МИНОБРНАУКИ РОССИИ

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

Кафедра информационной безопасности и систем связи

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 «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 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.3 Способность решать стандартные задачи профессиональной деятельности на основе правовых и этических норм и с учетом основных требований информационной безопасности

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.15 Способность оценивать эффективность системы защиты информации в компьютерных системах

ПК.6 Способность разрабатывать математические модели защищаемых систем и системы обеспечения информационной безопасности компьютерных систем

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

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

ПСК.2 способность проводить анализ программного кода с целью поиска потенциальных уязвимостей и недокументированных возможностей

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

Направления подготовки	10.05.01 Компьютерная безопасность (направленность: 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 российский 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 российский 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 аудиторные 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. Сергеев М. В. Интранет-технологии и информационная безопасность:метод. пособие/М. В. Сергеев.-Пермь,2007.-212.-Библиогр.: с. 203-206

3. 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. 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-образовательной 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.3

Способность решать стандартные задачи профессиональной деятельности на основе правовых и этических норм и с учетом основных требований информационной безопасности

Компетенция (индикатор)	Планируемые результаты обучения	Критерии оценивания результатов обучения
ОПК.3 Способность решать стандартные задачи профессиональной деятельности на основе правовых и этических норм и с учетом основных требований информационной безопасности	Знать основные требования информационной безопасности. Уметь решать стандартные задачи профессиональной деятельности. Владеть навыками решения стандартных задач профессиональной деятельности на основе правовых и этических норм и с учетом основных требований информационной безопасности.	**Неудовлетворител** Не способен решать стандартные задачи профессиональной деятельности на основе правовых и этических норм и с учетом основных требований информационной безопасности. **Удовлетворительн** Способен со значительными затруднениями решать стандартные задачи профессиональной деятельности на основе правовых и этических норм и с учетом основных требований информационной безопасности. **Хорошо** Способен с незначительными затруднениями решать стандартные задачи профессиональной деятельности на основе правовых и этических норм и с учетом основных требований информационной безопасности. **Отлично** Способен без затруднений решать стандартные задачи профессиональной деятельности на основе правовых и этических норм и с учетом основных требований информационной безопасности.

ПК.15

Способность оценивать эффективность системы защиты информации в компьютерных системах

Компетенция (индикатор)	Планируемые результаты обучения	Критерии оценивания результатов обучения
ПК.15 Способность оценивать эффективность системы	Знать компоненты системы защиты информации. Уметь оценивать эффективность	**Неудовлетворител** Не имеет представления о методике формирования профиля защиты.

Компетенция (индикатор)	Планируемые результаты обучения	Критерии оценивания результатов обучения
защиты информации в компьютерных системах	системы защиты информации в компьютерных системах. Владеть методами оценки эффективности системы защиты информации в компьютерных системах.	**Удовлетворительн** Имеет представление о методике формирования профиля защиты. **Хорошо** Имеет представление о методике формирования профиля защиты. Знает назначение и структуру профиля защиты. **Отлично** Обладает знаниями о современных технологиях программирования для разработки защищенного программного обеспечения. Имеет представление о методике формирования профиля защиты. Знает назначение и структуру профиля защиты.

ПК.7

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

Компетенция (индикатор)	Планируемые результаты обучения	Критерии оценивания результатов обучения
ПК.7 Способность провести обоснование и выбор рационального решения по уровню обеспечения информационной безопасности компьютерных систем с учетом заданных требований	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.	**Неудовлетворител** Не способен провести обоснование решения по уровню обеспечения информационной безопасности компьютерных систем с учетом заданных требований **Удовлетворительн** Имеет представление о функциональных требованиях безопасности, требованиях доверия, имеет представление об использовании требований современных стандартов по безопасности компьютерных систем. **Хорошо** Имеет представление о функциональных требованиях безопасности, требованиях доверия. Обладает знаниями использования требований современных стандартов по безопасности компьютерных систем. **Отлично** Имеет представление о функциональных требованиях безопасности, требованиях доверия, оценочных уровнях доверия. Использует требования современных

Компетенция (индикатор)	Планируемые результаты обучения	Критерии оценивания результатов обучения
		Отлично стандартов по безопасности компьютерных систем при решении поставленных задач.

ПК.6

Способность разрабатывать математические модели защищаемых систем и системы обеспечения информационной безопасности компьютерных систем

Компетенция (индикатор)	Планируемые результаты обучения	Критерии оценивания результатов обучения
ПК.6 Способность разрабатывать математические модели защищаемых систем и системы обеспечения информационной безопасности компьютерных систем	Знать компоненты системы обеспечения информационной безопасности компьютерных систем. Уметь разрабатывать математические модели защищаемых систем и системы обеспечения информационной безопасности компьютерных систем. Владеть необходимым математическим аппаратом для разработки математических моделей защищаемых систем и системы обеспечения информационной безопасности компьютерных систем.	**Неудовлетворител** Не способен разрабатывать математические модели защищаемых систем и системы обеспечения информационной безопасности компьютерных систем **Удовлетворительн** Способен со значительными затруднениями разрабатывать математические модели защищаемых систем и системы обеспечения информационной безопасности компьютерных систем **Хорошо** Способен с незначительными затруднениями разрабатывать математические модели защищаемых систем и системы обеспечения информационной безопасности компьютерных систем **Отлично** Способен без затруднений разрабатывать математические модели защищаемых систем и системы обеспечения информационной безопасности компьютерных систем

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

Компетенция (индикатор)	Планируемые результаты обучения	Критерии оценивания результатов обучения
ПК.10 Способность участвовать в разработке системы	Знать составляющие системы защиты информации предприятия и подсистемы информационной безопасности	**Неудовлетворител** Не способен участвовать в разработке системы защиты информации предприятия и подсистемы информационной безопасности

Компетенция (индикатор)	Планируемые результаты обучения	Критерии оценивания результатов обучения
защиты информации предприятия и подсистемы информационной безопасности компьютерной системы, разрабатывать формальные модели политик безопасности, политик управления доступом и информационными потоками в компьютерных системах	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	**Неудовлетворител** компьютерной системы, разрабатывать формальные модели политик безопасности, политик управления доступом и информационными потоками в компьютерных системах **Удовлетворительн** 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 **Хорошо** 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 **Отлично** Способен без затруднений 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

ПСК.1

способность использовать современные методики и технологии программирования для разработки защищенного программного обеспечения

Компетенция (индикатор)	Планируемые результаты обучения	Критерии оценивания результатов обучения
ПСК.1 способность использовать современные методики	Знать современные методики и технологии программирования. Уметь разрабатывать защищенное программное	**Неудовлетворител** Не имеет представления о возможностях использования современных методик и технологий программирования для

Компетенция (индикатор)	Планируемые результаты обучения	Критерии оценивания результатов обучения
и технологии программирования для разработки защищенного программного обеспечения	обеспечение. Владеть навыками использования современных методик и технологий программирования для разработки защищенного программного обеспечения	**Неудовлетворител** разработки защищенного программного обеспечения **Удовлетворительн** Имеет представления о возможностях использования современных методик и технологий программирования для разработки защищенного программного обеспечения **Хорошо** Использует современные методики и технологии программирования для разработки защищенного программного обеспечения **Отлично** 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

ПСК.6

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

Компетенция (индикатор)	Планируемые результаты обучения	Критерии оценивания результатов обучения
ПСК.6 Способность применять языки, системы и инструментальные средства программирования, работать с программными средствами прикладного, системного и специального назначения в профессиональной	Знать языки, системы и инструментальные средства программирования. Уметь работать с программными средствами прикладного, системного и специального назначения в профессиональной деятельности	**Неудовлетворител** Не имеет представления о методике формирования задания по безопасности **Удовлетворительн** Имеет представления о методике формирования задания по безопасности; о средствах прикладного, системного и специального назначения при его использования в процессе решения поставленных задач. **Хорошо** Имеет представления о методике формирования задания по безопасности; о системах и инструментальных средствах

Компетенция (индикатор)	Планируемые результаты обучения	Критерии оценивания результатов обучения
деятельности		**Хорошо** программирования; о средствах прикладного, системного и специального назначения при его использования в процессе решения поставленных задач. **Отлично** 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.

ПСК.2

способность проводить анализ программного кода с целью поиска потенциальных уязвимостей и недокументированных возможностей

Компетенция (индикатор)	Планируемые результаты обучения	Критерии оценивания результатов обучения
ПСК.2 способность проводить анализ программного кода с целью поиска потенциальных уязвимостей и недокументированных возможностей	Знать потенциальные уязвимости программного кода. Уметь проводить анализ программного кода с целью поиска потенциальных уязвимостей и недокументированных возможностей. Владеть методами анализа программного кода с целью поиска потенциальных уязвимостей и недокументированных возможностей.	**Неудовлетворител** Не способен проводить анализ программного кода с целью поиска потенциальных уязвимостей и недокументированных возможностей **Удовлетворительн** Способен со значительными затруднениями проводить анализ программного кода с целью поиска потенциальных уязвимостей и недокументированных возможностей **Хорошо** Способен с незначительными затруднениями проводить анализ программного кода с целью поиска потенциальных уязвимостей и недокументированных возможностей **Отлично** Способен без затруднений проводить анализ программного кода с целью поиска потенциальных уязвимостей и недокументированных возможностей

ПСК.4

способность проводить разработку программного обеспечения в соответствии с существующими технологиями промышленной разработки программных продуктов

Компетенция (индикатор)	Планируемые результаты обучения	Критерии оценивания результатов обучения
ПСК.4 способность проводить разработку программного обеспечения в соответствии с существующими технологиями промышленной разработки программных продуктов	Знать существующие технологии промышленной разработки программных продуктов. Уметь проводить разработку программного обеспечения в соответствии с существующими технологиями промышленной разработки программных продуктов	**Неудовлетворител** Не способен проводить разработку программного обеспечения в соответствии с существующими технологиями промышленной разработки программных продуктов **Удовлетворительн** Способен со значительными затруднениями проводить разработку программного обеспечения в соответствии с существующими технологиями промышленной разработки программных продуктов **Хорошо** Способен с незначительными затруднениями проводить разработку программного обеспечения в соответствии с существующими технологиями промышленной разработки программных продуктов **Отлично** Способен без затруднений проводить разработку программного обеспечения в соответствии с существующими технологиями промышленной разработки программных продуктов

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
ПК.7 Способность провести обоснование и выбор рационального решения по уровню обеспечения информационной безопасности компьютерных систем с учетом заданных требований	Функциональные требования безопасности, Требования доверия, Оценочные уровни доверия **Письменное контрольное мероприятие**	Функциональные требования безопасности, Требования доверия, Оценочные уровни доверия
ПК.6 Способность разрабатывать математические модели защищаемых систем и системы обеспечения информационной безопасности компьютерных систем **ПК.15** Способность оценивать эффективность системы защиты информации в компьютерных системах	Методика формирования ПЗ **Письменное контрольное мероприятие**	Формирование Профиля Защиты

Компетенция (индикатор)	Мероприятие текущего контроля	Контролируемые элементы результатов обучения
ПСК.2 способность проводить анализ программного кода с целью поиска потенциальных уязвимостей и недокументированных возможностей **ПСК.6** Способность применять языки, системы и инструментальные средства программирования, работать с программными средствами прикладного, системного и специального назначения в профессиональной деятельности	Методика формирования ЗБ **Письменное контрольное мероприятие**	Формирование Задания по Безопасности

Компетенция (индикатор)	Мероприятие текущего контроля	Контролируемые элементы результатов обучения
ПСК.1 способность использовать современные методики и технологии программирования для разработки защищенного программного обеспечения **ОПК.3** Способность решать стандартные задачи профессиональной деятельности на основе правовых и этических норм и с учетом основных требований информационной безопасности **ПСК.4** способность проводить разработку программного обеспечения в соответствии с существующими технологиями промышленной разработки программных продуктов **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	Разработка ИС в защищенном исполнении **Итоговое контрольное мероприятие**	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 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