МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ РОССИИ
ФГБОУ ВО «БАШКИРСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ»

ФИЗИКО - ТЕХНИЧЕСКИЙ ИНСТИТУТ

Утверждено:
на заседании кафедры общей физики
протокол № 3 от 19 января 2021 г.

Зав. кафедрой  /Балапанов М.Х.

Согласовано:
Председатель УМК ФТИ

 /Балапанов М.Х.

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ

Средства и методы защиты информации

Б1.В.ДВ.05.02, часть, формируемая

участниками образовательных отношений

Программа бакалавриата

Направление подготовки
03.03.02 Физика

Направленность (профиль) подготовки
Медицинская физика

Квалификация

Бакалавр

Форма обучения
очная

Разработчик (составитель) доцент, к.ф.-м.н., доцент	 /Акманова Г.Р.

Для приема: 2021 г.

Уфа 2021 г.

Составитель:

к.ф.-м.н., доцент Акманова Г.Р.

Рабочая программа дисциплины утверждена на заседании кафедры общей физики протокол № 3 от 19 января 2021 г.

Заведующий кафедрой  /Балапанов М.Х.

Дополнения и изменения, внесенные в рабочую программу дисциплины, утверждены на заседании кафедры общей физики протокол № 6 от 24 июня 2021 г.

Заведующий кафедрой  /Балапанов М.Х.

Список документов и материалов (оглавление)

1. Перечень планируемых результатов обучения по дисциплине, соотнесенных с установленными в образовательной программе индикаторами достижения компетенций

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

ПК-4: способен осуществлять технический контроль, настройку и эксплуатацию лечебного, диагностического и экспериментального оборудования, устройств медицинской электроники.

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

Категория (группа) компетенций[1] (при наличии ОПК)	**Формируемая компетенция (с указанием кода)**	**Код и наименование индикатора достижения компетенции**	**Результаты обучения по дисциплине**
	ПК-4: способен осуществлять технический контроль, настройку и эксплуатацию лечебного, диагностического и экспериментального оборудования, устройств медицинской электроники;	ПК-4.1: Знать основные положения и приемы фундаментальных разделов математики, математический аппарат для освоения теоретических основ и практического использования физических методов	Знать: основные средства и методы защиты информации; основные методы, способы и средства получения, хранения, переработки информации; современные методы обработки, анализа и синтеза физической информации;
		ПК-4.2: Уметь использовать математический аппарат для освоения теоретических основ и практического использования физических методов	Уметь: применять требования информационной безопасности для решения физических задач; применять на практике методы, способы и средства получения, хранения, переработки информации; пользоваться современными методами обработки, анализа и синтеза физической информации;
		ПК-4.3: Владеть: навыками работы с современными приборами и методами исследований; навыками пользования современными методами обработки, анализа и синтеза физической информации.	Владеть: основные методами, способами и средствами получения, хранения, переработки информации; навыками пользования современными методами обработки, анализа и синтеза физической информации.

2. Цель и место дисциплины в структуре образовательной программы

Дисциплина «Средства и методы защиты информации» относится к части, формируемой участниками образовательных отношений, рабочего учебного плана.

Дисциплина изучается на 4 курсе в 7 семестре.

Целью изучения дисциплины «Средства и методы защиты информации» 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 и индикаторов достижения компетенций с указанием соотнесенных с ними запланированных результатов обучения по дисциплине. Описание критериев и шкал оценивания результатов обучения по дисциплине

Код и формулировка компетенции

ПК-4: способен осуществлять технический контроль, настройку и эксплуатацию лечебного, диагностического и экспериментального оборудования, устройств медицинской электроники;

Код и наименование индикатора достижения компетенции	Результаты обучения по дисциплине	Критерии оценивания результатов обучения	
		«Зачтено»	«Не зачтено»
ПК-4.1: Знать основные положения и приемы фундаментальных разделов математики, математический аппарат для освоения теоретических основ и практического использования физических методов	Знать: основные средства и методы защиты информации; основные методы, способы и средства получения, хранения, переработки информации; современные методы обработки, анализа и синтеза физической информации;	Знает основные средства и методы защиты информации; основные методы, способы и средства получения, хранения, переработки информации; современные методы обработки, анализа и синтеза физической информации;	Не знает основные средства и методы защиты информации; основные методы, способы и средства получения, хранения, переработки информации; современные методы обработки, анализа и синтеза физической информации;
ПК-4.2: Уметь использовать математический аппарат для освоения теоретических основ и практического использования физических методов	Уметь: применять требования информационной безопасности для решения физических задач; применять на практике методы, способы и средства получения, хранения, переработки информации; пользоваться современными методами обработки, анализа и синтеза физической информации;	Умеет применять требования информационной безопасности для решения физических задач; применять на практике методы, способы и средства получения, хранения, переработки информации; пользоваться современными методами обработки, анализа и синтеза физической информации;	Не умеет применять требования информационной безопасности для решения физических задач; применять на практике методы, способы и средства получения, хранения, переработки информации; пользоваться современными методами обработки, анализа и синтеза физической информации;
ПК-4.3: Владеть: навыками работы с современными приборами и методами исследований; навыками пользования современными	Владеть: основные методами, способами и средствами получения, хранения, переработки информации;	Владеет основные методами, способами и средствами получения, хранения, переработки информации;	Не владеет основные методами, способами и средствами получения, хранения, переработки информации;

методами обработки, анализа и синтеза физической информации.	навыками пользования современными методами обработки, анализа и синтеза физической информации.	навыками пользования современными методами обработки, анализа и синтеза физической информации.	навыками пользования современными методами обработки, анализа и синтеза физической информации.

4.2. Типовые контрольные задания или иные материалы, необходимые для оценивания результатов обучения по дисциплине, соотнесенных с установленными в образовательной программе индикаторами достижения компетенций. Методические материалы, определяющие процедуры оценивания результатов обучения по дисциплине

Код и наименование индикатора достижения компетенции	Результаты обучения по дисциплине	Оценочные средства
ПК-4.1: Знать основные положения и приемы фундаментальных разделов математики, математический аппарат для освоения теоретических основ и практического использования физических методов	Знать: основные средства и методы защиты информации; основные методы, способы и средства получения, хранения, переработки информации; современные методы обработки, анализа и синтеза физической информации;	Устный опрос
ПК-4.2: Уметь использовать математический аппарат для освоения теоретических основ и практического использования физических методов	Уметь: применять требования информационной безопасности для решения физических задач; применять на практике методы, способы и средства получения, хранения, переработки информации; пользоваться современными методами обработки, анализа и синтеза физической информации;	Устный опрос Защита лабораторных работ
ПК-4.3: Владеть: навыками работы с современными приборами и методами исследований; навыками пользования современными методами обработки, анализа и синтеза физической информации.	Владеть: основные методами, способами и средствами получения, хранения, переработки информации; навыками пользования современными методами обработки, анализа и синтеза физической информации.	Защита лабораторных работ

Критериями оценивания при *модульно-рейтинговой системе* являются баллы, которые выставляются преподавателем за виды деятельности (оценочные средства) по итогам изучения модулей (разделов дисциплины), перечисленных в рейтинг-плане дисциплины (*для экзамена:* текущий контроль – максимум 40 баллов; рубежный контроль – максимум 30 баллов, поощрительные баллы – максимум 10; *для зачета:* текущий контроль – максимум 50 баллов; рубежный контроль – максимум 50 баллов, поощрительные баллы – максимум 10).

Шкалы оценивания:

(*для экзамена:*

от 45 до 59 баллов – «удовлетворительно»;

от 60 до 79 баллов – «хорошо»;

от 80 баллов – «отлично».

для зачета:

зачтено – от 60 до 110 рейтинговых баллов (включая 10 поощрительных баллов),

не зачтено – от 0 до 59 рейтинговых баллов).

Рейтинг – план дисциплины

«Средства и методы защиты информации»

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

Виды учебной деятельности студентов	Балл за конкретное задание	Число заданий за семестр	Баллы	
			Минималь-ный	Максималь-ный
Модуль I				
Текущий контроль				
1. Контрольная работа	0-15	1	0	15
2.Допуск, выполнение лабораторной работы, оформление отчета	0-2	5	0	10
Рубежный контроль				
1.Защита отчетов по лабораторной работе	0-5	5	0	25
Всего баллов за модуль:			**0**	**50**
Модуль II				
Текущий контроль				
1. Тестирование	0-15	1	0	15
2. Допуск, выполнение лабораторной работы, оформление отчета	0-2	5	0	10
Рубежный контроль				
1.Защита отчетов по лабораторной работе	0-5	5	0	25
Всего баллов за модуль:			**0**	**50**
Поощрительные баллы				
1. Студенческие олимпиады			0	10
2. Публикации статей				10
3. Работы со школьниками (кружок, конкурсы, олимпиады)				10
Посещаемость (баллы вычитаются из общей суммы набранных баллов)				
1.Посещаемость лекционных занятий			0	-6
2.Посещение практических занятий			0	-10
Итоговый контроль				
Зачет				

Вопросы для подготовки к зачету

1. Источники, риски и формы атак на компьютерные системы.
2. Модели безопасности информационных систем.
3. Стандарты безопасности. Законодательные меры защиты информации.
4. Криптографические модели и методы защиты информации.
5. Защита информации в современных операционных системах.
6. Защита информации в сети.

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

Планы практических занятий

1. Информационная часть графического файла (на примере *.bmp).
2. Преобразование изображений путем редактирования растрового массива в bmp-файле.
3. Работа с палитрой.
4. Вывод bmp-картинки на экран, используя функции VESA.
5. Вывод bmp-картинки через контекст дисплея.
6. Программа компрессии и декомпрессии изображения,сохраненного в bmp-формате.
7. Реализация алгоритма LZW.
8. Алгоритм Хаффмана.
9. Геометрические преобразования изображений.

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
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
3. Шаньгин, В.Ф. Информационная безопасность. - М.: ДМК Пресс, 2014, 702 с. [Электронный ресурс]: 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.

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
1	**2**	**3**
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 E2214Hb-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.

Приложение № 1

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

Вид работы	**Объем дисциплины**
Общая трудоемкость дисциплины (ЗЕТ / часов)	2/72
Учебных часов на контактную работу с преподавателем:	54.2
лекций	18
практических/ семинарских	
лабораторных	36
других (групповая, индивидуальная консультация и иные виды учебной деятельности, предусматривающие работу обучающихся с преподавателем) (ФКР)	0.2
Учебных часов на самостоятельную работу обучающихся (СР)	18
Учебных часов на подготовку к экзамену/зачету/дифференцированному зачету (Контроль)	

Формы контроля:
зачет____7_____семестр

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

								Тест
5	Защита информации в современных операционных системах			6	3	1-3	Подготовка к защите лабораторных работ	Лабораторная работа Контрольная работа Тест
6	Защита информации в сети	3		6	3	1-3	Подготовка к защите лабораторных работ	Лабораторная работа Контрольная работа Тест
	Всего часов:	**18**		**36**	**18**			

Примечание 1. Часы на самостоятельную работу включают время на подготовку к экзамену (контроль).
Примечание 2. 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).