БЕЛОРУССКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ

УТВЕРЖДАЮ
Проректор по учебной работе и образовательным инновациям

_____ О.И.Чуприс
(подпись)
18.05.18 2018 г.
(дата утверждения)
Регистрационный № УД-6151/уч.

РАДИОФИЗИЧЕСКИЕ МЕТОДЫ ЗАЩИТЫ ИНФОРМАЦИИ И ЭЛЕКТРОМАГНИТНАЯ СОВМЕСТИМОСТЬ

Учебная программа учреждения высшего образования по учебной дисциплине по специальности высшего образования второй ступени (магистратуры):

1-31 80 07 Радиофизика

2018 г.

Учебная программа составлена на основе образовательного стандарта высшего образования ОСВО 1-31 80 07-2012 Радиофизика и учебного плана БГУ G-31-284/уч. от 26.05.2017 г.

СОСТАВИТЕЛЬ:

В.Э.Яскевич, доцент кафедры радиофизики и цифровых медиатехнологий Белорусского государственного университета, кандидат технических наук.

РЕЦЕНЗЕНТЫ:

В.С.Садов, профессор кафедры интеллектуальных систем Белорусского государственного университета, кандидат технических наук, доцент;

С.В.Козлов, профессор кафедры информационных радиотехнологий Белорусского государственного университета информатики и радиоэлектроники, доктор технических наук, доцент.

РЕКОМЕНДОВАНА К УТВЕРЖДЕНИЮ:

Кафедрой радиофизики и цифровых медиатехнологий Белорусского государственного университета
(протокол № 14 от 19 июня 2018 года);

Научно-методическим советом Белорусского государственного университета
(протокол № 7 от 13 июля 2018 года).

ПОЯСНИТЕЛЬНАЯ ЗАПИСКА

ХАРАКТЕРИСТИКА УЧЕБНОЙ ДИСЦИПЛИНЫ

Учебная программа дисциплины «Радиофизические методы защиты информации и электромагнитная совместимость» разработана для студентов II ступени высшего образования (магистратуры) специальности 1-31 80 07 Радиофизика в соответствии с требованиями образовательного стандарта высшего образования ОСВО 1-31 80 07-2012.

Дисциплина входит в цикл дисциплин специальной подготовки и относится к дисциплинам государственного компонента.

«Радиофизические методы защиты информации и электромагнитная совместимость» – научно-практическая учебная дисциплина, в которой изучаются вопросы, связанные с формированием систем защиты информации от утечек по техническим каналам на объектах информатизации и обеспечение электромагнитной совместимости (ЭМС) оборудования информационных технологий радиофизическими методами.

ЦЕЛЬ, ЗАДАЧИ, РОЛЬ УЧЕБНОЙ ДИСЦИПЛИНЫ

Цель преподавания дисциплины: формирование базовых знаний и навыков специалиста в области радиофизических методов защиты информации и обеспечения ЭМС оборудования информационных технологий.

Задачи изучения дисциплины:

- изучение и классификация технических каналов утечки информации;
- изучение критериев защищенности и радиофизических методов защиты информации от утечек по техническим каналам;
- изучение разведывательных технологий и средств противодействия;
- изучение методов измерения побочных электромагнитных полей электронных устройств и комплексов и оценки защищенности объектов информатизации;
- изучение технических средств защиты информации;
- изучение основ обеспечения ЭМС, как в части снижения побочных электромагнитных излучений и наводок (ПЭМИН), так и в части повышения помехоустойчивости электронного оборудования.

Для успешного усвоения дисциплины необходимы знания, приобретенные магистрантами при обучении на I ступени высшего образования при изучении следующих дисциплин:

- «Теоретические основы информационной безопасности»;
- «Программно-аппаратные средства обеспечения информационной безопасности»;
- «Системы и сети передачи информации»;
- «Физические основы хранения, обработки и передачи информации»;
- «Статистическая радиофизика»;
- «Прикладная электродинамика»;

- «Квантовая радиофизика и оптоэлектроника»;
- «Теория колебаний и волн».

ТРЕБОВАНИЯ К УРОВНЮ ОСВОЕНИЯ СОДЕРЖАНИЯ УЧЕБНОЙ ДИСЦИПЛИНЫ

Освоение программы по учебной дисциплине «Радиофизические методы защиты информации и электромагнитная совместимость» должно обеспечить формирование следующих **компетенций**:

Академические:

- АК-1. Способность к самостоятельной научно-исследовательской деятельности (анализ, сопоставление, систематизация, абстрагирование, моделирование, проверка достоверности данных, применение решений), готовность генерировать и использовать новые идеи.
- АК-2. Методологические знания и исследовательские умения, обеспечивающие решение задач научно-исследовательской, научно-педагогической, организационно-управленческой и инновационной деятельности.

Социально-личностные:

- СЛК-1. Совершенствовать и развивать свой интеллектуальный и общекультурный уровень, добиваться нравственного и физического совершенствования своей личности.
- СЛК-3. Формировать и аргументировать собственные суждения и профессиональную позицию.
- СЛК-4. Анализировать и принимать решения по социальным, этическим, научным и техническим проблемам, возникающим в профессиональной деятельности.

Профессиональные:

- ПК-7. Работать с научно-технической информацией с использованием современных информационных технологий.
- ПК-8. Разрабатывать и совершенствовать радиофизические методы исследований.
- ПК-9. Осуществлять постановку и проведение теоретических и экспериментальных исследований
- ПК-10. Проводить математическое моделирование физических процессов и устройств.
- ПК-11. Разрабатывать численные алгоритмы и программы.
- ПК-12. Обосновывать достоверность полученных научных результатов.
- ПК-13. Формулировать выводы и рекомендации по применению результатов научно-исследовательской работы.

В результате изучения дисциплины магистрант должен:

знать:

- физические основы и особенности образования технических каналов утечки информации;
- основы контроля эффективности защиты информации от утечки по техническим каналам;

- методы и средства выявления угроз безопасности информации на объектах информатизации;

- методы и средства защиты информации от утечки по техническим каналам;

- порядок организации работ по технической защите конфиденциальной информации на объектах информатизации;

- требования и рекомендации по защите речевой конфиденциальной информации;

- требования и рекомендации по защите конфиденциальной информации, обрабатываемой в автоматизированных системах;

- методы и средства технической разведки;

- основные закономерности мешающего взаимодействия совместно работающих радиоэлектронных систем;

- принципы и методы анализа и обеспечения электромагнитной совместимости радиоэлектронных систем;

- нормативные документы для организации инженерно-технической защиты информации и обеспечения электромагнитной совместимости;

уметь:

- выявлять угрозы защищаемой информации;

- проводить анализ каналов несанкционированного получения информации и причин нарушения целостности информации;

- организовывать защиту информации на объектах её обработки;

- планировать, организовывать и контролировать выполнение мероприятий по технической защите конфиденциальной информации;

- оценивать эффективность защиты конфиденциальной информации;

- проводить анализ электромагнитной совместимости радиоэлектронных систем;

владеть:

- методами разработки и применения технических средств и систем защиты информации;

- методами обеспечения защищенности информации от утечек по техническим каналам;

- методами анализа электромагнитной совместимости радиоэлектронных систем;

- технологиями решения задач обеспечения электромагнитной совместимости.

Программа изучаемой дисциплины рассчитана на 206 часов, в том числе 54 аудиторных часа, из них: лекций - 18 часов, лабораторных работ – 36 часов.

Дисциплина изучается во II семестре I курса II ступени высшего образования (магистратура) студентами дневной (очной) формы получения образования. Текущая аттестация по дисциплине проводится в форме экзамена.

СОДЕРЖАНИЕ УЧЕБНОГО МАТЕРИАЛА

Тема 1. Основные понятия. Термины и определения.

Знакомство с изучаемой учебной дисциплиной. Цели и задачи. Тематический план.

Определение радиофизических методов:

- теоретические (аналитические, численные (вычислительные)) и экспериментальные методы исследований волновых и колебательных процессов;
- методы применения технологий, основанных на волновых и колебательных процессах различной природы: радио, акустическая и оптическая локация, радио, акустическая и оптическая связь (формирование каналов передачи данных), техническая защита информации (блокирование непреднамеренно возникающих акустических, электромагнитных и оптических технических каналов утечки информации).

Радиофизические методы в технической защите информации и электромагнитной совместимости.

Основные понятия в области технической защиты информации. Техническая защита информации как деятельность, и как одно из направлений науки – информатики. Определение защищаемых ресурсов: информация, программные средства, технические средства. Свойства информации. Уровни защиты информации. Объекты информатизации «средства вычислительной техники» (СВТ) и «защищаемое помещение» (ЗП). Техническая защита информации в общей системе мер защиты конфиденциальной информации, соотношения применяемых методов и средств.

Основные понятия в области электромагнитной совместимости (ЭМС). Определения понятий «электромагнитная совместимость», «техническое средство», «электромагнитная обстановка», «радио или электромагнитная помеха», «кондуктивная помеха», «помехоустойчивость», «рецепторы», «межсистемные и внутрисистемные помехи». Техническая защита информации и электромагнитная совместимость – области взаимных пересечений.

Тема 2. Технические каналы утечки информации (ТКУИ).

Определение ТКУИ. Модели ТКУИ. Классификация ТКУИ:

1.1 Акустические.

1.1.1 Звук.

1.1.2 Устройство микрофонов.

1.1.3 Направленные микрофоны.

1.2 Виброакустические.

1.2.1 Акселерометры.

1.2.2 Вибродатчик.

1.2.3 Стетоскопы.

1.2.4 Лазерная акустическая система разведки.

1.3 **Электрические** (электрические токи в проводах и электропроводящих строительных конструкциях).

1.3.1 Распределенные и сосредоточенные случайные антенны.
1.3.2 Акустоэлектрические преобразования.
1.3.3 Наводки на проводящих элементах.
1.3.4 Высокочастотное навязывание.
1.3.5 Токосъемники.
1.3.6 Пробники напряжения.
1.4 **Электромагнитные** (ПЭМИН), включающие модуляцию ВЧ-генераторов, и радиолокационные методы воздействия (эндовибраторы).
1.4.1 Антенны. Основные характеристики и типы.
1.5 **Оптические**.
1.5.1 Волоконно-оптические линии связи.
1.5.2 Утечка звуковой информации по оптическим каналам.
1.6 Материально-вещественные.
1.7 **Скрытые**.
1.8 **Искусственные**. Специальные технические средства (СТС).
1.8.1 Методы поиска закладных устройств.
1.8.2 Специальная техника поиска СТС.
1.8.3 СТС Агентства национальной безопасности США.

Тема 3. Объект информатизации – «защищаемое помещение». Оценка защищенности речевой информации от утечек по акустическим и виброакустическим каналам на объекте информатизации «защищаемое помещение».

Возможные технические каналы утечки информации на объекте информатизации «защищаемое помещение» (ЗП). Основные свойства речи. Критерий защищенности объекта информатизации ЗП – словесная разборчивость речи. Субъективный метод оценки разборчивости речи. Объективные методы оценки разборчивости речи. Метод Покровского Н.Б. Метод Железняка В.К. Тестовые (измерительные) сигналы оценки ТКУИ: шумовые, гармонические, сложные. Аппаратно-программные комплексы и системы оценки защищенности объекта информатизации ЗП. Аттестация объекта информатизации ЗП.

Тема 4. Методы защиты речевой информации от утечек по акустическим и виброакустическим каналам на объекте информатизации «защищаемое помещение»

Пассивные и активные методы защиты информации и их комбинация. Звукопоглощение. Индекс звукопоглощения. Звукоизоляция. Индекс изоляции воздушного шума. Способы повышения звукоизоляции строительных конструкций. Энтропия непрерывных сообщений. Шумы с максимальной энтропией. Энтропийная мощность реального шума. Коэффициент качества шума. Цвета шума. Оптимальный маскирующий шум для речевого сигнала.

Генераторы маскирующего шума для речи. Шумоочистка. Повышение разборчивости речи.

Тема 5. Объект информатизации – «средства вычислительной техники».

Структурная схема современного компьютера. Информативно опасные и неопасные интерфейсы. Принцип восьми разрядов. Возможные технические каналы утечки информации на объекте информатизации «средства вычислительной техники».

Аналоговый видеоинтерфейс VGA. Амплитудные и временные параметры сигналов VGA интерфейса. Спектральные характеристики сигналов VGA интерфейса. Оптимальный тестовый режим VGA интерфейса по критерию максимальной спектральной плотности мощности ПЭМИН.

Цифровой видеоинтерфейс DVI. Описание цифрового видеоинтерфейса DVI. Технология высокоскоростной передачи цифровых потоков TMDS. Варианты конструктивного исполнения интерфейса DVI-I(Single Link), DVI-I(Dual Link), DVI-D(Single Link), DVI-D(Dual Link), DVI-A. Алгоритм кодирования данных. Тестовый режим интерфейса DVI.

Интерфейс USB. Скоростные режимы. Формат пакета данных. Физический уровень. Кодирование данных. Тестовый режим интерфейса USB.

Последовательный интерфейс SATA (SATA2, SATA3). Система кодирования 8b/10b. Низковольтная дифференциальная передача сигналов LVDS. Спектральные характеристики сигнала интерфейса SATA.

Тема 6. Оценка защищенности информации от утечек по электрическому и электромагнитному каналам на объекте информатизации СВТ.

Критерий защищенности объекта информатизации СВТ от утечки информации по электрическому и электромагнитному техническим каналам – отношение энергии бита информации к спектральной плотности мощности шумов. Классификация электромагнитных помех. Естественные помехи: атмосферные, электростатические, шумы каналообразующей аппаратуры, искажения сигналов в среде распространения, космические (электромагнитные излучения Солнца). Рекомендация МСЭ-R P.372-9 Радиошум. Коэффициент (фактор) шума.

Радиусы контролируемых зон 1 (r1) и 2 (R2). Методы и средства расчета электромагнитной обстановки и распространения электромагнитного излучения. Методы и средства измерения распределения электромагнитных полей. Специальные исследования средств вычислительной техники. Тестовые сигналы. Оптимальный прием тестовых (измерительных) сигналов Аппаратно-программные комплексы и системы оценки защищенности объекта СВТ. Аттестация объекта информатизации СВТ.

Тема 7. Электромагнитная совместимость оборудования информационных технологий. Нормы и методы измерения побочных электромагнитных излучений и наводок (ПЭМИН).

Особенности изучения проблем ЭМС. Доступность для управления некоторых параметров источников и рецепторов помех.

Государственный стандарт Республики Беларусь СТБ EN 55022-2012 «Электромагнитная совместимость. Радиопомехи оборудования информационных

технологий. Нормы и методы измерений». Деление оборудования информационных технологий на классы А и В. Нормы радиопомех на сетевых зажимах и на телекоммуникационных портах связи. Пиковый, квазипиковый детектор. Детектор среднеквадратичных значений. Детектор средних значений. Нормы на излучаемые радиопомехи. Методика измерений затухания альтернативной измерительной площадки.

Тема 8. Характеристики помехоустойчивости оборудования информационных технологий. Нормы и методы измерений.

Государственный стандарт Республики Беларусь СТБ EN 55024-2006 «Электромагнитная совместимость. Оборудование информационных технологий. Характеристики помехоустойчивости. Нормы и методы измерений». Критерии качества функционирования А, В, С. Порты оборудования. Помехоустойчивость, порт корпуса. Помехоустойчивость, сигнальные и телекоммуникационные порты. Помехоустойчивость, входные порты электропитания постоянного и переменного тока. Методы испытаний. Частные условия для отдельных типов информационного оборудования.

Тема 9. Методы снижения ПЭМИН СВТ и защиты информации от утечек по электрическому и электромагнитному каналам.

Методы защиты информации на объекте информатизации «средства вычислительной техники». Пассивные методы. Активные методы. Комбинация пассивных и активных методов.

Методы повышения экранирующих свойств корпусов устройств, входящих в комплекс объекта СВТ. Использование радиопоглощающих материалов. Методы фильтрации. Схемно-конструктивные методы снижения побочных электромагнитных излучений и наводок объектов СВТ.

Генераторы маскирующего шума. Пространственное зашумление. Линейное зашумление. Применение специального параллельного кодирования. Криптографические методы маскировки информативно опасного сигнала.

УЧЕБНО-МЕТОДИЧЕСКАЯ КАРТА УЧЕБНОЙ ДИСЦИПЛИНЫ

Номер раздела, темы	Название раздела, темы	Количество аудиторных часов					Количество часов УСР	Материальное обеспечение занятия	Форма контроля знаний
		Лекции	Практические занятия	Семинарские занятия	Лабораторные занятия	Иное			
1	2	3	4	5	6	7	8	9	10
1.	Основные понятия. Термины и определения (2 ч.)	2							
2.	Технические каналы утечки информации (8 ч.)	2			6			Метод. указ. к лаб. раб.	Отчет. по лаб.раб.
3.	Объект информатизации – «защищаемое помещение» (ЗП). Оценка защищенности речевой информации от утечек по техническим каналам на объекте информатизации ЗП (8 ч.)	2			6			Метод. указ. к лаб. раб.	Отчет. по лаб.раб.
4.	Методы защиты речевой информации от утечек по акустическим и виброакустическим каналам на объекте информатизации ЗП (8 ч.)	2			6			Метод. указ. к лаб. раб.	Отчет. по лаб.раб.
5.	Объект информатизации – «средства вычислительной техники (СВТ)» (8 ч.)	2			6			Метод. указ. к лаб. раб.	Отчет. по лаб.раб.
6.	Оценка защищенности информации от утечек по электрическому и электромагнитному каналам на объекте информатизации СВТ (8 ч.)	2			6			Метод. указ. к лаб. раб.	Отчет. по лаб.раб.
7.	Электромагнитная совместимость оборудования информационных технологий. Нормы и методы	2			6			Метод. указ. к лаб. раб.	Отчет. по лаб.раб.

1	2	3	4	5	6	7	8	9	10
	измерения побочных электромагнитных излучений и наводок (ПЭМИН) (8 ч.)								
8.	Характеристики помехоустойчивости оборудования информационных технологий. Нормы и методы измерений (2 ч.)	2							
9.	Методы снижения ПЭМИН СВТ и защиты информации от утечек по электрическому и электромагнитному каналам (2 ч.)	2							

ИНФОРМАЦИОННО-МЕТОДИЧЕСКАЯ ЧАСТЬ
Список рекомендуемой литературы

Основная литература

1. Железняк В.К. Защита информации от утечки по техническим каналам: учеб. пособие / В.К Железняк; ГУАП .-СПб., 2006 .- 188с.
2. Технические средства и методы защиты информации: Учебник для вузов / Зайцев А.П., Шелупанов А.А., Мещеряков Р.В. и др.; под ред. А.П. Зайцева и А.А. Шелупанова. – М.: ООО «Издательство Машиностроение», 2009 – 508 с.
3. Бузов Г.А., Калини С.В., Кондратьев А.В. Защита от утечки информации по техническим каналам. Учебное пособие.-М.:Горячая линия – Телеком, 2005ю-2005.-416с.ил.
4. Виноградов Е. М. Анализ электромагнитной совместимости радиоэлектронных средств: Учеб. пособие. СПб.: Изд-во СПбГЭТУ «ЛЭТИ», 2009. 301 с.
5. СТБ EN 55022-2012 Электромагнитная совместимость. Радиопомехи от оборудования информационных технологий. Нормы и методы измерений
6. СТБ ЕН 55024-2006 Электромагнитная совместимость. Оборудование информационных технологий. Характеристики помехоустойчивости. Нормы и методы измерений.

Дополнительная литература

1. Е.Б. Белов, В.П. Лось и др. Основы информационной безопасности. Учебное пособие для вузов. М.: Горячая линия - Телеком, 2006, 544 с.
2. Малюк А.А. Информационная безопасность: концептуальные и методологические основы защиты информации. М.: Горячая линия-Телеком, 2004, 280.
3. В. А. Хорошко, А. А. Чекатков. Методы и средства защиты информации. М. Юниор, 203, 504с.
4. Герасименко В.А., Малюк А.А. Основы защиты информации. — М.: МГИФИ, 1997. —538 с.
5. Домарев В.В. Защита информации и безопасность компьютерных систем. — К.: Издательство ДиаСофт, 1999. — 480 с.
6. Тихонов В.И. Статистическая радиотехника = 2-е изд., перераб. и доп. – М.: Радио и связь, 1982 – 624с.
7. Денисенко А.Н. Сигналы. Теоретическая радиотехника. Справочное пособие. М.: Горячая линия .- Телеком .- 2005 .-704с.
8. Технический регламент таможенного союза. ТР ТС 020/2011. Электромагнитная совместимость технических средств.

Список компьютерных программ

1. Signal+3G. Программное обеспечение Signal+3G предназначено для работы с файлами и телеметрией шумомера – анализатора спектра - виброметра ОКТАВА-110А.

2. SignalVu-PC. Программное обеспечение SignalVu-PC позволяет на базе компьютера и USB приставки Tektronix RSA306B реализовывать функции анализатора спектра реального времени в диапазоне от 9 кГц до 6,3 ГГц.

3. MMANA – программа электродинамического моделирования тонкопроволочных антенн.

4. RInspectorRT. Программное обеспечение RadioInspector представляет собой набор приложений для поиска, мониторинга, контроля, анализа сигналов в радиочастотном спектре и локализации их источников. Может использоваться для обеспечения эффективного и высокоскоростного процесса инструментального контроля радиочастотного спектра, поиска источников радиосигналов, выполнения метрологически аттестованных измерений параметров излучений, выполнения ряда других прикладных задач радиоконтроля и радиомониторинга.

Примерный перечень лабораторных работ

1. Оценка защищенности объекта информатизации «защищаемое помещение».
2. Разработка системы защиты информации на объекте информатизации «защищаемое помещение».
3. Оценка защищенности объекта информатизации «средства вычислительной техники».
4. Электродинамическое моделирование электромагнитных излучений ПЭВМ на основе проволочной модели.
5. Проведение поисковых работ на базе аппаратно-программного комплекса радиомониторинга.
6. Исследования электромагнитной обстановки на объекте информатизации.

ДИАГНОСТИКА КОМПЕТЕНЦИЙ СТУДЕНТА

Учебным планом специальности в качестве формы текущей аттестации по учебной дисциплине «Радиофизические методы защиты информации и электромагнитная совместимость» предусмотрен экзамен по лекционному курсу и лабораторному практикуму. Оценка учебных достижений студента производится по десятибалльной шкале.

Для промежуточного контроля по учебной дисциплине и диагностики компетенций студентов используются следующие формы:

- тестирование;
- отчеты по лабораторным работам с их устной защитой.

МЕТОДИКА ФОРМИРОВАНИЯ ИТОГОВОЙ ОЦЕНКИ

Итоговая оценка по дисциплине формируется на основе экзаменационной оценки и оценки текущего контроля. Весовой коэффициент экзаменационной оценки - 0,6; весовой коэффициент текущей успеваемости - 0,4. Оценка текущего контроля формируется на основании оценок отчетов по лабораторному практикуму и результатов тестирования с равными весовыми коэффициентами.

Итоговая оценка формируется в соответствии со следующими документами:

1. «Об утверждении правил проведения аттестации студентов, курсантов, слушателей при освоении содержания образовательных программ высшего образования».Постановление Министерства образования Республики Беларусь от 29 мая 2012 г. № 53.
2. «Положение о рейтинговой системе оценки знаний по дисциплине в Белорусском государственном университете». Приказ ректора БГУ от 18.08.2015 № 382-ОД.
3. «Критерии оценки знаний и компетенций студентов по десятибалльной шкале».Письмо Министерства образования Республики Беларусь №09-10/53-ПО от 28.05.2013г.

ПРОТОКОЛ
СОГЛАСОВАНИЯ УЧЕБНОЙ ПРОГРАММЫ ПО ИЗУЧАЕМОЙ УЧЕБНОЙ ДИСЦИПЛИНЕ С ДРУГИМИ ДИСЦИПЛИНАМИ СПЕЦИАЛЬНОСТИ

Название дисциплины, с которой требуется согласование	Название кафедры	Предложения об изменениях в содержании учебной программы по изучаемой учебной дисциплине	Решение, принятое кафедрой, разработавшей учебную программу (с указанием даты и номера протокола)
Теоретические основы информационной безопасности	Телекоммуникаций и информационных технологий	Предложений об изменениях в содержании учебной программы нет	Изменения не требуются, протокол №14 от 19.06.2018.
Программно-аппаратные средства обеспечения информационной безопасности	Телекоммуникаций и информационных технологий	Предложений об изменениях в содержании учебной программы нет	Изменения не требуются, протокол №14 от 19.06.2018.

ДОПОЛНЕНИЯ И ИЗМЕНЕНИЯ
К УЧЕБНОЙ ПРОГРАММЕ ПО ИЗУЧАЕМОЙ УЧЕБНОЙ ДИСЦИПЛИНЕ НА _____ / _____ УЧЕБНЫЙ ГОД

№ п/п	Дополнения и изменения	Основание

Учебная программа пересмотрена и одобрена на заседании кафедры радиофизики и цифровых медиа технологий
(протокол № ____ от _____ 20___ г.)

Заведующий кафедрой радиофизики и
цифровых медиа технологий
к.ф.-м.н., доцент И.Э.Хейдоров

УТВЕРЖДАЮ
Декан факультета радиофизики и
компьютерных технологий
к.ф.-м.н., доцент С.В.Малый