

МИНОБРНАУКИ РОССИИ

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

Институт компьютерных наук и технологий

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

Рабочая программа дисциплины

**ПРОЕКТИРОВАНИЕ И РАЗРАБОТКА ПРИЛОЖЕНИЙ В ЗАЩИЩЕННОМ
ИСПОЛНЕНИИ**

Код УМК 92449

Утверждено
Протокол №6
от «06» мая 2022 г.

Пермь, 2022

1. Наименование дисциплины

Проектирование и разработка приложений в защищенном исполнении

2. Место дисциплины в структуре образовательной программы

Дисциплина входит в обязательную 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)

ОПК.13 Способен разрабатывать компоненты программных и программно-аппаратных средств защиты информации в компьютерных системах и проводить анализ их безопасности

Индикаторы

ОПК.13.1 Применяет теоретические знания информационной безопасности и программирования для разработки компонент программно-аппаратных средств защиты информации

ОПК.13.2 Проводит анализ безопасности компьютерных систем при применении разработанных компонент программно-аппаратных средств защиты информации

ПК.2 Способен принимать участие в проектировании программных (программно-технических) средств защиты информации

Индикаторы

ПК.2.1 Ориентируется в методах проектирования программных (программно-технических) средств защиты информации

ПК.2.2 Применяет на практике методы проектирования программных (программно-технических) средств защиты информации

ПК.3 Способен принимать участие в разработке программных (программно-технических) средств защиты информации

Индикаторы

ПК.3.1 Ориентируется в методах разработки программных (программно-технических) средств защиты информации

ПК.3.2 Применяет на практике методы разработки программных (программно-технических) средств защиты информации

ОПСК.2 Способен использовать современные технологии программирования для разработки защищенного программного обеспечения

Индикаторы

ОПСК.2.1 Применяет на практике современные среды разработки программного обеспечения

ОПСК.2.2 Анализирует средства сред разработки программного обеспечения с целью выбора оптимального варианта для разработки защищенного программного обеспечения

ОПСК.2.3 Разрабатывает программное обеспечение в защищенном исполнении

ОПСК.3 Способен разрабатывать техническую и сопроводительную документацию на защищенное программное обеспечение в соответствии с действующими стандартами и иными нормативными требованиями

Индикаторы

ОПСК.3.1 Подготавливает типовые виды документации на защищенное программное обеспечение

ОПСК.3.2 Оформляет типовые виды документации на защищенное программное обеспечение в соответствии с действующими стандартами и иными нормативными требованиями

4. Объем и содержание дисциплины

Специальность	10.05.01 Компьютерная безопасность (специализация: Разработка защищенного программного обеспечения)
форма обучения	очная
№№ триместров, выделенных для изучения дисциплины	14
Объем дисциплины (з.е.)	4
Объем дисциплины (ак.час.)	144
Контактная работа с преподавателем (ак.час.), в том числе:	56
Проведение лекционных занятий	28
Проведение лабораторных работ, занятий по иностранному языку	28
Самостоятельная работа (ак.час.)	88
Формы текущего контроля	Итоговое контрольное мероприятие (1) Письменное контрольное мероприятие (3)
Формы промежуточной аттестации	Экзамен (14 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

Рассматривается история развития стандартов в области безопасности

Характеристики современных стандартов.

Рассматриваются характеристики современных стандартов

Тенденции в развитии российских и международных стандартов

Рассматриваются тенденции в развитии российских и международных стандартов

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

Рассматриваются цели и задачи РД ОК, Структура РД ОК, функциональные требования безопасности, Требования доверия, Оценочные уровни доверия

Цели и задачи РД ОК, Структура РД ОК

Рассматриваются цели и задачи РД ОК, Структура РД ОК

Функциональные требования безопасности, Требования доверия, Оценочные уровни доверия

Рассматриваются функциональные требования безопасности, Требования доверия, Оценочные уровни доверия

Профили защиты: структура и методика их формирования

Рассматриваются профили защиты: структура и методика их формирования

Назначение и структура ПЗ

Рассматривается назначение и структура ПЗ

Методика формирования ПЗ

Рассматривается методика формирования ПЗ

Задания по безопасности: структура и методика их формирования

Рассматриваются задания по безопасности: структура и методика их формирования

Назначение и структура ЗБ

Рассматривается назначение и структура ЗБ

Методика формирования ЗБ

Рассматривается методика формирования ЗБ

Разработка информационной системы в защищенном исполнении

Рассматривается разработка информационной системы в защищенном исполнении

Жизненный цикл информационной системы

Рассматривается жизненный цикл информационной системы

Принципы организации проектирования и разработки ИС в защищенном исполнении

Рассматриваются принципы организации проектирования и разработки ИС в защищенном исполнении

Формирование проектной документации

Рассматривается формирование проектной документации

Разработка ИС в защищенном исполнении

Осуществляется разработка приложения 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: учебное пособие для студентов вузов, обучающихся по специальности "Компьютерная безопасность"/П. Н. Девянин.-Москва: Академия, 2005, ISBN 5-7695-2053-1.-144.-Библиогр.: с. 139-140
2. Сергеев М. В. Интранет-технологии и информационная безопасность: методическое пособие/М. В. Сергеев.-Пермь, 2007.-212.-Библиогр.: с. 203-206
3. Шумский А. А., Шелупанов А. А. Системный анализ в защите информации: учебное пособие для студентов вузов, обучающихся по специальностям в области информационной безопасности/А. А. Шумский, А. А. Шелупанов.-Москва: Гелиос АРВ, 2005, ISBN 5-85438-128-1.-224.-Библиогр.: с. 218-219

Дополнительная:

1. Малюк А. А., Пазизин С. В., Погожин Н. С. Введение в защиту информации в автоматизированных системах: Учеб. пособие для студентов, обучающихся по спец. не входящим в группу спец. в области информ. безопасности/А. А. Малюк, С. В. Пазизин, Н. С. Погожин.-М.: Горячая линия-Телеком, 2004, ISBN 5-93517-062-0.-147.-Библиогр.: с. 143-145
2. Харт Джонсон М. Системное программирование в среде Win32: Руководство разработчика приложений для системы Windows 2000: Пер. с англ./Джонсон М. Харт.-М.: Изд. дом "Вильямс", 2001, ISBN 5-8459-0177-4.-464.

9. Перечень ресурсов сети Интернет, необходимых для освоения дисциплины

<http://www.psu.ru/elektronnye-resursy-dlya-psu> Электронные ресурсы для ПГНИУ
<http://www.psu.ru/elektronnye-resursy-dlya-psu> Электронные ресурсы для ПГНИУ
<http://www.psu.ru/elektronnye-resursy-dlya-psu> Электронные ресурсы для ПГНИУ
<http://www.psu.ru/elektronnye-resursy-dlya-psu> Электронные ресурсы для ПГНИУ
<http://www.psu.ru/elektronnye-resursy-dlya-psu> Электронные ресурсы для ПГНИУ
<http://www.psu.ru/elektronnye-resursy-dlya-psu> Электронные ресурсы для ПГНИУ
<http://www.psu.ru/elektronnye-resursy-dlya-psu> Электронные ресурсы для ПГНИУ
<http://www.psu.ru/elektronnye-resursy-dlya-psu> Электронные ресурсы для ПГНИУ
<http://www.psu.ru/elektronnye-resursy-dlya-psu> Электронные ресурсы для ПГНИУ
<http://www.psu.ru/elektronnye-resursy-dlya-psu> Электронные ресурсы для ПГНИУ
<http://www.psu.ru/elektronnye-resursy-dlya-psu> Электронные ресурсы для ПГНИУ
<http://www.psu.ru/elektronnye-resursy-dlya-psu> Электронные ресурсы для ПГНИУ
<http://www.psu.ru/elektronnye-resursy-dlya-psu> Электронные ресурсы для ПГНИУ
<http://www.psu.ru/elektronnye-resursy-dlya-psu> Электронные ресурсы для ПГНИУ
<http://www.psu.ru/elektronnye-resursy-dlya-psu> Электронные ресурсы для ПГНИУ
<http://www.psu.ru/elektronnye-resursy-dlya-psu> Электронные ресурсы для ПГНИУ
<http://www.psu.ru/elektronnye-resursy-dlya-psu> Электронные ресурсы для ПГНИУ
<http://www.psu.ru/elektronnye-resursy-dlya-psu> Электронные ресурсы для ПГНИУ
<http://www.psu.ru/elektronnye-resursy-dlya-psu> Электронные ресурсы для ПГНИУ

10. Перечень информационных технологий, используемых при осуществлении образовательного процесса по дисциплине

Образовательный процесс по дисциплине **Проектирование и разработка приложений в защищенном исполнении** предполагает использование следующего программного обеспечения и информационных справочных систем:

Образовательный процесс по данной дисциплине предполагает использование следующего программного обеспечения и информационных справочных систем:

- доступ в режиме on-line в Электронную библиотечную систему (ЭБС);
- доступ в электронную информационно-образовательную среду университета.

Необходимое лицензионное и (или) свободно распространяемое программное обеспечение:

- приложение позволяющее просматривать и воспроизводить медиаконтент PDF-файлов «Adobe Acrobat Reader DC»;
- офисный пакет приложений «LibreOffice».

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

При освоении материала и выполнения заданий по дисциплине рекомендуется использование материалов, размещенных в Личных кабинетах обучающихся ЕТИС ПГНИУ (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 (проектор, экран, компьютер/ноутбук) с соответствующим программным обеспечением, и маркерной доской.

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

Для проведения текущего контроля - аудитория, оснащенная маркерной доской.

Самостоятельная работа студентов: аудитория, оснащенная компьютерной техникой с возможностью подключения к сети «Интернет», с обеспеченным доступом в электронную информационно-образовательную среду университета, помещения Научной библиотеки ПГНИУ.

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.
Индикаторы и критерии их оценивания**

ОПК.13

Способен разрабатывать компоненты программных и программно-аппаратных средств защиты информации в компьютерных системах и проводить анализ их безопасности

Компетенция (индикатор)	Планируемые результаты обучения	Критерии оценивания результатов обучения
<p>ОПК.13.1 Применяет теоретические знания информационной безопасности и программирования для разработки компонент программно-аппаратных средств защиты информации</p>	<p>Применяет теоретические знания информационной безопасности и программирования для разработки компонент программно-аппаратных средств защиты информации</p>	<p align="center">Неудовлетворител Не способен провести обоснование решения по уровню обеспечения информационной безопасности компьютерных систем с учетом заданных требований</p> <p align="center">Удовлетворительн Имеет представление о функциональных требованиях безопасности, требованиях доверия, имеет представление об использовании требований современных стандартов по безопасности компьютерных систем.</p> <p align="center">Хорошо Имеет представление о функциональных требованиях безопасности, требованиях доверия. Обладает знаниями использования требований современных стандартов по безопасности компьютерных систем.</p> <p align="center">Отлично 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>ОПК.13.2 Проводит анализ безопасности компьютерных систем при применении разработанных компонент программно-аппаратных средств защиты информации</p>	<p>Проводит анализ безопасности компьютерных систем при применении разработанных компонент программно-аппаратных средств защиты информации</p>	<p align="center">Неудовлетворител Не имеет представления о методике формирования профиля защиты.</p> <p align="center">Удовлетворительн Имеет представление о методике формирования профиля защиты.</p> <p align="center">Хорошо Имеет представление о методике формирования профиля защиты. Знает назначение и структуру профиля защиты.</p> <p align="center">Отлично</p>

Компетенция (индикатор)	Планируемые результаты обучения	Критерии оценивания результатов обучения
		<p style="text-align: center;">Отлично</p> <p>Обладает знаниями о современных технологиях программирования для разработки защищенного программного обеспечения. Имеет представление о методике формирования профиля защиты. Знает назначение и структуру профиля защиты.</p>

ОПСК.2

Способен использовать современные технологии программирования для разработки защищенного программного обеспечения

Компетенция (индикатор)	Планируемые результаты обучения	Критерии оценивания результатов обучения
<p>ОПСК.2.1 Применяет на практике современные среды разработки программного обеспечения</p>	<p>Применяет на практике современные среды разработки программного обеспечения</p>	<p style="text-align: center;">Неудовлетворител</p> <p>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 style="text-align: center;">Удовлетворительн</p> <p>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 style="text-align: center;">Хорошо</p> <p>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 информационными потоками в компьютерных системах</p> <p style="text-align: center;">Отлично</p> <p>Способен без затруднений участвовать в</p>

Компетенция (индикатор)	Планируемые результаты обучения	Критерии оценивания результатов обучения
		<p align="center">Отлично</p> <p>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>ОПСК.2.2 Анализирует средства сред разработки программного обеспечения с целью выбора оптимального варианта для разработки защищенного программного обеспечения</p>	<p>Анализирует средства сред разработки программного обеспечения с целью выбора оптимального варианта для разработки защищенного программного обеспечения</p>	<p align="center">Неудовлетворител</p> <p>Не способен проводить анализ программного кода с целью поиска потенциальных уязвимостей и недокументированных возможностей</p> <p align="center">Удовлетворительн</p> <p>Способен со значительными затруднениями проводить анализ программного кода с целью поиска потенциальных уязвимостей и недокументированных возможностей</p> <p align="center">Хорошо</p> <p>Способен с незначительными затруднениями проводить анализ программного кода с целью поиска потенциальных уязвимостей и недокументированных возможностей</p> <p align="center">Отлично</p> <p>Способен без затруднений проводить анализ программного кода с целью поиска потенциальных уязвимостей и недокументированных возможностей</p>

ОПСК.3

Способен разрабатывать техническую и сопроводительную документацию на защищенное программное обеспечение в соответствии с действующими стандартами и иными нормативными требованиями

Компетенция (индикатор)	Планируемые результаты обучения	Критерии оценивания результатов обучения
<p>ОПСК.3.1 Подготавливает типовые виды документации на защищенное программное обеспечение</p>	<p>Подготавливает типовые виды документации на защищенное программное обеспечение</p>	<p align="center">Неудовлетворител</p> <p>Не способен проводить разработку программного обеспечения в соответствии с существующими технологиями промышленной разработки программных продуктов</p> <p align="center">Удовлетворительн</p> <p>Способен со значительными затруднениями проводить разработку программного обеспечения в соответствии с</p>

Компетенция (индикатор)	Планируемые результаты обучения	Критерии оценивания результатов обучения
		<p style="text-align: center;">Удовлетворительн</p> <p>существующими технологиями промышленной разработки программных продуктов</p> <p style="text-align: center;">Хорошо</p> <p>Способен с незначительными затруднениями проводить разработку программного обеспечения в соответствии с существующими технологиями промышленной разработки программных продуктов</p> <p style="text-align: center;">Отлично</p> <p>Способен без затруднений проводить разработку программного обеспечения в соответствии с существующими технологиями промышленной разработки программных продуктов</p>

ПК.2

Способен принимать участие в проектировании программных (программно-технических) средств защиты информации

Компетенция (индикатор)	Планируемые результаты обучения	Критерии оценивания результатов обучения
<p>ПК.2.2 Применяет на практике методы проектирования программных (программно-технических) средств защиты информации</p>	<p>Применяет на практике методы проектирования программных (программно-технических) средств защиты информации</p>	<p style="text-align: center;">Неудовлетворител</p> <p>Не имеет представления о методике формирования задания по безопасности</p> <p style="text-align: center;">Удовлетворительн</p> <p>Имеет представления о методике формирования задания по безопасности; о средствах прикладного, системного и специального назначения при его использования в процессе решения поставленных задач.</p> <p style="text-align: center;">Хорошо</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.</p> <p style="text-align: center;">Отлично</p> <p>Имеет представления о методике формирования задания по безопасности; о системах и инструментальных средствах</p>

Компетенция (индикатор)	Планируемые результаты обучения	Критерии оценивания результатов обучения
		<p align="center">Отлично</p> программирования; о средствах прикладного, системного и специального назначения при его использования в процессе решения поставленных задач. Знает назначение и структуру задания по безопасности.

ПК.3

Способен принимать участие в разработке программных (программно-технических) средств защиты информации

Компетенция (индикатор)	Планируемые результаты обучения	Критерии оценивания результатов обучения
<p>ПК.3.1 Ориентируется в методах разработки программных (программно-технических) средств защиты информации</p>	Ориентируется в методах разработки программных (программно-технических) средств защиты информации	<p align="center">Неудовлетворител</p> Не имеет представления о возможностях использования современных методик и технологий программирования для разработки защищенного программного обеспечения <p align="center">Удовлетворительн</p> Имеет представления о возможностях использования современных методик и технологий программирования для разработки защищенного программного обеспечения <p align="center">Хорошо</p> Использует современные методики и технологии программирования для разработки защищенного программного обеспечения <p align="center">Отлично</p> Имеет представления о возможностях использования современных методик и технологий программирования для разработки защищенного программного обеспечения. Использует современных методик и технологии программирования для разработки защищенного программного обеспечения
<p>ПК.3.2 Применяет на практике методы разработки программных (программно-</p>	Применяет на практике методы разработки программных (программно-технических) средств защиты информации	<p align="center">Неудовлетворител</p> Не способен разрабатывать математические модели защищаемых систем и системы обеспечения информационной безопасности компьютерных систем

Компетенция (индикатор)	Планируемые результаты обучения	Критерии оценивания результатов обучения
технических) средств защиты информации		<p style="text-align: center;">Удовлетворительн</p> <p>Способен со значительными затруднениями разрабатывать математические модели защищаемых систем и системы обеспечения информационной безопасности компьютерных систем</p> <p style="text-align: center;">Хорошо</p> <p>Способен с незначительными затруднениями разрабатывать математические модели защищаемых систем и системы обеспечения информационной безопасности компьютерных систем</p> <p style="text-align: center;">Отлично</p> <p>Способен без затруднений разрабатывать математические модели защищаемых систем и системы обеспечения информационной безопасности компьютерных систем</p>

Оценочные средства текущего контроля и промежуточной аттестации

Схема доставки : Очная 2019

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 (индикатор)	Мероприятие текущего контроля	Контролируемые элементы результатов обучения
ОПК.13.1 Применяет теоретические знания информационной безопасности и программирования для разработки компонент программно-аппаратных средств защиты информации	Функциональные требования безопасности, Требования доверия, Оценочные уровни доверия Письменное контрольное мероприятие	Функциональные требования безопасности, Требования доверия, Оценочные уровни доверия
ПК.3.2 Применяет на практике методы разработки программных (программно-технических) средств защиты информации ОПК.13.2 Проводит анализ безопасности компьютерных систем при применении разработанных компонент программно-аппаратных средств защиты информации	Методика формирования ПЗ Письменное контрольное мероприятие	Формирование Профиля Защиты

Компетенция (индикатор)	Мероприятие текущего контроля	Контролируемые элементы результатов обучения
<p>ПК.2.2 Применяет на практике методы проектирования программных (программно-технических) средств защиты информации</p> <p>ОПСК.2.2 Анализирует средства сред разработки программного обеспечения с целью выбора оптимального варианта для разработки защищенного программного обеспечения</p>	<p>Методика формирования ЗБ</p> <p>Письменное контрольное мероприятие</p>	<p>Формирование Задания по Безопасности</p>
<p>ОПСК.2.1 Применяет на практике современные среды разработки программного обеспечения</p> <p>ПК.3.1 Ориентируется в методах разработки программных (программно-технических) средств защиты информации</p> <p>ОПСК.3.1 Подготавливает типовые виды документации на защищенное программное обеспечение</p>	<p>Разработка ИС в защищенном исполнении</p> <p>Итоговое контрольное мероприятие</p>	<p>Разработанная документация на спроектированную информационную систему</p>

Спецификация мероприятий текущего контроля

Функциональные требования безопасности, Требования доверия, Оценочные уровни доверия

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 классов функциональных требований безопасности	10
Знание классов требований доверия	5
Знание оценочных уровней доверия	5

Методика формирования ПЗ

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 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 самостоятельной работы**

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

Проходной балл: **10**

Показатели оценивания	Баллы
Способность сформировать ЗБ для предоставленного объекта оценки	15
Знание методики формирования ЗБ	5

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: **40**

Проходной балл: **20**

Показатели оценивания	Баллы
Способность спроектировать и разработать ИС в защищенном исполнении	20
Знание принципов организации проектирования и разработки ИС в защищенном исполнении	10
Способность разработать проектную документацию	10