МИНОБРНАУКИ РОССИИ

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

Кафедра информационной безопасности и систем связи

Авторы-составители: **Лобков Армандо Львович**
Мустакимова Яна Романовна

Рабочая программа дисциплины

РАЗРАБОТКА СРЕДСТВ ЗАЩИТЫ ИНФОРМАЦИИ

Код УМК 46034

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

Пермь, 2020

1. Наименование дисциплины

Разработка средств защиты информации

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 **Разработка средств защиты информации** 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.22 способность использовать нормативные правовые документы в своей профессиональной деятельности

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

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

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	13
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 практических занятий, семинаров	28
Самостоятельная работа (ак.час.)	88
Формы текущего контроля	Защищаемое контрольное мероприятие (2) Итоговое контрольное мероприятие (1)
Формы промежуточной аттестации	Экзамен (13 триместр)

5. Аннотированное описание содержания разделов и тем дисциплины

Разработка средств защиты информации.Первый семестр

Раздел 1. Законодательная база РФ в области осущсетвления деятельности по разработке средств защиты информации

Законы РФ в области разработки средств защиты информации
- структура законодательства в области разработки и применения средств защиты информации;
- ФЗ "О лицензировании отдельных видов деятельности".

Положение о лицензировании деятельности по разработке срелдств защиты информации
- постановление Правительства РФ "О лицензировании деятельности по технической защите конфиденциальной информации";
- постановление Правительства РФ "О лицензировании деятельности по разработке и (или) производству средств защиты информации".

Раздел 2. Электромагнитные волны и их распространение

Принципы распространения радиоволн
- распространение радиоволн вдоль поверхности Земли;
- состав и строение земной атмосферы, тропосферы и их особенности.

Принципы распространения радиоволн СДВ и СК диапазонов
- сверхдлинные, длинные поверхностные и ионосферные волны, особенности их распространения;
- средние волны, дневное и ночное их распространение.

Принципы распространения радиоволн КВ и УКВ диапазонов
- короткие волны, роль различных слоев ионосферы в формировании ионосферных волн;
- зоны молчан7ия и замирания, возникающие при распространении КВ радиоволн;
- особенности распространения радиоволн УКВ диапазона, влияние тропосферы, ионосферы и не гладкости поверхности Земли.

Раздел 3. Принципы построения антенных устройств как средств защиты информации

Использование антенных устройств для обнаружения каналов утечки информации
- основные параметры и характеристики антенных устройств и их взаимность;
- элементарный электрический излучатель, симметричный и несимметричный вибраторы и их особенности.

Классификация антенных устройств и принципы их построения
- разновидности антенных устройств ДВ, СВ диапазонов длин волн;
- антенные системы КВ диапазонов длин волн;
- антенные устройства УКВ диапазонов длин волн.

Раздел 4. Построение средств защиты объектов информатизации для закрытия каналов утечки информации

Принципы построения генераторов как устройств создания преднамеренных помех радиоэлектронному каналу утечки информации
- трехточечные схемы автогенераторов;
- стабилизация частоты в автогенераторе.

Принципы построения широкополосных генераторов

- функциональные и принципиальные схемы широкополосных генераторов.

Основы передачи информации по радиоканалам

- принципы построения радиопередающих устройств как средств защиты информации;
- структурные и функциональные схемы радиопередающих устройств.

Принципы работы функциональных каскадов радиопередающих устройств

- генерирование радиочастотных колебаний в передающих устройствах;
- резонансные усилители и делители частоты;
- усилители мощности и модуляторы.

Основы приема информации по радиоканалам

- структурные и функциональные схемы радиоприемных устройств;
- принципы построения супергетеродинных приемных устройств.

Принципы работы функциональных каскадов радиоприемных устройств как техническихъ средств защиты информации

- входные цепи, избирательность и помехоустойчивость приема;
- резонансные усилители радиочастоты и преобразователи частоты;
- усилители промежуточной частоты;
- разновидности и принцип действия детекторных устройств;
- усилители низкой частоты.

Принципы построения приемных устройств в оптическом диапазоне длин волн как технических средств защиты информации

- разновидности приемных устройств, работающих в оптическом диапазоне длин волн;
- принципы работы функциональных и принципиальных каскадов приемных устройств в оптическом диапазоне длин волн.

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. Соболев А. Н.,Кириллов В. М. Физические основы технических средств обеспечения информационной безопасности:учеб. пособие для студентов вузов/А. Н. Соболев, В. М. Кириллов.-М.:Гелиос АРВ,2004, ISBN 5-85438-084-6.-224.-Библиогр.: с. 215-218

Дополнительная:

1. Технические средства обеспечения информационной безопасности.учеб. пособие: В 2 ч./М-во образования и науки РФ.Ч. 1.Технические каналы утечки информации,2004.-199

2. Технические средства обеспечения информационной безопасности.Ч. 2.Средства защиты информации от утечки по техническим каналам,2004.-279

3. Торокин А. А. Иженерно-техническая защита информации:учеб. пособие/А. А. Торокин.-М.:Гелиос АРВ,2005, ISBN 5-85438-140-0.-960.-Библиогр.: с. 934-949

9. Перечень ресурсов сети Интернет, необходимых для освоения дисциплины

http://www.psu.ru/elektronnye-resursy-dlya-psu Электронные ресурсы для ПГНИУ
http://www.mathnet.ru/ Общероссийский математический портал
http://window.edu.ru/ Единое окно доступа к образовательным ресурсам

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

Образовательный процесс по дисциплине **Разработка средств защиты информации** предполагает использование следующего программного обеспечения и информационных справочных систем:
Образовательный процесс по дисциплине "Разработка средств защиты информации" 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";
- MS Word; MS Excel; Multisim; MathCAD.
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, меловой (и) или маркерной доской.
Для проведения практических занятий - аудитория, аудитория оснащенная презентационной техникой (проектор, экран, компьютер/ноутбук) с соответствующим программным обеспечением, меловой (и) или маркерной доской.
Для групповых (индивидуальных) консультаций - аудитория, оснащенная презентационной техникой (проектор, экран, компьютер/ноутбук) с соответствующим программным обеспечением, меловой (и) или маркерной доской.
Для проведения текущего контроля - аудитория, оснащенная меловой (и) или маркерной доской.
Самостоятельная работа студентов: аудитория, оснащенная компьютерной техникой с возможностью подключения к сети "Интерне, 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
Разработка средств защиты информации

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

Компетенция	Планируемые результаты обучения	Критерии оценивания результатов обучения
ПК.22 способность использовать нормативные правовые документы в своей профессиональной деятельности	знать нормативные правовые документы уметь использовать их в своей профессиональной деятельности	**Неудовлетворител** Не демонстрирует знание основного содержания дисциплины «Разработка средств защиты информации». Не владеет основными понятиями, законами и теорией, необходимыми для объяснения процессов в сфере построения средств защиты информации. Не умеет выполнять типовые задания и задачи, предусмотренные программой. **Удовлетворительн** Демонстрирует знание основного содержания дисциплины «Разработка средств защиты информации» и его элементов в соответствии с прослушанным лекционным курсом; Владение основными понятиями, законами и теорией, необходимыми для объяснения процессов связанных с разработкой средств защиты информации; Показывает умение выполнять типовые задания и задачи, предусмотренные программой; Выполняет математические расчеты с ошибками. **Хорошо** Ответ по вопросу или заданию аргументированный, демонстрирующий знание основного содержания дисциплины «разработка средств защиты информации» и его элементов в соответствии с прослушанным лекционным курсом и с учебной литературой. Демонстрирует понимание материала, приводит примеры в соответствии с

Компетенция	Планируемые результаты обучения	Критерии оценивания результатов обучения
		Хорошо программой изученного материала. Владение основными понятиями, законами и теорией, необходимыми для объяснения закономерностей при разработке средств защиты информации; Показывает владение методологией дисциплины, умение выполнять типовые задания и задачи, предусмотренные программой дисциплины «Разработка средств защиты информации». Выполняет теоретические расчеты с ошибками. **Отлично** Ответ на поставленный вопрос аргументированный, логически выстроенный, полный, демонстрирующий знание основного содержания дисциплины «Разработка средств защиты информации» и его элементов в соответствии с прослушанным лекционным курсом и с учебной литературой. Демонстрирует полное понимание материала дисциплины «Разработка средств защиты информации», выводы доказательны, приводит примеры из области построения технических средств защиты информации. Свободное владение основными понятиями, законами и теорией, необходимыми для объяснения закономерностей вопросов дисциплины «Разработка средств защиты информации». Показывает владение методологией дисциплины, умение выполнять типовые задания и задачи, предусмотренные программой дисциплины «разработка средств защиты информации». Выполняет расчеты без ошибок. Демонстрирует способность творчески применять знание теории к решению профессиональных практических задач в области построения средств защиты информации.

Компетенция	Планируемые результаты обучения	Критерии оценивания результатов обучения
ПК.23 Способность организовать защиту информации техническими и программными средствами, включая приемы антивирусной защиты при работе с компьютерными системами	знать технические и программные средства защиты информации уметь проводить настройку технических и программных средств защиты информации, включая антивирусные средства защиты владеть навыками применения технических и программных средств защиты информации, включая применения антивирусных средств защиты	**Неудовлетворител** Не демонстрирует знание основного содержания дисциплины «Разработка средств защиты информации». Не владеет основными понятиями, законами и теорией, необходимыми для объяснения процессов в сфере построения средств защиты информации. Не умеет выполнять типовые задания и задачи, предусмотренные программой. **Удовлетворительн** Демонстрирует знание основного содержания дисциплины «Разработка средств защиты информации» и его элементов в соответствии с прослушанным лекционным курсом; Владение основными понятиями, законами и теорией, необходимыми для объяснения процессов связанных с разработкой средств защиты информации; Показывает умение выполнять типовые задания и задачи, предусмотренные программой; Выполняет математические расчеты с ошибками. **Хорошо** Ответ по вопросу или заданию аргументированный, демонстрирующий знание основного содержания дисциплины «разработка средств защиты информации» и его элементов в соответствии с прослушанным лекционным курсом и с учебной литературой. Демонстрирует понимание материала, приводит примеры в соответствии с программой изученного материала. Владение основными понятиями, законами и теорией, необходимыми для объяснения закономерностей при разработке средств защиты информации; Показывает владение методологией дисциплины, умение выполнять типовые задания и задачи, предусмотренные

Компетенция	Планируемые результаты обучения	Критерии оценивания результатов обучения
		Хорошо программой дисциплины «Разработка средств защиты информации». Выполняет теоретические расчеты с ошибками. **Отлично** Ответ на поставленный вопрос аргументированный, логически выстроенный, полный, демонстрирующий знание основного содержания дисциплины «Разработка средств защиты информации» и его элементов в соответствии с прослушанным лекционным курсом и с учебной литературой. Демонстрирует полное понимание материала дисциплины «Разработка средств защиты информации», выводы доказательны, приводит примеры из области построения технических средств защиты информации. Свободное владение основными понятиями, законами и теорией, необходимыми для объяснения закономерностей вопросов дисциплины «Разработка средств защиты информации». Показывает владение методологией дисциплины, умение выполнять типовые задания и задачи, предусмотренные программой дисциплины «разработка средств защиты информации». Выполняет расчеты без ошибок. Демонстрирует способность творчески применять знание теории к решению профессиональных практических задач в области построения средств защиты информации.
ПК.7 Способность провести обоснование и выбор рационального решения по уровню обеспечения информационной безопасности компьютерных систем с	знать основы информационной безопасности, средства защиты информации уметь определять уровень обеспечения информационной безопасности в компьютерных системах владеть навыками проводить	**Неудовлетворител** Не демонстрирует знание основного содержания дисциплины «Разработка средств защиты информации». Не владеет основными понятиями, законами и теорией, необходимыми для объяснения процессов в сфере построения средств защиты информации.

Компетенция	Планируемые результаты обучения	Критерии оценивания результатов обучения
учетом заданных требований	обоснование и выбор рационального решения по уровню обеспечения информационной безопасности применения средств защиты информации с учетом заданных требований	**Неудовлетворител** Не умеет выполнять типовые задания и задачи, предусмотренные программой. **Удовлетворительн** Демонстрирует знание основного содержания дисциплины «Разработка средств защиты информации» и его элементов в соответствии с прослушанным лекционным курсом; Владение основными понятиями, законами и теорией, необходимыми для объяснения процессов связанных с разработкой средств защиты информации; Показывает умение выполнять типовые задания и задачи, предусмотренные программой; Выполняет математические расчеты с ошибками. **Хорошо** Ответ по вопросу или заданию аргументированный, демонстрирующий знание основного содержания дисциплины «разработка средств защиты информации» и его элементов в соответствии с прослушанным лекционным курсом и с учебной литературой. Демонстрирует понимание материала, приводит примеры в соответствии с программой изученного материала. Владение основными понятиями, законами и теорией, необходимыми для объяснения закономерностей при разработке средств защиты информации; Показывает владение методологией дисциплины, умение выполнять типовые задания и задачи, предусмотренные программой дисциплины «Разработка средств защиты информации». Выполняет теоретические расчеты с ошибками. **Отлично** Ответ на поставленный вопрос

Компетенция	Планируемые результаты обучения	Критерии оценивания результатов обучения
		Отлично аргументированный, логически выстроенный, полный, демонстрирующий знание основного содержания дисциплины «Разработка средств защиты информации» и его элементов в соответствии с прослушанным лекционным курсом и с учебной литературой. Демонстрирует полное понимание материала дисциплины «Разработка средств защиты информации», выводы доказательны, приводит примеры из области построения технических средств защиты информации. Свободное владение основными понятиями, законами и теорией, необходимыми для объяснения закономерностей вопросов дисциплины «Разработка средств защиты информации». Показывает владение методологией дисциплины, умение выполнять типовые задания и задачи, предусмотренные программой дисциплины «разработка средств защиты информации». Выполняет расчеты без ошибок. Демонстрирует способность творчески применять знание теории к решению профессиональных практических задач в области построения средств защиты информации.
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	знать содержание формальных моделей политик информационной безопасности уметь разрабатывать формальные модели политик информационной безопасности на предприятии	**Неудовлетворител** Не демонстрирует знание основного содержания дисциплины «Разработка средств защиты информации». Не владеет основными понятиями, законами и теорией, необходимыми для объяснения процессов в сфере построения средств защиты информации. Не умеет выполнять типовые задания и задачи, предусмотренные программой. **Удовлетворительн** Демонстрирует знание основного содержания дисциплины «Разработка средств защиты информации» и его

Компетенция	Планируемые результаты обучения	Критерии оценивания результатов обучения
информационными потоками в компьютерных системах		**Удовлетворительн** элементов в соответствии с прослушанным лекционным курсом; Владение основными понятиями, законами и теорией, необходимыми для объяснения процессов связанных с разработкой средств защиты информации; Показывает умение выполнять типовые задания и задачи, предусмотренные программой; Выполняет математические расчеты с ошибками. **Хорошо** Ответ по вопросу или заданию аргументированный, демонстрирующий знание основного содержания дисциплины «разработка средств защиты информации» и его элементов в соответствии с прослушанным лекционным курсом и с учебной литературой. Демонстрирует понимание материала, приводит примеры в соответствии с программой изученного материала. Владение основными понятиями, законами и теорией, необходимыми для объяснения закономерностей при разработке средств защиты информации; Показывает владение методологией дисциплины, умение выполнять типовые задания и задачи, предусмотренные программой дисциплины «Разработка средств защиты информации». Выполняет теоретические расчеты с ошибками. **Отлично** Ответ на поставленный вопрос аргументированный, логически выстроенный, полный, демонстрирующий знание основного содержания дисциплины «Разработка средств защиты информации» и его элементов в соответствии с прослушанным лекционным курсом и с учебной литературой.

Компетенция	Планируемые результаты обучения	Критерии оценивания результатов обучения
		Отлично Демонстрирует полное понимание материала дисциплины «Разработка средств защиты информации», выводы доказательны, приводит примеры из области построения технических средств защиты информации. Свободное владение основными понятиями, законами и теорией, необходимыми для объяснения закономерностей вопросов дисциплины «Разработка средств защиты информации». Показывает владение методологией дисциплины, умение выполнять типовые задания и задачи, предусмотренные программой дисциплины «разработка средств защиты информации». Выполняет расчеты без ошибок. Демонстрирует способность творчески применять знание теории к решению профессиональных практических задач в области построения средств защиты информации.
ПСК.6 Способность применять языки, системы и инструментальные средства программирования, работать с программными средствами прикладного, системного и специального назначения в профессиональной деятельности	знать языки, системы и инструментальные средства программирования уметь работать с программными средствами прикладного, системного и специального назначения в профессиональной деятельности	**Неудовлетворител** Не демонстрирует знание основного содержания дисциплины «Разработка средств защиты информации». Не владеет основными понятиями, законами и теорией, необходимыми для объяснения процессов в сфере построения средств защиты информации. Не умеет выполнять типовые задания и задачи, предусмотренные программой. **Удовлетворительн** Демонстрирует знание основного содержания дисциплины «Разработка средств защиты информации» и его элементов в соответствии с прослушанным лекционным курсом; Владение основными понятиями, законами и теорией, необходимыми для объяснения процессов связанных с разработкой средств защиты информации; Показывает умение выполнять типовые

Компетенция	Планируемые результаты обучения	Критерии оценивания результатов обучения
		Удовлетворительн задания и задачи, предусмотренные программой; Выполняет математические расчеты с ошибками. **Хорошо** Ответ по вопросу или заданию аргументированный, демонстрирующий знание основного содержания дисциплины «разработка средств защиты информации» и его элементов в соответствии с прослушанным лекционным курсом и с учебной литературой. Демонстрирует понимание материала, приводит примеры в соответствии с программой изученного материала. Владение основными понятиями, законами и теорией, необходимыми для объяснения закономерностей при разработке средств защиты информации; Показывает владение методологией дисциплины, умение выполнять типовые задания и задачи, предусмотренные программой дисциплины «Разработка средств защиты информации». Выполняет теоретические расчеты с ошибками. **Отлично** Ответ на поставленный вопрос аргументированный, логически выстроенный, полный, демонстрирующий знание основного содержания дисциплины «Разработка средств защиты информации» и его элементов в соответствии с прослушанным лекционным курсом и с учебной литературой. Демонстрирует полное понимание материала дисциплины «Разработка средств защиты информации», выводы доказательны, приводит примеры из области построения технических средств защиты информации. Свободное владение основными понятиями, законами и теорией, необходимыми для

Компетенция	Планируемые результаты обучения	Критерии оценивания результатов обучения
		Отлично объяснения закономерностей вопросов дисциплины «Разработка средств защиты информации». Показывает владение методологией дисциплины, умение выполнять типовые задания и задачи, предусмотренные программой дисциплины «разработка средств защиты информации». Выполняет расчеты без ошибок. Демонстрирует способность творчески применять знание теории к решению профессиональных практических задач в области построения средств защиты информации.

Оценочные средства текущего контроля и промежуточной аттестации

Схема доставки : СУОС

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
ПК.23 Способность организовать защиту информации техническими и программными средствами, включая приемы антивирусной защиты при работе с компьютерными системами	Принципы распространения радиоволн КВ и УКВ диапазонов **Защищаемое контрольное мероприятие**	Знание принципов распространения радиоволн различныхдиапазонов
ПК.7 Способность провести обоснование и выбор рационального решения по уровню обеспечения информационной безопасности компьютерных систем с учетом заданных требований	Принципы построения широкополосных генераторов **Защищаемое контрольное мероприятие**	Умение проводить расчеты по построению электрических схем средств защиты информации

Компетенция	Мероприятие текущего контроля	Контролируемые элементы результатов обучения
ПСК.6 Способность применять языки, системы и инструментальные средства программирования, работать с программными средствами прикладного, системного и специального назначения в профессиональной деятельности **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.22** способность использовать нормативные правовые документы в своей профессиональной деятельности	Принципы построения приемных устройств в оптическом диапазоне длин волн как технических средств защиты информации **Итоговое контрольное мероприятие**	Знать математический аппарат расчета электрических схем устройств защиты информации

Спецификация мероприятий текущего контроля

Принципы распространения радиоволн КВ и УКВ диапазонов

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
Умение проводить расчеты по распространению радиоволн	30

Принципы построения широкополосных генераторов

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

Знание принципов построения электрических схем устройств защиты информации	30

Принципы построения приемных устройств в оптическом диапазоне длин волн как технических средств защиты информации

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
Умение проводить расчеты параметров электрических схем устройств защиты информации	40