МИНОБРНАУКИ РОССИИ

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

Кафедра радиоэлектроники и защиты информации

Авторы-составители: **Лунегов Игорь Владимирович**

Рабочая программа дисциплины

РАДИОТЕХНИЧЕСКИЕ СРЕДСТВА ЗАЩИТЫ ИНФОРМАЦИИ

Код УМК 63277

Утверждено
Протокол №4
от «24» июня 2020 г.

Пермь, 2020

1. Наименование дисциплины

Радиотехнические средства защиты информации

2. Место дисциплины в структуре образовательной программы

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

Направление: **03.03.03** Радиофизика

направленность Электроника, микро- и наноэлектроника

3. Планируемые результаты обучения по дисциплине

В результате освоения дисциплины **Радиотехнические средства защиты информации** у обучающегося должны быть сформированы следующие компетенции:

03.03.03 Радиофизика (направленность : Электроника, микро- и наноэлектроника)

ПК.3 владеть методами защиты интеллектуальной собственности

ПК.6 способность к подготовке документации на проведение НИР (смет, заявок на материалы, оборудование, трудовых договоров и т.п.), а также поиску в сети Интернет материально-технических и информационных ресурсов для обеспечения НИР

4. Объем и содержание дисциплины

Направления подготовки	03.03.03 Радиофизика (направленность: Электроника, микро- и наноэлектроника)
форма обучения	очная
№№ триместров, выделенных для изучения дисциплины	11
Объем дисциплины (з.е.)	3
Объем дисциплины (ак.час.)	108
Контактная работа с преподавателем (ак.час.), в том числе:	42
Проведение лекционных занятий	14
Проведение лабораторных работ, занятий по иностранному языку	28
Самостоятельная работа (ак.час.)	66
Формы текущего контроля	Входное тестирование (1) Защищаемое контрольное мероприятие (2) Итоговое контрольное мероприятие (1)
Формы промежуточной аттестации	Зачет (11 триместр)

5. Аннотированное описание содержания разделов и тем дисциплины

Радиотехнические средства защиты информации.Первый семестр

Основы информационной безопасности. Основные понятия

Системный подход к защите информации

Основные понятия в области информационной безопасности. Основные проблемы инженерно-технической защиты информации. Основные параметры систем защиты информации

Основные положения инженерно-технической защиты информации

Цели и задачи защиты информации. Ресурсы, выделяемы на защиту информации. Принципы защиты информации техническими средствами. Основные направления инженерно-технической защиты информации. Показатели эффективности защиты информации

Государственная система защиты информации

Основные руководящие, нормативные и методические документы по защите информации. Основные организационные и технические меры по защите информации. Аттестация объектов, лицензирование деятельности по защите информации и сертифицирование ее средств

Теоретические основы инженерно-технической защиты информации

Информации как предмет защиты

Особенности информации как предмета защиты. Свойства информации. Виды, источники и носители защищаемой информации

Источники опасных сигналов

Понятие об опасном сигнале. Основные и вспомогательные технические средства и системы как источники опасных сигналов. Состав и краткая характеристика основных и вспомогательных технических средств и сисем. Образование опасных сигналов в результате побочных электромагнитных излучений и наводок

Технические каналы утечки информации

Понятие и особенности утечки информации. Структура, классификация и основные характеристики технических каналов утечки информации. Оптические, акустические, радиоэлектронные и материально-вещественные каналы утечки информации, их характеристика

Методы инженерной защиты и технической охраны объектов

Классификация способов и методов защиты информации. Основные угрозы и факторы в автоматизированных системах. Модели злоумышленника

Физические основы защиты информации

Физические основы побочных излучений и наводок

Акустоэлектрические преобразования. Источники побочных излучений. Характер электромагнитных излучений в ближней и дальней зонах. Виды паразитных связей и наводок. Утечка опасных сигналов по цепям электропитания и заземления

Распространение сигналов в технических каналах утечки информации

Распространение акустических сигналов в атмосфере, воде и в твердой среде. Особенности распространения акустических сигналов в помещениях. Распространение оптических сигналов в атмосфере и в светопроводах. Распространение радиосигналов различных диапазонов в пространстве и по направляюшим линиям связи.. Характеристика среды распространения сигналов различных

технических каналов утечки информации

Радиотехнические средства инженерно-технической защиты информации

Средства инженерной защиты и технической охраны

Основные инженерные конструкции, применяемые для предотвращения проникновения злоумышленника к источникам информации. Средства управления доступом. Классификация и характеристика охранных, охранно-пожарных и пожарных извещателей. Средства видеоконтроля и видеоохраны. Средства нейтрализации угроз. Средства управления и передачи извещений. Автоматизированные интегральные системы охраны

Средства предотвращения утечки информации по техническим каналам

Средства защиты в радиодиапазонах. Средства звукоизоляции из звукопоглощения. Средства обнаружения, локализации и подавления сигналов закладных устройств. Средства подавления сигналов акустоэлектрических преобразователей, фильтрации и заземления. Генераторы линейного и пространственного зашумления

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. Внуков, А. А. Основы информационной безопасности: защита информации : учебное пособие для среднего профессионального образования / А. А. Внуков. — 3-е изд., перераб. и доп. — Москва : Издательство Юрайт, 2020. — 161 с. — (Профессиональное образование). — ISBN 978-5-534-13948-8. — Текст : электронный // ЭБС Юрайт [сайт]. https://urait.ru/bcode/467356

2. Скрипник, Д. А. Общие вопросы технической защиты информации : учебное пособие / Д. А. Скрипник. — 3-е изд. — Москва, Саратов : Интернет-Университет Информационных Технологий (ИНТУИТ), Ай Пи Ар Медиа, 2020. — 424 с. — ISBN 978-5-4497-0336-1. — Текст : электронный // Электронно-библиотечная система IPR BOOKS : [сайт]. http://www.iprbookshop.ru/89451.html

Дополнительная:

1. Галатенко В. А. Основы информационной безопасности:курс лекций : учеб. пособие для студентов вузов, обучающихся по спец. 351400 "Прикл. информатика"/под ред. В. Б. Бетелина; Интернет-Ун-т Информ. Технологий.-Москва:Интернет-Университет информационных технологий,2004, ISBN 5-9556-0015-9.-264.-Библиогр.: с. 256-257

2. Фомин, Д. В. Информационная безопасность и защита информации: специализированные аттестованные программные и программно-аппаратные средства : учебно-методическое пособие / Д. В. Фомин. — Саратов : Вузовское образование, 2018. — 218 c. — ISBN 978-5-4487-0297-6. — Текст : электронный // Электронно-библиотечная система IPR BOOKS : [сайт]. http://www.iprbookshop.ru/77317.html

9. Перечень ресурсов сети Интернет, необходимых для освоения дисциплины

https://www.securitycode.ru Сайт компании код безопасности
https://nelk.ru/ Сайт компании "Нелк" производителя систем безопасности

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

Образовательный процесс по дисциплине **Радиотехнические средства защиты информации** предполагает использование следующего программного обеспечения и информационных справочных систем:
В учебном процессе для освоения дисциплины могут использоваться различные информационные технологии:
- презентационные материалы (слайды по темам лекционных и практических занятий);
- доступ в режиме on-line в Электронную библиотечную систему (ЭБС);
- доступ в электронную информационно-образовательную среду университета;
- интернет-сервисы и электронные ресурсы (поисковые системы, электронная почта, профессиональные тематические чаты и форумы, системы аудио и видео конференций, онлайн энциклопедии и т.д.).
Перечень необходимого лицензионного и (или) свободно распространяемого программного обеспечения:
1.Приложение позволяющее просматривать и воспроизводить медиаконтент PDF-файлов «Adobe Acrobat Reader DC».
2.Программы для демонстрации видео материалов (проигрыватель) «WindowsMediaPlayer».
3.Программа просмотра интернет контента (браузер) «Google Chrome».
4.Офисный пакет приложений «LibreOffice»
5. Операционная система Alt Linux

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

Аудитория для проведения занятий лекционного типа и проведения мероприятий текущего контроля оснащена презентационной техникой:
1) персональный компьютер или ноутбук с соответствующим программным обеспечением;
2) мультимедийное оборудование (проектор, экран);
3) маркерная доска и маркеры (или меловая доска и мел)

Аудитория для лабораторных занятий.
Лабораторные занятия проводятся в лаборатории радиотехнических средств защиты информации.
Учебные места лаборатории:
1. Исследование побочных электромагнитных излучений комплексом «Навигатор П3Г»

2. Измерение электромагнитных помех комплексом R&S ESL
3. Обнаружение радиоизлучающих средств комплексом "КРОНА Плюс"
4. Обнаружение скрытых источников радиоизлучения комплексом радиомониторинга «Кассандра»
5. Оценка защищенности акустической (речевой) информации от ее утечки комплексом «Спрут»
6. Обнаружение скрытых электронных средств с помощью нелинейного локатора "NR-900EMS"
7. Исследование средств активной виброакустической защиты
8. Исследование средств активной защиты информации от утечек по каналам GSM
Техническое оснащение лаборатории радиотехнических средств зашиты информации представлено в паспорте лаборатории.

Аудитория для самостоятельной работы:
1) компьютерная техника с возможностью подключения к сети «Интернет», с доступом в электронную информационно-образовательную среду ПГНИУ;
2) помещения Научной библиотеки ПГНИУ.

Аудитория для текущего контроля:
1) персональный компьютер или ноутбук с соответствующим программным обеспечением;
2) мультимедийное оборудование (проектор, экран);
3) маркерная доска и маркеры (или меловая доска и мел)

Аудитория для индивидуальных (групповых) консультаций:
1) персональный компьютер или ноутбук с соответствующим программным обеспечением;
2) мультимедийное оборудование (проектор, экран);
3) маркерная доска и маркеры (или меловая доска и мел)

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
Радиотехнические средства защиты информации

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

Компетенция	Планируемые результаты обучения	Критерии оценивания результатов обучения
ПК.3 владеть методами защиты интеллектуальной собственности	- знать нормативную базу по вопросам защиты информации, угрозы информационной безопасности, каналы утечки информации, технические средства по защите информации; - уметь определить состояние защищенности предприятия, выявлять потенциальные внешние и внутренние угрозы; - владеть методами по защите информации при передаче данных по открытым каналам связи.	**Неудовлетворител** Не знает основ дисциплины, необходимых при формировании компетенции Отсутствие умений Отсутствие навыков **Удовлетворительн** Общие, но не структурированные знания нормативной базы в области защиты информации, каналов утечки информации и технических средств по ее защите. Частично сформированные умения определить состояние защищенности предприятия, выявлять потенциальные внешние и внутренние угрозы. Фрагментарное применение навыков владения методами по защите информации при передаче данных по открытым каналам связи. **Хорошо** Сформированные но содержащие отдельные пробелы знания нормативной базы в области защиты информации, каналов утечки информации и технических средств по ее защите. В целом успешные, но содержащие отдельные пробелы умения определить состояние защищенности предприятия, выявлять потенциальные внешние и внутренние угрозы. В целом успешное, но содержащее отдельные пробелы применение навыков владения методами по защите информации при передаче данных по открытым каналам связи. **Отлично** Сформированные систематические знания нормативной базы в области защиты

Компетенция	Планируемые результаты обучения	Критерии оценивания результатов обучения
		Отлично информации, каналов утечки информации и технических средств по ее защите. Сформированное умение определить состояние защищенности предприятия, выявлять потенциальные внешние и внутренние угрозы. Успешное и систематическое применение навыков владения методами по защите информации при передаче данных по открытым каналам связи.
ПК.6 способность к подготовке документации на проведение НИР (смет, заявок на материалы, оборудование, трудовых договоров и т.п.), а также поиску в сети Интернет материально-технических и информационных ресурсов для обеспечения НИР	Знать основы документирования научной информации в области защиты информации. Уметь составлять документации на проведение НИР по технической защите информации. Владеть методами поиска в сети Интернет материально-технических и информационных ресурсов в области защиты информации	**Неудовлетворител** Отсутствие знаний Не знает основ дисциплины, необходимых при формировании компетенции Отсутствие умений Отсутствие навыков **Удовлетворительн** Общие, но не структурированные знания основ документирования научной информации в области защиты информации. Частично сформированное умение составлять документации на проведение НИР по технической защите информации. Фрагментарное применение навыков поиска в сети Интернет материально-технических и информационных ресурсов в области защиты информации. **Хорошо** Сформированные, но содержащие отдельные пробелы знания основ документирования научной информации в области защиты информации. В целом успешные, но содержащие отдельные пробелы умения составлять документации на проведение НИР по технической защите информации. В целом успешное, но содержащее отдельные пробелы применение навыков поиска в сети Интернет материально-технических и информационных ресурсов в области защиты информации. **Отлично** Сформированные систематические знания основ документирования научной

Компетенция	Планируемые результаты обучения	Критерии оценивания результатов обучения
		Отлично информации в области защиты информации. Сформированное умение составлять документации на проведение НИР по технической защите информации. Успешное и систематическое применение методов поиска в сети Интернет материально-технических и информационных ресурсов в области защиты информации

Оценочные средства текущего контроля и промежуточной аттестации

Схема доставки : СУОС

Вид мероприятия промежуточной аттестации : Зачет
Способ проведения мероприятия промежуточной аттестации : Оценка по дисциплине в рамках промежуточной аттестации определяется на основе баллов, набранных обучающимся на контрольных мероприятиях, проводимых в течение учебного периода.
Максимальное количество баллов : 100

Конвертация баллов в отметки

«отлично» - от 81 до 100
«хорошо» - от 61 до 80
«удовлетворительно» - от 41 до 60
«неудовлетворительно» / «незачтено» менее 41 балла

Компетенция	Мероприятие текущего контроля	Контролируемые элементы результатов обучения
Входной контроль	Системный подход к защите информации **Входное тестирование**	проверка остаточных знаний по электричеству, радиоэлектронике, методам радиофизических измерений
ПК.3 владеть методами защиты интеллектуальной собственности **ПК.6** способность к подготовке документации на проведение НИР (смет, заявок на материалы, оборудование, трудовых договоров и т.п.), а также поиску в сети Интернет материально-технических и информационных ресурсов для обеспечения НИР	Технические каналы утечки информации **Защищаемое контрольное мероприятие**	знание технических каналов утечки каналов утечки информации, методов несанкционированного доступа к информации
ПК.3 владеть методами защиты интеллектуальной собственности **ПК.6** способность к подготовке документации на проведение НИР (смет, заявок на материалы, оборудование, трудовых договоров и т.п.), а также поиску в сети Интернет материально-технических и информационных ресурсов для обеспечения НИР	Распространение сигналов в технических каналах утечки информации **Защищаемое контрольное мероприятие**	умение определить состояние защищенности предприятия, выявлять потенциальные внешние и внутренние угрозы

Компетенция	Мероприятие текущего контроля	Контролируемые элементы результатов обучения
ПК.3 владеть методами защиты интеллектуальной собственности **ПК.6** способность к подготовке документации на проведение НИР (смет, заявок на материалы, оборудование, трудовых договоров и т.п.), а также поиску в сети Интернет материально-технических и информационных ресурсов для обеспечения НИР	Средства предотвращения утечки информации по техническим каналам **Итоговое контрольное мероприятие**	знание нормативной базы по вопросам защиты информации, угроз информационной безопасности, каналов утечки информации, технических средств по защите информации; - умение определить состояние защищенности предприятия, выявлять потенциальные внешние и внутренние угрозы; - навыки владения методами по защите информации при передаче данных по открытым каналам связи.

Спецификация мероприятий текущего контроля

Системный подход к защите информации

Продолжительность проведения мероприятия промежуточной аттестации: **.5 часа**
Условия проведения мероприятия: **в часы аудиторной работы**
Максимальный балл, выставляемый за мероприятие промежуточной аттестации: **0**
Проходной балл: **0**

Показатели оценивания	Баллы
Допущено не более одной ошибки при тестировании	81
Допущено не более трех ошибок при тестировании	61
Допущено не более пяти ошибок при тестировании	41
Допущено более пяти ошибок при тестировании	0

Технические каналы утечки информации

Продолжительность проведения мероприятия промежуточной аттестации: **2 часа**
Условия проведения мероприятия: **в часы аудиторной работы**
Максимальный балл, выставляемый за мероприятие промежуточной аттестации: **30**
Проходной балл: **12**

Показатели оценивания	Баллы
Ответить на вопросы по теме лабораторной работы. Каждая ошибка при ответе на вопрос снижает балл на 2	15
Выполнить лабораторную работу и представить отчет	15

Распространение сигналов в технических каналах утечки информации

Продолжительность проведения мероприятия промежуточной аттестации: **2 часа**
Условия проведения мероприятия: **в часы аудиторной работы**
Максимальный балл, выставляемый за мероприятие промежуточной аттестации: **30**
Проходной балл: **12**

Показатели оценивания	Баллы
Ответить на вопросы преподавателя. Каждая ошибка при ответе на вопрос снижает балл на 2	15
выполнить лабораторные работы	15

Средства предотвращения утечки информации по техническим каналам

Продолжительность проведения мероприятия промежуточной аттестации: **2 часа**
Условия проведения мероприятия: **в часы аудиторной работы**
Максимальный балл, выставляемый за мероприятие промежуточной аттестации: **40**
Проходной балл: **17**

Показатели оценивания	Баллы
Ответить на вопросы преподавателя по теме лабораторной работы. Каждая ошибка при ответе на вопрос снижает балл на 2	20
выполнить лабораторную работу	20