современных методик и технологий программирования для разработки защищенного программного обеспечения.  Использует современных методики и технологии программирования для разработки защищенного программного обеспечения</p>

## Оценочные средства текущего контроля и промежуточной аттестации

Схема доставки : СУОС КМБ

**Вид мероприятия промежуточной аттестации :** Зачет

**Способ проведения мероприятия промежуточной аттестации :** Оценка по дисциплине в рамках промежуточной аттестации определяется на основе баллов, набранных обучающимся на контрольных мероприятиях, проводимых в течение учебного периода.

**Максимальное количество баллов :** 100

### Конвертация баллов в отметки

«отлично» - от 81 до 100

«хорошо» - от 61 до 80

«удовлетворительно» - от 50 до 60

«неудовлетворительно» / «незачтено» менее 50 балла

<b>Компетенция</b>	<b>Мероприятие текущего контроля</b>	<b>Контролируемые элементы результатов обучения</b>
<b>ПСК.3</b> способность руководствоваться требованиями современных стандартов по безопасности компьютерных систем	Функциональные требования безопасности, Требования доверия, Оценочные уровни доверия <b>Защищаемое контрольное мероприятие</b>	Функциональные требования безопасности, Требования доверия, Оценочные уровни доверия

Компетенция	Мероприятие текущего контроля	Контролируемые элементы результатов обучения
<p><b>ПСК.3</b> способность руководствоваться требованиями современных стандартов по безопасности компьютерных систем</p> <p><b>ПК.9</b> Способность проводить анализ проектных решений по обеспечению информационной безопасности компьютерных систем</p> <p><b>ПК.10</b> Способность участвовать в разработке системы защиты информации предприятия и подсистемы информационной безопасности компьютерной системы, разрабатывать формальные модели политик безопасности, политик управления доступом и информационными потоками в компьютерных системах</p>	<p>Методика формирования ПЗ</p> <p><b>Письменное контрольное мероприятие</b></p>	<p>Формирование Профиля Защиты</p>
<p><b>ПК.5</b> Способность осуществлять аналитические обзоры по вопросам обеспечения информационной безопасности компьютерных систем, передавать результат проведенных исследований в виде конкретных рекомендаций</p> <p><b>ПСК.6</b> Способность применять языки, системы и инструментальные средства программирования, работать с программными средствами прикладного, системного и специального назначения в профессиональной деятельности</p>	<p>Методика формирования ЗБ</p> <p><b>Письменное контрольное мероприятие</b></p>	<p>Формирование Задания по Безопасности</p>

<b>Компетенция</b>	<b>Мероприятие текущего контроля</b>	<b>Контролируемые элементы результатов обучения</b>
<b>ПСК.1</b> способность использовать современные методики и технологии программирования для разработки защищенного программного обеспечения <b>ПК.23</b> Способность организовать защиту информации техническими и программными средствами, включая приемы антивирусной защиты при работе с компьютерными системами	Разработка ИС в защищенном исполнении <b>Письменное контрольное мероприятие</b>	Разработанная документация на спроектированную информационную систему

### **Спецификация мероприятий текущего контроля**

#### **Функциональные требования безопасности, Требования доверия, Оценочные уровни доверия**

Продолжительность проведения мероприятия промежуточной аттестации: **1 часа**

Условия проведения мероприятия: **в часы аудиторной работы**

Максимальный балл, выставляемый за мероприятие промежуточной аттестации: **20**

Проходной балл: **10**

<b>Показатели оценивания</b>	<b>Баллы</b>
Знание классов функциональных требований безопасности	10
Знание оценочных уровней доверия	5
Знание классов требований доверия	5

#### **Методика формирования ПЗ**

Продолжительность проведения мероприятия промежуточной аттестации: **1 часа**

Условия проведения мероприятия: **в часы аудиторной работы**

Максимальный балл, выставляемый за мероприятие промежуточной аттестации: **20**

Проходной балл: **10**

<b>Показатели оценивания</b>	<b>Баллы</b>
Способность сформировать ПЗ для предоставленного объекта оценки	15
Знание методики формирования ПЗ	5

#### **Методика формирования ЗБ**

Продолжительность проведения мероприятия промежуточной аттестации: **1 часа**

Условия проведения мероприятия: **в часы аудиторной работы**

Максимальный балл, выставляемый за мероприятие промежуточной аттестации: **30**

Проходной балл: **15**

Показатели оценивания	Баллы
Способность сформировать ЗБ для предоставленного объекта оценки	20
Знание методики формирования ЗБ	10

### Разработка ИС в защищенном исполнении

Продолжительность проведения мероприятия промежуточной аттестации: **1 часа**

Условия проведения мероприятия: **в часы самостоятельной работы**

Максимальный балл, выставляемый за мероприятие промежуточной аттестации: **30**

Проходной балл: **15**

Показатели оценивания	Баллы
Способность спроектировать и разработать ИС в защищенном исполнении	15
Способность разработать проектную документацию	8
Знание принципов организации проектирования и разработки ИС в защищенном исполнении	7

**Вид мероприятия промежуточной аттестации :** Экзамен

**Способ проведения мероприятия промежуточной аттестации :** Оценка по дисциплине в рамках промежуточной аттестации определяется на основе баллов, набранных обучающимся на контрольных мероприятиях, проводимых в течение учебного периода.

**Максимальное количество баллов :** 100

### Конвертация баллов в отметки

«отлично» - от 81 до 100

«хорошо» - от 61 до 80

«удовлетворительно» - от 50 до 60

«неудовлетворительно» / «незачтено» менее 50 балла

Компетенция	Мероприятие текущего контроля	Контролируемые элементы результатов обучения
<p><b>ПК.11</b> способность оценивать степень надежности выбранных механизмов обеспечения безопасности для решения поставленной задачи</p> <p><b>ПК.15</b> Способность оценивать эффективность системы защиты информации в компьютерных системах</p>	<p>Метрики качества ПО</p> <p><b>Письменное контрольное мероприятие</b></p>	<p>Метрики качества программного обеспечения</p>

Компетенция	Мероприятие текущего контроля	Контролируемые элементы результатов обучения
<p><b>ПК.7</b> Способность провести обоснование и выбор рационального решения по уровню обеспечения информационной безопасности компьютерных систем с учетом заданных требований</p> <p><b>ПК.13</b> способность к проведению экспериментального исследования компьютерных систем с целью выявления уязвимостей</p>	<p>Показатели функциональной безопасности</p> <p><b>Письменное контрольное мероприятие</b></p>	<p>Показатели функциональной безопасности и надежности программного обеспечения</p>
<p><b>ПСК.4</b> способность проводить разработку программного обеспечения в соответствии с существующими технологиями промышленной разработки программных продуктов</p> <p><b>ПК.14</b> способность обосновывать правильность выбранной модели решения профессиональной задачи, сопоставлять экспериментальные данные и теоретические решения</p> <p><b>ПК.16</b> способность организовывать работу малых коллективов исполнителей, находить и принимать управленческие решения в сфере профессиональной деятельности</p>	<p>Разработка приложений в защищенном исполнении</p> <p><b>Письменное контрольное мероприятие</b></p>	<p>Принципах организации разработки приложений в защищенном исполнении, формировании документации для разрабатываемого приложения. Организация работы в малых группах исполнителей.</p>
<p><b>ПК.16</b> способность организовывать работу малых коллективов исполнителей, находить и принимать управленческие решения в сфере профессиональной деятельности</p>	<p>Итоговое контрольное мероприятие</p> <p><b>Итоговое контрольное мероприятие</b></p>	<p>Принципах организации разработки приложений в защищенном исполнении, формировании документации для разрабатываемого приложения.</p>

### Спецификация мероприятий текущего контроля

## Метрики качества ПО

Продолжительность проведения мероприятия промежуточной аттестации: **1 часа**

Условия проведения мероприятия: **в часы самостоятельной работы**

Максимальный балл, выставляемый за мероприятие промежуточной аттестации: **20**

Проходной балл: **10**

Показатели оценивания	Баллы
Знание метрик качества ПО	10
Знание методов обеспечения надежности и безопасности ПО	10

## Показатели функциональной безопасности

Продолжительность проведения мероприятия промежуточной аттестации: **1 часа**

Условия проведения мероприятия: **в часы аудиторной работы**

Максимальный балл, выставляемый за мероприятие промежуточной аттестации: **20**

Проходной балл: **10**

Показатели оценивания	Баллы
Знание показателей функциональной безопасности	10
Знание показателей функциональной надежности	10

## Разработка приложений в защищенном исполнении

Продолжительность проведения мероприятия промежуточной аттестации: **1 часа**

Условия проведения мероприятия: **в часы самостоятельной работы**

Максимальный балл, выставляемый за мероприятие промежуточной аттестации: **20**

Проходной балл: **10**

Показатели оценивания	Баллы
Способность разработать приложение в защищенном исполнении	15
Знание принципов организации разработки приложения в защищенном исполнении	5

## Итоговое контрольное мероприятие

Продолжительность проведения мероприятия промежуточной аттестации: **1 часа**

Условия проведения мероприятия: **в часы самостоятельной работы**

Максимальный балл, выставляемый за мероприятие промежуточной аттестации: **40**

Проходной балл: **20**

Показатели оценивания	Баллы
Знание целей и задач РД ОК, структуры РД ОК	10
Знание назначения и структуры ПЗ	10
Знание назначения и структуры ЗБ	10
Знание функциональных требований и требований доверия	10