

МИНОБРНАУКИ РОССИИ  
ФГБОУ ВО «БАШКИРСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ»

ФИЗИКО - ТЕХНИЧЕСКИЙ ИНСТИТУТ

Актуализировано:  
на заседании кафедры общей физики  
протокол № 8 от «16» июня 2017 г.

Согласовано:  
Председатель УМК ФТИ

Зав. кафедрой



/Балапанов М.Х.



/Балапанов М.Х.

**РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ (МОДУЛЯ)**

дисциплина Средства и методы защиты информации

\_\_\_\_\_ вариативная \_\_\_\_\_

**программа бакалавриата**

Направление подготовки (специальность)

**03.03.02 Физика**

Направленность (профиль) подготовки

**Медицинская физика**

Квалификация

**бакалавр**

Разработчик (составитель)

доцент, к.ф.-м.н., доцент

(должность, ученая степень, ученое звание)



/\_Акманова Г.Р.

(подпись, Фамилия И.О.)

Для приема: 2016 г.

Уфа 2017 г.

Составитель:  
Акманова Г.Р.

Рабочая программа дисциплины актуализирована на заседании кафедры общей физики протокол от «16» июня 2017 г. № 8.

Дополнения и изменения, внесенные в рабочую программу дисциплины, утверждены на заседании кафедры, протокол № 6 от « 6 » июня 2018 г.: обновлены программное обеспечение и база данных.

Заведующий кафедрой

 / Балапанов М.Х.

### Список документов и материалов (оглавление)

1. Перечень планируемых результатов обучения по дисциплине, соотнесенных с планируемыми результатами освоения образовательной программы	4
2. Цель и место дисциплины в структуре образовательной программы	5
3. Содержание рабочей программы (объем дисциплины, типы и виды учебных занятий, учебно-методическое обеспечение самостоятельной работы обучающихся) - (Приложение №1)	5 (17)
4. Фонд оценочных средств по дисциплине	6
4.1. Перечень компетенций с указанием этапов их формирования в процессе освоения образовательной программы. Описание показателей и критериев оценивания компетенций на различных этапах их формирования, описание шкал оценивания	6
4.2. Типовые контрольные задания или иные материалы, необходимые для оценки знаний, умений, навыков и опыта деятельности, характеризующих этапы формирования компетенций в процессе освоения образовательной программы. Методические материалы, определяющие процедуры оценивания знаний, умений, навыков и опыта деятельности, характеризующих этапы формирования компетенций	8
4.3. Рейтинг-план дисциплины (Приложение №2)	8(20)
5. Учебно-методическое и информационное обеспечение дисциплины	15
5.1. Перечень основной и дополнительной учебной литературы, необходимой для освоения дисциплины	15
5.2. Перечень ресурсов информационно-телекоммуникационной сети «Интернет» и программного обеспечения, необходимых для освоения дисциплины	15
6. Материально-техническая база, необходимая для осуществления образовательного процесса по дисциплине	16

## 1. Перечень планируемых результатов обучения по дисциплине, соотнесенных с планируемыми результатами освоения образовательной программы

При изучении дисциплины «Средства и методы защиты информации» у обучающегося должны формироваться следующие компетенции:

ОПК-4: способностью понимать сущность и значение информации в развитии современного общества, осознавать опасность и угрозу, возникающие в этом процессе, соблюдать основные требования информационной безопасности;

ОПК-5: способностью использовать основные методы, способы и средства получения, хранения, переработки информации и навыки работы с компьютером как со средством управления информацией;

ПК-5: способностью пользоваться современными методами обработки, анализа и синтеза физической информации в избранной области физических исследований;

Для формирования указанных компетенций и освоения образовательной программы обучающийся должен показать следующие результаты обучения по дисциплине:

Результаты обучения		Формируемая компетенция (с указанием кода)	Примечание
Знания	1. Знать основные средства и методы защиты информации.	ОПК-4	
	2. Знать основные методы, способы и средства получения, хранения, переработки информации.	ОПК-5	
	3. Знать современные методы обработки, анализа и синтеза физической информации	ПК-5	
Умения	1. Уметь применять требования информационной безопасности для решения физических задач.	ОПК-4	
	2. Уметь применять на практике методы, способы и средства получения, хранения, переработки информации.	ОПК-5	
	3. Уметь пользоваться современными методами обработки, анализа и синтеза физической информации	ПК-5	
Владения (навыки / опыт деятельности)	1. Владеть основными методами, способами и средствами получения, хранения, переработки информации.	ОПК-5	
	2. Владеть навыками пользования современными методами обработки, анализа и синтеза физической информации	ПК-5	

## **2. Цель и место дисциплины в структуре образовательной программы**

Дисциплина «Средства и методы защиты информации» относится к *вариативной* части рабочего учебного плана.

Дисциплина изучается на 4 курсе в 7 семестре.

Цели изучения дисциплины «Средства и методы защиты информации»:

Целью учебной дисциплины «Средства и методы защиты информации» на 4 курсе в 7 семестре является формирование системы знаний в области информационной безопасности и применения на практике методов и средств защиты информации.

Задачами изучения дисциплины являются:

формирование умения обеспечить защиту информации и объектов информатизации; формирование умения составлять заявительную документацию в надзорные государственные органы инфокоммуникационной отрасли; формирование навыков выполнения работ в области технического регулирования, сертификации технических средств, систем, процессов, оборудования и материалов; формирование навыков обеспечения защиты объектов интеллектуальной собственности и результатов исследований и разработок как коммерческой тайны предприятия; настройка и обслуживание аппаратно-программных средств.

Для изучения дисциплины «Средства и методы защиты информации» необходимо знание следующих разделов курсов общей физики: механики, молекулярной физики, электричество и магнетизма, оптики, атомной физики. Студенты должны владеть основными законами и понятиями этих разделов, а также обладать знаниями в области информатики и программирования.

Освоение этой дисциплины необходимо для дальнейшего изучения специальных дисциплин профиля «Медицинской физики» («Физические основы томографии», «Радиационная физика», «Основы интроскопии», «Медицинские приборы, аппараты, системы», «Физические основы использования лазеров и оптических источников света в медицине», «Ультразвук в медицине»).

## **3. Содержание рабочей программы (объем дисциплины, типы и виды учебных занятий, учебно-методическое обеспечение самостоятельной работы обучающихся)**

Содержание рабочей программы представлено в Приложении № 1.

#### 4. Фонд оценочных средств по дисциплине

##### 4.1. Перечень компетенций с указанием этапов их формирования в процессе освоения образовательной программы. Описание показателей и критериев оценивания компетенций на различных этапах их формирования, описание шкал оценивания

Код и формулировка компетенции

**ОПК-4:** способностью понимать сущность и значение информации в развитии современного общества, осознавать опасность и угрозу, возникающие в этом процессе, соблюдать основные требования информационной безопасности;

Этап (уровень) освоения компетенции	Планируемые результаты обучения (показатели достижения заданного уровня освоения компетенций)	Критерии оценивания результатов обучения	
		«Зачтено»	«Не зачтено»
Первый этап	Знать: 1) основные средства и методы защиты информации.	Знает основные средства и методы защиты информации;	Не знает основные средства и методы защиты информации;
Второй этап	Уметь: 1) применять требования информационной безопасности для решения физических задач;	Умеет применять требования информационной безопасности для решения физических задач;	Не умеет применять требования информационной безопасности для решения физических задач;

**ОПК-5:** способностью использовать основные методы, способы и средства получения, хранения, переработки информации и навыки работы с компьютером как со средством управления информацией;

Этап (уровень) освоения компетенции	Планируемые результаты обучения (показатели достижения заданного уровня освоения компетенций)	Критерии оценивания результатов обучения	
		«Зачтено»	«Не зачтено»
Первый этап	Знать: 2) основные методы, способы и средства получения, хранения, переработки информации;	Знает основные методы, способы и средства получения, хранения, переработки информации;	Не знает основные методы, способы и средства получения, хранения, переработки информации;
Второй этап	Уметь: 2) применять на практике методы, способы и средства получения, хранения, переработки информации;	Умеет применять на практике методы, способы и средства получения, хранения, переработки информации;	Не умеет применять на практике методы, способы и средства получения, хранения, переработки информации;
Третий этап	Владеть: 1) основными методами, способами и средствами получения, хранения, переработки информации;	Владеет основными методами, способами и средствами получения, хранения, переработки информации;	Не владеет основными методами, способами и средствами получения, хранения, переработки информации;

**ПК-5:** способностью пользоваться современными методами обработки, анализа и синтеза физической информации в избранной области физических исследований;

Этап (уровень) освоения компетенции	Планируемые результаты обучения (показатели достижения заданного уровня освоения компетенций)	Критерии оценивания результатов обучения	
		«Зачтено»	«Не зачтено»
Первый этап	Знать: 3) современные методы обработки, анализа и синтеза физической информации;	Знает основные положения в современных методах обработки, анализа и синтеза физической информации;	Не знает современные методы обработки, анализа и синтеза физической информации;

	информации.	синтеза физической информации.	информации.
Второй этап	Уметь: 3) пользоваться современными методами обработки, анализа и синтеза физической информации.	Умеет пользоваться современными методами обработки, анализа и синтеза физической информации.	Не умеет пользоваться современными методами обработки, анализа и синтеза физической информации.
Третий этап	Владеть: 2) навыками пользования современными методами обработки, анализа и синтеза физической информации.	Владеет навыками пользования современными методами обработки, анализа и синтеза физической информации.	Не владеет навыками пользования современными методами обработки, анализа и синтеза физической информации.

Критериями оценивания являются баллы, которые выставляются преподавателем за виды деятельности (оценочные средства) по итогам изучения модулей (разделов дисциплины), перечисленных в рейтинг-плане дисциплины.

**4.2. Типовые контрольные задания или иные материалы, необходимые для оценки знаний, умений, навыков и опыта деятельности, характеризующих этапы формирования компетенций в процессе освоения образовательной программы. Методические материалы, определяющие процедуры оценивания знаний, умений, навыков и опыта деятельности, характеризующих этапы формирования компетенций**

Этапы освоения	Результаты обучения	Компетенция	Оценочные средства
1-й этап Знания	1. Знать основные средства и методы защиты информации.	ОПК-4	Письменная работа
	2. Знать основные методы, способы и средства получения, хранения, переработки информации.	ОПК-5	Защита лабораторных работ
	3. Знать современные методы обработки, анализа и синтеза физической информации	ПК-5	Защита лабораторных работ
2-й этап Умения	1. Уметь применять требования информационной безопасности для решения физических задач.	ОПК-4	Тест Письменная работа
	2. Уметь применять на практике методы, способы и средства получения, хранения, переработки информации.	ОПК-5	Письменная работа
	3. Уметь пользоваться современными методами обработки, анализа и синтеза физической информации	ПК-5	Письменная работа
3-й этап Владеть навыками	1. Владеть основными методами, способами и средствами получения, хранения, переработки информации.	ОПК-5	Защита лабораторных работ
	2. Владеть навыками пользования современными методами обработки, анализа и синтеза физической информации	ПК-5	Защита лабораторных работ

### 4.3 Рейтинг-план дисциплины

Рейтинг-план дисциплины представлен в Приложении № 2.

#### Вопросы для подготовки к зачету

1. Биологические системы в электромагнитном поле
1. Шкала электромагнитных волн
2. Указать свойства электромагнитных волн
3. Искусственные и природные источники НИИ
4. Критерий деления видов излучения на ионизирующее и неионизирующее.
2. Электромагнитное излучение человека
5. Потенциалы покоя и действия.
6. Природа возникновения токов в клетках сердца
7. Автоволновые процессы в сердце.

8. Векторный характер токов в клетках сердца, регистрация ЭКГ.
9. Биопотенциалы головного мозга.
10. Структуры мозга, генерирующие электрические токи. Электроэнцефалография.
11. Объяснить механизм ритмических осцилляций мембранных потенциалов нейронов.
12. Основные ритмы ЭЭГ и их частотные диапазоны
3. Взаимодействие тканей с акустическими волнами
13. Особенности распространения акустических волн в тканях
14. Физические свойства ультразвуковых волн
15. Акустическая кавитация
16. Источники и приемники УЗ волн.
17. Биологическое действие УЗ на организм человека
18. Применение УЗ в терапии и диагностике
4. Биологическое действие электромагнитных полей
19. Параметры ЭМП, влияющие на биологическую реакцию
20. Прямое воздействие электромагнитных на человека
21. Механизмы косвенного воздействия ЭМП на человека
22. Влияние радиочастотных, и сверхвысокочастотных полей, полей крайне низкой частоты на живые организмы.
23. Действие постоянных и импульсных магнитных полей на биообъекты.
24. Влияние КВЧ излучения на биологические объекты.
25. Механизм действия низкоинтенсивных миллиметровых волн на организм человека
5. Основы фотоники биологических объектов
26. Основные количественные показатели, характеризующие поглощение
27. Поглощение света и пути дезактивации поглощенной энергии
28. Излучение света возбужденными молекулами: фотолюминесценция, хемилюминесценция и фосфоресценция
29. Основные параметры люминесценции
30. Спектры поглощения и люминесценции компонентов нуклеиновых кислот
31. Информация, получаемая из спектров поглощения и люминесценции
32. Искажение спектров в биологических объектах
6. Фотолюминесценция биологических систем
33. Лазерный люминесцентный анализ биомакромолекул, клеток и тканей.
34. Автофлуоресценция
35. Спектральные свойства эндогенных и экзогенных флуорофоров  
Методы и средства лазерной флуоресцентной диагностики
36. Примеры биомедицинских приложений
7. ИК-излучение
37. Источники и приемники ИК излучения
38. Поглощение инфракрасного излучения молекулами, комбинационное рассеяние света
39. Применение ИК и рамановской спектроскопии в клинической диагностике
40. Тепловидение
8. Действие УФ-излучения на биологические структуры.
41. Фотоинактивация биологически важных молекул под действием УФ облучения
42. Действие УФ на рибозу и дезоксирибозу
43. Действие УФ на пуриновые основания
44. Гидратация пиримидиновых оснований
45. Влияние УФ облучения на молекулярную массу ДНК (разрыв цепи, образование сшивок ДНК-ДНК и ДНК-белок)
46. Воздействие УФ-излучения на кожные покровы. Эритема.

47. Пигментация кожи. Канцерогенез.
48. Биологическое значение повреждений белков и нуклеиновых кислот

Шкалы оценивания:

зачтено – от 60 до 110 рейтинговых баллов (включая 10 поощрительных баллов), не зачтено – от 0 до 59 рейтинговых баллов).

## **Задания для контрольной работы**

### Описание контрольной работы

Максимальный балл – 10 баллов.

### Пример контрольной работы

1. Начиная с какого класса защищенности СВТ требуется руководство пользователя
2. Начиная с какого класса требований ГТК РФ к защите информации в автоматизированных многопользовательских системах с различным доступом требуется интерактивное оповещение администраторов системы о попытках несанкционированного доступа
3. Начиная с какого класса защищенности СВТ требуется взаимодействие пользователя с комплексом средств защиты
4. Начиная с какого класса требований ГТК РФ к защите информации в автоматизированных многопользовательских системах с различным доступом требуется учет и регистрация изменений полномочий субъектов доступа
5. Начиная с какого класса требований ГТК РФ к защите информации в автоматизированных многопользовательских системах с одинаковыми полномочиями доступа требуется очистка освобождаемых областей оперативной памяти
6. Начиная с какого класса защищенности СВТ требуется мандатный принцип контроля доступа
7. Начиная с какого класса требований ГТК РФ к защите информации в автоматизированных многопользовательских системах с различным доступом требуется шифрование конфиденциальной информации
8. Начиная с какого класса требований ГТК РФ к защите информации в автоматизированных многопользовательских системах с одинаковым доступом требуется наличие администратора (службы) защиты информации в АС
9. Начиная с какого класса защищенности СВТ требуется регистрация
10. Начиная с какого класса требований ГТК РФ к защите информации в автоматизированных многопользовательских системах с различным доступом требуется использование сертифицированных криптографических средств

### **Описание методики оценивания вопросов контрольной работы:**

- 10 баллов выставляется студенту, если представлен полный ответ;  
- 8-9 баллов выставляется студенту, если при верном ответе, но допущены недочеты;  
- 5-7 баллов выставляется студенту, если дан неполный ответ;  
- 1-4 баллов выставляется студенту, если дан частичный ответ;  
- 0 баллов ставится при отсутствии ответа или при полностью неверном ответе.

### **Задания для проведения письменных опросов (тестов)**

#### Описание теста.

Содержит задания для рубежного контроля усвоения материала. Тест рассчитан на 45 минут, состоит из 10 заданий. Каждое задание оценивается в 1 балл.

#### Пример варианта теста

##### Вариант 1.

1. Угроза нарушения конфиденциальности вычислительной системы (ВС) означает:
  - 1) Искажение информации, хранящейся в компьютерной системе или передаваемой по каналу связи.
  - 2) Разглашение секретной информации.

- 3) Создание таких ситуаций, когда определенные преднамеренные действия либо снижают работоспособность ВС, либо блокируют доступ к некоторым ее ресурсам.
- 4) Информация становится известной лицам, которые не должны иметь к ней доступ.

2. Угроза нарушения целостности информации означает:

- 1) Искажение информации, хранящейся в компьютерной системе или передаваемой по каналу связи.
- 2) Разглашение секретной информации.
- 3) Санкционированное изменение информации, которое выполняется полномочными лицами.
- 4) Создание таких ситуаций, когда определенные преднамеренные действия либо снижают работоспособность ВС, либо блокируют доступ к некоторым ее ресурсам.

3. Угроза нарушения работоспособности вычислительной системы (ВС) означает:

- 1) Разглашение конфиденциальной или секретной информации.
- 2) Искажение информации, хранящейся в компьютерной системе или передаваемой по каналу связи.
- 3) Блокирование доступа к ресурсу.
- 4) Создание таких ситуаций, когда определенные преднамеренные действия либо снижают работоспособность ВС, либо блокируют доступ к некоторым ее ресурсам.

4. «Компьютерный вирус» - это программа, которая :

- 1) Может заражать другие программы, модифицируя их посредством включения в них своей, возможно, измененной копии, причем последняя сохраняет способность к дальнейшему размножению.
- 2) Осуществляет перехват паролей.
- 3) Наряду с действиями, описанными в ее документации, выполняет некоторые другие действия, ведущие к нарушению безопасности системы и деструктивным результатам
- 4) выполняет какие-либо действия одним пользователем от имени другого пользователя, обладающего соответствующими полномочиями.

5. Причинами случайных разрушающих воздействий при работы ВС могут быть:

- 1) Ошибки в работе ВС.
- 2) Отказы и сбой аппаратуры.
- 3) Помехи в линиях связи из-за воздействия внешней среды.
- 4) Результат работы компьютерного вируса или троянской программы.

6. Угрозами безопасности вычислительной системы (ВС) являются:

- 1) Вмешательство человека в работу ВС.
- 2) Аппаратно-техническое вмешательство в работу ВС.
- 3) Администрирование ВС со стороны администратора.
- 4) Разрушающее воздействие на программные компоненты ВС с помощью программных средств.

7. Атака на компьютерную систему:

- 1) Действие, предпринимаемое злоумышленником, которое заключается в поиске и использовании той или иной уязвимости системы.
- 2) Оценка производительности системы.
- 3) Реализация угрозы безопасности.
- 4) Тестирование ВС.

8. К разрушающим программным средствам относятся:

- 1) Анализаторы протоколов.
- 2) Компьютерные вирусы.
- 3) Серверы приложений.
- 4) Троянские программы.

9. «Троянский конь» - это программа, которая:

- 1) Может заражать другие программы, модифицируя их посредством включения в них своей, возможно, измененной копии, причем последняя сохраняет способность к дальнейшему размножению.
- 2) Осуществляет перехват паролей.
- 3) Наряду с действиями, описанными в ее документации, выполняет некоторые другие действия, ведущие к нарушению безопасности системы и деструктивным результатам.
- 4) Выполняет какие-либо действия одним пользователем от имени другого пользователя, обладающего соответствующими полномочиями.

10. «Маскарад» - это программа, которая:

- 1) Может заражать другие программы, модифицируя их посредством включения в них своей, возможно, измененной копии, причем последняя сохраняет способность к дальнейшему размножению;
- 2) Осуществляет перехват паролей.
- 3) Наряду с действиями, описанными в ее документации, выполняет некоторые другие действия, ведущие к нарушению безопасности системы и деструктивным результатам.
- 4) Выполняет какие-либо действия одним пользователем от имени другого пользователя, обладающего соответствующими полномочиями.

11. Комплексный подход» в обеспечению безопасности ВС:

- 1) Ориентирован на создание защищенной среды обработки информации в ВС, объединяющий в единый комплекс разнородные меры противодействия угрозам.
- 2) Направлен на противодействие четко определенным угрозам в заданных условиях.
- 3) Не создает единую защищенную среду обработки информации.
- 4) Гарантирует определенный уровень безопасности ВС в целом.

12. Политика безопасности может быть:

- 1) Манчестерской.
- 2) Дискреционной.
- 3) Мандатной.
- 4) Паспортной.

13. В материалах Гостехкомиссия (ГТК) при Президенте Российской Федерации (РФ) основное внимание уделяется вопросам:

- 1) Обеспечения целостности
- 2) Обеспечения конфиденциальности
- 3) Обеспечения работоспособности
- 4) Обеспечения аутентификации

#### **Описание методики оценивания тестов:**

- 1 балл выставляется студенту, если студент полностью дал ответ на вопрос;
- 0 баллов ставится при неверном ответе.

#### **Задания для оценивания выполнения и защиты лабораторных работ**

За допуск, выполнение лабораторной работы, оформление отчета студент может получить 2 балла. За защиту отчетов по лабораторной работе студент может получить до 5 баллов. Максимальный балл за выполнение и защиту лабораторной работы 7 баллов.

### **Контрольные вопросы к защите лабораторной работы №1 «Современные симметричные криптосистемы»**

1. Каков размер блока и ключа в алгоритме DES?
2. Каков размер блока и ключа в алгоритме DES?
3. Что такое двукратный DES? Какая атака делает двукратный DES бесполезным?
4. Почему режим OFB (Output Feed Back – Обратная связь по выходу) алгоритма DES применяют для шифрования в спутниковых системах связи?
5. Каков размер блока и ключа в алгоритме ГОСТ 28147-89?
6. Каков размер циклового ключа в алгоритме ГОСТ 28147-89?
7. Какой режим работы алгоритма ГОСТ 28147-89 можно использовать при формировании ЭЦП?
8. Перечислите параметры (размер блока, размер ключа и число раундов) для трех версий AES?
9. Сколько преобразований имеется в каждой версии AES? Сколько ключей необходимо для каждой версии?

#### **Описание методики оценивания выполнения и защиты лабораторных работ:**

- 7 баллов получает студент, если им сдан допуск к лабораторной работе, полностью выполнена лабораторная работа и полностью оформлен отчет; полностью ответил на заданные вопросы;
- 5-6 баллов получает студент, если им сдан допуск к лабораторной работе, полностью выполнена лабораторная работа и полностью оформлен отчет, ответил на вопросы; но допущены недочеты;
- 3-4 балла получает студент, если им сдан допуск к лабораторной работе, полностью выполнена лабораторная работа и полностью оформлен отчет; но частично ответил на заданные вопросы;
- 1-2 балла получает студент, если при сдаче допуска к лабораторным работам, выполнения лабораторной работы и оформлении отчета допущены недочеты;
- 0 баллов ставится при невыполнении лабораторной работы.

**5. Учебно-методическое и информационное обеспечение дисциплины**  
**5.1. Перечень основной и дополнительной учебной литературы, необходимой для освоения дисциплины**

**Основная литература:**

1. Бирюков, А.А. Информационная безопасность: защита и нападение. - М.: ДМК Пресс, 2012, 474 с. [Электронный ресурс]: [http://e.lanbook.com/books/element.php?pl1\\_id=39990](http://e.lanbook.com/books/element.php?pl1_id=39990)
2. Петров, А.А. Компьютерная безопасность. Криптографические методы защиты. - М. : ДМК Пресс, 2008, 451 с. [Электронный ресурс]: [http://e.lanbook.com/books/element.php?pl1\\_id=3027](http://e.lanbook.com/books/element.php?pl1_id=3027)
3. Шаньгин, В.Ф. Информационная безопасность. - М.: ДМК Пресс, 2014, 702 с. [Электронный ресурс]: [http://e.lanbook.com/books/element.php?pl1\\_id=50578](http://e.lanbook.com/books/element.php?pl1_id=50578).

**Дополнительная литература:**

1. Беломойцев, Д.Е., Волосатова Т.М., Родионов С.В. Основные методы криптографической: / Д.Е. Беломойцев, Т.М. Волосатова, С.В. Родионов. - М. : МГТУ им. Н.Э. Баумана, 2014, 80 с. [Электронный ресурс]: [http://e.lanbook.com/books/element.php?pl1\\_id=58438](http://e.lanbook.com/books/element.php?pl1_id=58438).

**5.2. Перечень ресурсов информационно-телекоммуникационной сети «Интернет» и программного обеспечения, необходимых для освоения дисциплины**

1. Электронная библиотечная система. ЭБ БашГУ. - Собственная электронная библиотека учебных и научных электронных изданий, которая включает издания преподавателей БашГУ. Авторизованный доступ по паролю из любой точки сети Интернет. Регистрация в Библиотеке БашГУ, дальнейший доступ из любой точки сети Интернет. - <https://elib.bashedu.ru/>
2. Электронная библиотечная система. Университетская библиотека онлайн. Полнотекстовая БД учебных и научных электронных изданий. Авторизованный доступ по паролю из любой точки сети Интернет. Регистрация в Библиотеке БашГУ, дальнейший доступ из любой точки сети Интернет. - <https://biblioclub.ru/>
3. Электронная библиотечная система издательства. Лань. - Полнотекстовая БД учебных и научных электронных изданий. Авторизованный доступ по паролю из любой точки сети Интернет. Регистрация в Библиотеке БашГУ, дальнейший доступ из любой точки сети Интернет. = <https://e.lanbook.com/>
4. Электронный каталог Библиотеки БашГУ - Справочно-поисковый аппарат библиотеки. Включает в себя систему каталогов и картотек, справочно-библиографический фонд. - <http://www.bashlib.ru/catalogi/>

## 6. Материально-техническая база, необходимая для осуществления образовательного процесса по дисциплине

Материально-техническая база, необходимая для осуществления образовательного процесса по дисциплине приведена в таблице:

Наименование специализированных аудиторий, кабинетов, лабораторий	Вид занятий	Наименование оборудования, программного обеспечения
<b>1</b>	<b>2</b>	<b>3</b>
Учебная аудитория для проведения занятий: аудитории № 322 или № 324 или № 318 или № 216 (физмат корпус)	Лекции	Доска, компьютер, мультимедийный проектор, экран
Учебная лаборатория для проведения лабораторных занятий: аудитории № 412	Лабораторные занятия	Учебная мебель, доска, компьютеры в сборе DELL E2214Нв-15 шт.
Читальный зал №1 (главный корпус, 1 этаж)	Самостоятельная работа	Научный и учебный фонд, научная периодика, ПК (моноблок) - 3 шт, Wi-Fi доступ для мобильных устройств, неограниченный доступ к ЭБС и БД; количество посадочных мест – 76.
Читальный зал №2 (корпус физмата, 2 этаж)	Самостоятельная работа	Научный и учебный фонд, научная периодика, Wi-Fi доступ для мобильных устройств, неограниченный доступ к ЭБС и БД; количество посадочных мест – 50.

МИНОБРНАУКИ РОССИИ  
ФГБОУ ВО «БАШКИРСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ»  
ФИЗИКО - ТЕХНИЧЕСКИЙ ИНСТИТУТ

**СОДЕРЖАНИЕ РАБОЧЕЙ ПРОГРАММЫ**

дисциплины «Средства и методы защиты информации» на 7 семестр  
(наименование дисциплины)

очная

форма обучения

<b>Вид работы</b>	<b>Объем дисциплины</b>
Общая трудоемкость дисциплины (ЗЕТ / часов)	3/108
Учебных часов на контактную работу с преподавателем:	36,2
лекций	18
лабораторных	18
других (групповая, индивидуальная консультация и иные виды учебной деятельности, предусматривающие работу обучающихся с преподавателем) (ФКР)	0,2
Учебных часов на самостоятельную работу обучающихся (СР)	71,8
Учебных часов на подготовку к экзамену/зачету/дифференцированному зачету (Контроль)	

Форма контроля:  
зачет 7 семестр

№ п.п.	Тема и содержание	Форма изучения материалов:				Основная и дополнительная литература, рекомендуемая студентам (номера из списка)	Задания по самостоятельной работе студентов (СРС)	Форма текущего контроля успеваемости
		лекции, занятия, семинарские занятия, лабораторные работы, самостоятельная работа и трудоемкость (в часах)	ЛК	ПР/СЕМ	ЛР			
1	2	3	4	5	6	7	8	9
<b>Модуль 1.</b>								
1	Источники, риски и формы атак на компьютерные системы.	3		3	12	1-3	Подготовка к защите лабораторных работ	Лабораторная работа Контрольная работа Тест
2	Модели безопасности информационных систем	3		3	12	1-3	Подготовка к защите лабораторных работ	Лабораторная работа Контрольная работа Тест
3	Стандарты безопасности. Законодательные меры защиты информации	3		3	12	1-3	Подготовка к защите лабораторных работ	Лабораторная работа Контрольная работа Тест
<b>Модуль 2.</b>								
4	Криптографические модели и методы защиты информации	3		3	12	1-3	Подготовка к защите лабораторных работ	Лабораторная работа Контрольная работа Тест

5	Защита информации в современных операционных системах			3	12	1-3	Подготовка к защите лабораторных работ	Лабораторная работа Контрольная работа Тест
6	Защита информации в сети	3		3	11,8	1-3	Подготовка к защите лабораторных работ	Лабораторная работа Контрольная работа Тест
<b>Всего часов:</b>		<b>18</b>		<b>44</b>	<b>71,8</b>			

**Примечание 1.** В таблицу не включено 0.2 часа ФКР (групповая, индивидуальная консультация и иные виды учебной деятельности во время семестра, подразумевающие контактную работу обучающихся с преподавателем) .

## Рейтинг – план дисциплины

«Средства и методы защиты информации»

(название дисциплины согласно рабочему учебному плану)

направление «Физика»,  
 профиль «Медицинская физика»  
 курс 4, семестр 7

Виды учебной деятельности студентов	Балл за конкретное задание	Число заданий за семестр	Баллы	
			Минимальный	Максимальный
<b>Модуль I</b>				
<b>Текущий контроль</b>				
1. Контрольная работа	0-15	1	0	15
2. Допуск, выполнение лабораторной работы, оформление отчета	0-2	5	0	10
<b>Рубежный контроль</b>				
1. Защита отчетов по лабораторной работе	0-5	5	0	25
<b>Всего баллов за модуль:</b>			<b>0</b>	<b>50</b>
<b>Модуль II</b>				
<b>Текущий контроль</b>				
1. Тестирование	0-15	1	0	15
2. Допуск, выполнение лабораторной работы, оформление отчета	0-2	5	0	10
<b>Рубежный контроль</b>				
1. Защита отчетов по лабораторной работе	0-5	5	0	25
<b>Всего баллов за модуль:</b>			<b>0</b>	<b>50</b>
<b>Поощрительные баллы</b>				
1. Студенческие олимпиады			0	10
<b>Посещаемость (баллы вычитаются из общей суммы набранных баллов)</b>				
1. Посещаемость лекционных занятий			0	-6
2. Посещение практических занятий			0	-10
<b>Итоговый контроль</b>				
Зачет				