

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

Актуализирована:  
на заседании кафедры  
протокол от «20» июня 2017 г. №7  
Зав. кафедрой \_\_\_\_\_ /Салихов Р.Б.

Согласовано:  
Председатель УМК факультета /института  
\_\_\_\_\_ /Балапанов М.Х.

**РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ (МОДУЛЯ)**

дисциплина Основы информационной безопасности сетей и систем связи

Б1.В.1.ДВ.04.01; дисциплина по выбору

(Цикл дисциплины и его часть (базовая, вариативная, дисциплина по выбору))

**программа бакалавриата**

Направление подготовки

11.03.02 Инфокоммуникационные технологии и системы связи

Направленность (профиль) подготовки

Оптические системы и сети связи

Квалификация

бакалавр

Разработчик (составитель)  
\_\_\_\_\_ /доцент, к.ф.м.н.

\_\_\_\_\_ /Тавлыкаев Р.Ф.

Для приема: 2015 г.

Уфа - 2017 г.

Составитель / составители: доцент, к.ф.м.н. Тавлыкаев Р.Ф.

Рабочая программа дисциплины актуализирована на заседании кафедры инфокоммуникационных технологий и наноэлектроники, протокол от «20» июня 2017 г. №7

## Список документов и материалов

1. Перечень планируемых результатов обучения по дисциплине, соотнесенных с планируемыми результатами освоения образовательной программы.....	4
2. Цели 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).....	5
4. Фонд оценочных средств по дисциплине .....	5
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.....	5
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.....	10
4.3. Рейтинг-план дисциплины.....	13
5. Учебно-методическое и информационное обеспечение дисциплины .....	13
5.1. Перечень основной и дополнительной учебной литературы, необходимой для освоения дисциплины .....	13
5.2. Перечень ресурсов информационно-телекоммуникационной сети «Интернет» и программного обеспечения, необходимых для освоения дисциплины .....	14
6. Материально-техническая база, необходимая для осуществления образовательного процесса по дисциплине .....	14

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

В результате освоения образовательной программы обучающийся должен овладеть следующими результатами обучения по дисциплине:

способность использовать основы правовых знаний в различных сферах деятельности (ОК-4);

способность понимать сущность и значение информации в развитии современного информационного общества, сознавать опасности и угрозы, возникающие в этом процессе, соблюдать основные требования информационной безопасности, в том числе защиты государственной тайны (ОПК-1);

способность решать стандартные задачи профессиональной деятельности на основе информационной и библиографической культуры с применением инфокоммуникационных технологий и с учетом основных требований информационной безопасности (ОПК-2);

способность использовать нормативную и правовую документацию, характерную для области инфокоммуникационных технологий и систем связи (нормативные правовые акты Российской Федерации, технические регламенты, международные и национальные стандарты, рекомендации Международного союза электросвязи) (ОПК-5);

умение собирать и анализировать информацию для формирования исходных данных для проектирования средств и сетей связи и их элементов (ПК-8).

Результаты обучения		Формируемая компетенция (с указанием кода)	Примечание
Знания	<p>Основные понятия безопасности: угрозы, уязвимые элементы и риски, особенности информационных ресурсов и требования, предъявляемые к информации как объекту защиты; основные требования информационной безопасности (ИБ) сетей и систем связи, в том числе защиты государственной тайны;</p> <p>Основные методы нарушения конфиденциальности, целостности и доступности информации; модели, стратегии и системы обеспечения ИБ; критерии и классы защищенности сетей и систем связи;</p> <p>Структуру и принципы функционирования современных вычислительных систем; базовые этапы построения системы комплексной защиты сетей и систем связи; показатели защищенности от НСД к информации;</p> <p>Функции системы защиты сетей и систем связи по предупреждению угроз и устранению последствий их реализации.</p>	ОК-4; ОПК-1; ОПК-2; ОПК-5; ПК-8	
Умения	<p>Оценивать характеристику конкретного вида опасности (угрозы) секретности, целостности информации сетей и систем связи;</p> <p>Использовать нормативную и правовую документацию, характерную для информационной безопасности и методологии защиты сетей и систем связи (законы РФ, технические регламенты, международные и национальные стандарты, рекомендации МСЭ, стандарты связи, протоколы, терминологию);</p> <p>Определять обобщенные и базовые показатели уязвимости информации, вычислять показатели защищенности информации, анализировать опасности многоуровневых систем защиты в сетях и системах связи;</p>	ОК-4; ОПК-1; ОПК-2; ОПК-5; ПК-8	

	изучать научно-техническую информацию, отечественный и зарубежный опыт в области теории информационной безопасности сетей и систем связи и методологии защиты инфокоммуникаций; разрабатывать модели защиты информации сетей и систем связи от несанкционированного доступа; модели систем разграничения доступа к ресурсам инфокоммуникаций; модели общей оценки угроз информации.		
Владения (навыки / опыт деятельности)	основными методами защиты информации в сетях и системах связи, способами и средствами получения, хранения, переработки информации ; навыками самостоятельной работы на компьютере и в компьютерных сетях с целью выбора программных решений для обеспечения информационной безопасности сетей и систем связи, вычисления показателя степени риска и анализа опасностей инфокоммуникаций;	ОПК-1; ОПК-2.	

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

Целью преподавания дисциплины является изучение основ информационной безопасности и защиты информации в системах и сетях связи при их создании и эксплуатации. Дисциплина «Основы информационной безопасности сетей и систем связи» относится к вариативной части образовательной программы (дисциплина по выбору).

Дисциплина изучается на 4 курсе в 7 семестре.

Для освоения дисциплины необходимы компетенции, сформированные в рамках изучения следующих дисциплин:

1. Б1.Б.06 Правоведение
2. Б1.Б.25 Вычислительная техника и информационные технологии
3. Б1.В.1.07 Сети связи и системы коммутации

## 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: способность использовать основы правовых знаний в различных сферах деятельности (ОК-4):

Этап (уровень) освоения компетенции	Планируемые результаты обучения (показатели достижения заданного уровня освоения компетенций)	Критерии оценивания результатов обучения	
		Незачтено	Зачтено

Первый этап (уровень)	Основные понятия безопасности: угрозы, уязвимые элементы и риски, особенности информационных ресурсов и требования, предъявляемые к информации как объекту защиты; основные требования информационной безопасности (ИБ) сетей и систем связи, в том числе защиты государственной тайны;	Отсутствие знаний или фрагментарные представления об основных понятиях и утверждениях, входящих в содержание дисциплины	Сформированные (возможно неполные) представления об основных понятиях и утверждениях, входящих в содержание дисциплины
Второй этап (уровень)	Использовать нормативную и правовую документацию, характерную для информационной безопасности и методологии защиты сетей и систем связи (законы РФ, технические регламенты, международные и национальные стандарты, рекомендации МСЭ, стандарты связи, протоколы, терминологию);	Отсутствие умений или фрагментарные умения употреблять правильную терминологию, определения, обозначения в области безопасности и методологии защиты сетей и систем связи	В целом успешное (возможно не систематическое) умение употреблять правильную терминологию, определения, обозначения в области безопасности и методологии защиты сетей и систем связи.
Третий этап (уровень)	основными методами защиты информации в сетях и системах связи, способами и средствами получения, хранения, переработки информации ; навыками самостоятельной работы на компьютере и в компьютерных сетях с целью выбора программных решений для обеспечения информационной безопасности сетей и систем связи, вычисления показателя степени риска и анализа опасностей инфокоммуникаций	Отсутствие владения или фрагментарное владение навыками работы со стандартами и спецификациями современных средств обеспечения информационной безопасности сетей и систем связи.	В целом успешное (возможно не систематическое) владение навыками работы со стандартами и спецификациями современных средств обеспечения информационной безопасности сетей и систем связи.

Код и формулировка компетенции: способность понимать сущность и значение информации в развитии современного информационного общества, сознавать опасности и угрозы, возникающие в этом процессе, соблюдать основные требования информационной безопасности, в том числе защиты государственной тайны (ОПК-1):

Этап (уровень) освоения компетенции	Планируемые результаты обучения (показатели достижения заданного уровня освоения компетенций)	Критерии оценивания результатов обучения	
		Незачтено	Зачтено
Первый этап (уровень)	Основные понятия безопасности: угрозы, уязвимые элементы и риски, особенности информационных ресурсов и требования, предъявляемые к информации как объекту защиты; основные требования информационной безопасности (ИБ) сетей и систем связи, в том числе защиты государственной тайны; Основные методы нарушения конфиденциальности, целостности и доступности информации; модели, стратегии и системы обеспечения ИБ	Отсутствие знаний или фрагментарные представления об основных понятиях и утверждениях, входящих в содержание дисциплины	Сформированные (возможно неполные) представления об основных понятиях и утверждениях, входящих в содержание дисциплины

Второй этап (уровень)	Оценивать характеристику конкретного вида опасности (угрозы) секретности, целостности информации сетей и систем связи; Определять обобщенные и базовые показатели уязвимости информации, вычислять показатели защищенности информации, анализировать опасности многоуровневых систем защиты в сетях и системах связи; изучать научно-техническую информацию, отечественный и зарубежный опыт в области теории информационной безопасности сетей и систем связи и методологии защиты инфокоммуникаций	Отсутствие умений или фрагментарные умения употреблять правильную терминологию, определения, обозначения в области теории информационной безопасности сетей и систем связи и методологии защиты инфокоммуникаций	В целом успешное (возможно не систематическое) умение употреблять правильную терминологию, определения, обозначения и единицы измерения величин в области теории информационной безопасности сетей и систем связи и методологии защиты инфокоммуникаций
Третий этап (уровень)	основными методами защиты информации в сетях и системах связи, способами и средствами получения, хранения, переработки информации ; навыками самостоятельной работы на компьютере и в компьютерных сетях с целью выбора программных решений для обеспечения информационной безопасности сетей и систем связи, вычисления показателя степени риска и анализа опасностей инфокоммуникаций.	Отсутствие владения или фрагментарное владение навыками организации экспериментальных испытаний на соответствие требованиям стандартов, спецификаций и требований в области информационной безопасности сетей и систем связи и методологии защиты инфокоммуникаций	В целом успешное (возможно не систематическое) владение навыками вычисления показателя степени риска и анализа опасностей инфокоммуникаций..

Код и формулировка компетенции: способность решать стандартные задачи профессиональной деятельности на основе информационной и библиографической культуры с применением инфокоммуникационных технологий и с учетом основных требований информационной безопасности (ОПК-2).

Этап (уровень) освоения компетенции	Планируемые результаты обучения (показатели достижения заданного уровня освоения компетенций)	Критерии оценивания результатов обучения	
		Незачтено	Зачтено
Первый этап (уровень)	Структуру и принципы функционирования современных вычислительных систем; базовые этапы построения системы комплексной защиты сетей и систем связи; показатели защищенности от НСД к информации;	Отсутствие знаний или фрагментарные представления об основных понятиях и утверждениях, входящих в содержание дисциплины	Сформированные (возможно неполные) представления об основных понятиях и утверждениях, входящих в содержание дисциплины
Второй этап (уровень)	Определять обобщенные и базовые показатели уязвимости информации, вычислять показатели защищенности информации, анализировать опасности многоуровневых систем защиты в сетях и системах связи; изучать научно-техническую информацию, отечественный и	Отсутствие умений или фрагментарные умения употреблять правильную терминологию, определения, обозначения и единицы измерения величин в области	В целом успешное (возможно не систематическое) умение употреблять правильную терминологию, определения, обозначения и единицы измерения величин в области информационной

	зарубежный опыт в области теории информационной безопасности сетей и систем связи и методологии защиты инфокоммуникаций.	информационной безопасности сетей и систем связи	безопасности сетей и систем связи
Третий этап (уровень)	навыками самостоятельной работы на компьютере и в компьютерных сетях с целью выбора программных решений для обеспечения информационной безопасности сетей и систем связи	Отсутствие владения или фрагментарное владение навыками выбора программных решений для обеспечения информационной безопасности сетей и систем связи.	В целом успешное (возможно не систематическое) владение навыками выбора программных решений для обеспечения информационной безопасности сетей и систем связи..

Код и формулировка компетенции: способность использовать нормативную и правовую документацию, характерную для области инфокоммуникационных технологий и систем связи (нормативные правовые акты Российской Федерации, технические регламенты, международные и национальные стандарты, рекомендации Международного союза электросвязи) (ОПК-5).

Этап (уровень) освоения компетенции	Планируемые результаты обучения (показатели достижения заданного уровня освоения компетенций)	Критерии оценивания результатов обучения	
		Незачтено	Зачтено
Первый этап (уровень)	Основные требования информационной безопасности (ИБ) сетей и систем связи, в том числе защиты государственной тайны; Основные методы нарушения конфиденциальности, целостности и доступности информации; модели, стратегии и системы обеспечения ИБ; критерии и классы защищенности сетей и систем связи; Структуру и принципы функционирования современных вычислительных систем; базовые этапы построения системы комплексной защиты сетей и систем связи; показатели защищенности от НСД к информации;. Функции системы защиты сетей и систем связи по предупреждению угроз и устранению последствий их реализации.	Отсутствие знаний или фрагментарные представления об основных понятиях и утверждениях, входящих в содержание дисциплины	Сформированные (возможно неполные) представления об основных понятиях и утверждениях, входящих в содержание дисциплины
Второй этап (уровень)	Оценивать характеристику конкретного вида опасности (угрозы) секретности, целостности информации сетей и систем связи; Использовать нормативную и правовую документацию, характерную для информационной безопасности и методологии защиты сетей и систем связи (законы РФ, технические регламенты, международные и национальные стандарты, рекомендации МСЭ, стандарты связи, протоколы,	Отсутствие умений или фрагментарные умения употреблять правильную терминологию, определения, обозначения и единицы измерения величин в области информационной безопасности и методологии защиты сетей и систем связи	В целом успешное (возможно не систематическое) умение употреблять правильную терминологию, определения, обозначения и единицы измерения величин в области информационной безопасности и методологии защиты сетей и систем связи



	терминологию).		
Третий этап (уровень)	основными методами защиты информации в сетях и системах связи, способами и средствами получения, хранения, переработки информации; вычисления показателя степени риска и анализа опасностей инфокоммуникаций;	Отсутствие владения или фрагментарное владение навыками организации экспериментальных испытаний на соответствие требованиям стандартов, спецификаций и требований в области информационной безопасности и методологии защиты сетей и систем связи.	В целом успешное (возможно не систематическое) владение навыками организации экспериментальных испытаний на соответствие требованиям стандартов, спецификаций и требований в области информационной безопасности и методологии защиты сетей и систем связи.

Код и формулировка компетенции: умение собирать и анализировать информацию для формирования исходных данных для проектирования средств и сетей связи и их элементов (ПК-8).

Этап (уровень) освоения компетенции	Планируемые результаты обучения (показатели достижения заданного уровня освоения компетенций)	Критерии оценивания результатов обучения	
		Незачтено	Зачтено
Первый этап (уровень)	Основные методы нарушения конфиденциальности, целостности и доступности информации; модели, стратегии и системы обеспечения ИБ; критерии и классы защищенности сетей и систем связи; Структуру и принципы функционирования современных вычислительных систем; базовые этапы построения системы комплексной защиты сетей и систем связи; показатели защищенности от НСД к информации;. Функции системы защиты сетей и систем связи по предупреждению угроз и устранению последствий их реализации.	Отсутствие знаний или фрагментарные представления об основных понятиях и утверждениях, входящих в содержание дисциплины	Сформированные (возможно неполные) представления об основных понятиях и утверждениях, входящих в содержание дисциплины
Второй этап (уровень)	Определять обобщенные и базовые показатели уязвимости информации, вычислять показатели защищенности информации, анализировать опасности многоуровневых систем защиты в сетях и системах связи; разрабатывать модели защиты информации сетей и систем связи от несанкционированного доступа; модели систем разграничения доступа к ресурсам инфокоммуникаций; модели общей оценки угроз информации.	Отсутствие умений или фрагментарные умения употреблять правильную терминологию, определения, обозначения и единицы измерения величин в области информационной безопасности и методологии защиты сетей и систем связи	В целом успешное (возможно не систематическое) умение употреблять правильную терминологию, определения, обозначения и единицы измерения величин в области информационной безопасности и методологии защиты сетей и систем связи

Третий этап (уровень)	основными методами защиты информации в сетях и системах связи, способами и средствами получения, хранения, переработки информации; навыками самостоятельной работы на компьютере и в компьютерных сетях с целью выбора программных решений для обеспечения информационной безопасности сетей и систем связи, вычисления показателя степени риска и анализа опасностей инфокоммуникаций	Отсутствие владения или фрагментарное владение навыками вычисления показателей степени риска и анализа опасностей инфокоммуникаций и использования основных методов защиты информации в сетях и системах связи	В целом успешное (возможно не систематическое) владение навыками вычисления показателей степени риска и анализа опасностей инфокоммуникаций и использования основных методов защиты информации в сетях и системах связи.
-----------------------	---	--	--

Показатели сформированности компетенции:

Критериями оценивания являются баллы, которые выставляются преподавателем за виды деятельности (оценочные средства) по итогам изучения модулей (разделов дисциплины), перечисленных в рейтинг-плане дисциплины: текущий контроль – максимум 50 баллов; рубежный контроль – максимум 50 баллов, поощрительные баллы – максимум 10).

Шкалы оценивания:

для зачета:

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

**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	Основные понятия безопасности: угрозы, уязвимые элементы и риски, особенности информационных ресурсов и требования, предъявляемые к информации как объекту защиты; основные требования информационной безопасности (ИБ) сетей и систем связи, в том числе защиты государственной тайны; Основные методы нарушения конфиденциальности, целостности и доступности информации; модели, стратегии и системы обеспечения ИБ; критерии и классы защищенности сетей и систем связи; Структуру и принципы функционирования современных вычислительных систем; базовые этапы построения системы комплексной защиты сетей и систем связи; показатели защищенности от НСД к информации;. Функции системы защиты сетей и систем связи по предупреждению угроз	ОК-4; ОПК-1; ОПК-2; ОПК-5; ПК-8	Лабораторные работы; устный опрос; тестирование

	и устранению последствий их реализации.		
2-й этап Умения	<p>Оценивать характеристику конкретного вида опасности (угрозы) секретности, целостности информации сетей и систем связи;</p> <p>Использовать нормативную и правовую документацию, характерную для информационной безопасности и методологии защиты сетей и систем связи (законы РФ, технические регламенты, международные и национальные стандарты, рекомендации МСЭ, стандарты связи, протоколы, терминологию);</p> <p>Определять обобщенные и базовые показатели уязвимости информации, вычислять показатели защищенности информации, анализировать опасности многоуровневых систем защиты в сетях и системах связи;</p> <p>изучать научно-техническую информацию, отечественный и зарубежный опыт в области теории информационной безопасности сетей и систем связи и методологии защиты инфокоммуникаций;</p> <p>разрабатывать модели защиты информации сетей и систем связи от несанкционированного доступа; модели систем разграничения доступа к ресурсам инфокоммуникаций; модели общей оценки угроз информации.</p>	ОК-4; ОПК-1; ОПК-2; ОПК-5; ПК-8	Лабораторные работы; устный опрос; тестирование
3-й этап Владеть навыками	<p>основными методами защиты информации в сетях и системах связи, способами и средствами получения, хранения, переработки информации ;</p> <p>навыками самостоятельной работы на компьютере и в компьютерных сетях с целью выбора программных решений для обеспечения информационной безопасности сетей и систем связи,</p> <p>вычисления показателя степени риска и анализа опасностей инфокоммуникаций</p>	ОПК-1; ОПК-2.	Лабораторные работы; устный опрос; тестирование

### Примеры тестовых заданий (для рубежного контроля)

1. Как называется умышленно искаженная информация?
  - а) Дезинформация
  - б) Информативный поток
  - в) Достоверная информация
  - г) Перестает быть информацией
  
2. Как называется информация, к которой ограничен доступ?
  - а) Конфиденциальная
  - б) Противозаконная
  - в) Открытая

г) Недоступная

3. Какими путями может быть получена информация?

- а) проведением, покупкой и противоправным добыванием информации научных исследований
- б) захватом и взломом ПК информации научных исследований
- в) добыванием информации из внешних источников и скремблированием информации научных исследований
- г) захватом и взломом защитной системы для информации научных исследований

4. Как называются компьютерные системы, в которых обеспечивается безопасность информации?

- а) защищенные КС
- б) небезопасные КС
- в) самодостаточные КС
- г) саморегулирующиеся КС

5. Основной документ, на основе которого проводится политика информационной безопасности?

- а) программа информационной безопасности
- б) регламент информационной безопасности
- в) политическая информационная безопасность
- г) протекторат

б) В зависимости от формы представления информация может быть разделена на...

- а) речевую, документированную и телекоммуникационную
- б) мысль, слово и речь
- г) цифровая, звуковая и тайная
- в) цифровая, звуковая

**Критерии оценки (в баллах):**

***За каждый правильный ответ- 1 балл***

***За ошибочный ответ – 0 баллов***

### **Лабораторные работы**

Порядок выполнения лабораторных работ приведен в «Описании лабораторных работ по дисциплине «Основы информационной безопасности сетей и систем связи», имеющихся в специализированной лаборатории (ауд. 210 физ.-мат. корп. БашГУ).

Тематика и перечень лабораторных работ:

1. Моделирование IPSec VPN в Cisco Packet Tracer
2. Настройка Firewall на маршрутизаторе в Cisco Packet Tracer
3. Работа протокола Radius в Cisco Packet Tracer
4. Шифрование с открытым ключом и электронная цифровая подпись на GPG
5. Метод шифрования с открытым ключом RSA
6. Использование хэш-функций на примере MD5. Оценка устойчивости пароля ко взлому.

**Критерии оценки (в баллах)**

**Работа выполнена, к отчету нет существенных замечаний**

***5 баллов***

**Работа выполнена, отчет не представлен или в нем имеются существенные**

***2 баллов***

**Примеры вопросов для устного опроса и  
для проведения зачета (для заочной формы обучения)**

1. Назовите известные вам модели защиты от несанкционированного доступа к информации.
2. Перечислите основные принципы защиты информации от несанкционированного доступа. В чем суть каждого из них?
3. В чем отличие идентификации от аутентификации пользователей?
4. Раскройте основные особенности известных методов аутентификации с использованием индивидуальных физиологических характеристик пользователей.
5. Какие основные способы шифрования вы знаете? Каковы их преимущества и недостатки?

*Развернутость и полнота ответов на вопросы определяется в соответствии с критериями из п.4.1*

*За правильный развернутый полный ответ - 10 баллов*

*За правильный, но неполный ответ – 5 баллов*

*За ошибочный ответ или отсутствие ответа – 0 баллов*

**Критерии оценивания для заочной формы обучения:**

Обучающиеся заочной формы обучения допускаются к сдаче зачета при условии выполнения всех предложенных лабораторных работ и тестирования, в результате которого будет дано не менее 50% правильных ответов.

- оценка «зачтено» выставляется студенту, если он ответил на 2 вопроса из перечня;

- оценка «не зачтено» выставляется студенту, если он не ответил на один или оба вопроса.

Ответы на вопросы должны соответствовать критериям оценивания результатов обучения, приведенным в разделе 4.1.

**4.3 Рейтинг-план дисциплины**

Рейтинг–план дисциплины представлен в приложении 2.

**5. Учебно-методическое и информационное обеспечение дисциплины**

**5.1. Перечень основной и дополнительной учебной литературы, необходимой для освоения дисциплины**

Основная литература:

1. Малюк, А.А. Защита информации в информационном обществе : учебное пособие / А.А. Малюк. - Москва : Горячая линия-Телеком, 2015. - 229 с. : ил., схем., табл. - Библиогр. в кн. - ISBN 978-5-9912-0481-1 ; То же [Электронный ресурс]. - URL: <http://biblioclub.ru/index.php?page=book&id=457170> (19.02.2018).
2. Технические средства и методы защиты информации : учебное пособие для вузов / А.П. Зайцев, А.А. Шелупанов, Р.В. Мещеряков и др. ; под ред. А.П. Зайцева, А.А. Шелупанова. - 4-е изд., испр. и доп. - Москва : Горячая линия - Телеком, 2012. - 616 с. : ил. - Библиогр. в кн. - ISBN 978-5-9912-0084-4 ; То же [Электронный ресурс]. - URL: <http://biblioclub.ru/index.php?page=book&id=253207> (19.02.2018).
3. Бузов, Г.А. Защита информации ограниченного доступа от утечки по техническим каналам / Г.А. Бузов. - Москва : Горячая линия-Телеком, 2015. - 585 с. : ил., схем., табл. - Библиогр. в

кн. - ISBN 978-5-9912-0424-8 ; То же [Электронный ресурс]. - URL: <http://biblioclub.ru/index.php?page=book&id=457143> (19.02.2018).

Дополнительная литература:

4. Основы информационной безопасности : учебное пособие для вузов / Е.Б. Белов, В.П. Лось, Р.В. Мещеряков, А.А. Шелупанов. - Москва : Горячая линия - Телеком, 2011. - 558 с. : ил. - ISBN 5-93517-292-5 ; То же [Электронный ресурс]. - URL: <http://biblioclub.ru/index.php?page=book&id=253056> (19.02.2018).
5. Новиков, В.К. Организационно-правовые основы информационной безопасности (защиты информации): юридическая ответственность за правонарушения : учебное пособие / В.К. Новиков. - Москва : Горячая линия-Телеком, 2015. - 175 с. : ил., схем., табл. - Библиогр. в кн. - ISBN 978-5-9912-0525-2 ; То же [Электронный ресурс]. - URL: <http://biblioclub.ru/index.php?page=book&id=457171> (19.02.2018).
6. Программно-аппаратные средства обеспечения информационной безопасности : учебное пособие для вузов / А.В. Душкин, О.М. Барсуков, К.В. Славнов, Е.В. Кравцов ; под ред. А.В. Душкина. - Москва : Горячая линия - Телеком, 2016. - 248 с. : схем., табл., ил. - Библиогр.: с. 234-235 - ISBN 978-5-9912-0470-5 ; То же [Электронный ресурс]. - URL: <http://biblioclub.ru/index.php?page=book&id=483768> (19.02.2018).
7. Аутентификация. Теория и практика обеспечения безопасного доступа к информационным ресурсам : учебное пособие для вузов / А.А. Афанасьев, Л.Т. Веденьев, А.А. Воронцов и др. ; под ред. А.А. Шелупанова, С.Л. Груздева, Ю.С. Нахаева. - 2-е изд., стер. - Москва : Горячая линия - Телеком, 2012. - 552 с. : ил. - Библиогр.: с. 244-246 - ISBN 978-5-9912-0257-2 ; То же [Электронный ресурс]. - URL: <http://biblioclub.ru/index.php?page=book&id=252979> (19.02.2018)

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

1. Нормативно – правовые документы Министерства связи и массовых коммуникаций Российской Федерации – [www.minsvyaz.ru](http://www.minsvyaz.ru).
2. Рекомендации Международного союза электросвязи – ITU-T – International Telecommunication Union – Telecommunication standardization sector – Сектор стандартизации телекоммуникаций Международного союза электросвязи –МСЭ-Т - [http://www.rfcmd.ru/sphider/docs/ITU-T/ITU-T\\_Rec\\_List\\_A-Z\\_ANO\\_E.htm](http://www.rfcmd.ru/sphider/docs/ITU-T/ITU-T_Rec_List_A-Z_ANO_E.htm).
3. Рекомендации Европейского института стандартизации телекоммуникаций - ETSI - European Telecommunications Standards Institute - [www.etsi.org](http://www.etsi.org).
4. Документы инженерной рабочей группы Интернет – RFC IETF – Request For Comment - Internet Engineering Task Force - [rfc.com.ru](http://rfc.com.ru).

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

Для проведения лекционных занятий используется аудиторный фонд физико-технического института.

<i>Наименование специализированных аудиторий, кабинетов, лабораторий</i>	<i>Вид занятий</i>	<i>Наименование оборудования, программного обеспечения</i>
<i>1</i>	<i>2</i>	<i>3</i>
Аудитория (к.323)	Лекции	Компьютер, мультимедийный проектор, экран, доска.
Лаборатория (к.210)	Лабораторные	Учебная мебель, доска аудиторная.

	работы	<p>1. Windows 8 Russian; Windows Professional 8 Russian Upgrade. Договор №104 от 17.06.2013 г. Лицензия- OLP NL Academic Edition. Бессрочная.</p> <p>2. Microsoft Office Standard 2013 Russian. Договор №114 от 12.11.2014 г.. Лицензия-OLP NL Academic Edition. Бессрочная.</p> <p>3. Компас-3D V13. Проектирование и конструирование в машиностр. Дог. №263 от 07.12.2012 г. Бессрочная.</p>
Читальный зал № 2 (физико-математический корпус)	Самостоятельная работа	Учебная мебель, учебно-наглядные пособия, стенд по пожарной безопасности, моноблоки стационарные – 5 шт., принтер – 1 шт., сканер- 1 шт.

## СОДЕРЖАНИЕ РАБОЧЕЙ ПРОГРАММЫ

дисциплины Основы информационной безопасности сетей и систем связи на 7 семестр

очная

форма обучения

Вид работы	Объем дисциплины
Общая трудоемкость дисциплины (ЗЕТ / часов)	3/108
Учебных часов на контактную работу с преподавателем:	
лекций	16
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)	53,8
Учебных часов на подготовку к экзамену/зачету/дифференцированному зачету (Контроль)	-

Форма(ы) 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 самостоятель ной работе студентов	Форма текущего контроля успеваемости (коллоквиумы, контрольные работы, компьютерные тесты и т.п.)
		ЛК	ПР/СЕМ	ЛР	СРС			
1	2	4	5	6	7	8	9	10
1.	Информационное общество и информационная безопасность. Определение угрозы и уязвимости информации. Системная классификация угроз. Количественная оценка угроз. Понятие информационного риска.	4	-	-	18	[1]:гл.1-3 [4]:ч.1; ч.2,гл.5	[6]:гл.1 [5]:гл.1	тест
2	Организационно-правовое обеспечение защиты информации. Доктрина информационной безопасности Российской Федерации. Концепция правового обеспечения защиты информации. Опыт законодательного регулирования информатизации за рубежом.	4	-	-	8	[1]:гл.11 [3]:гл.3,5 [4] ч.1, гл.6,7 [4] ч.2, гл.8	[5]:гл.1-5	тест
3.	Защита информации от несанкционированного доступа. Правила разграничения доступа. Модели разграничения доступа. Проблемы опознавания пользователя. Характеристики устройств аутентификации	2	-	12	12	[1]:гл.5 [2]:гл.4.11 [4]: ч.2, гл.3	[6]:гл.2 [7] гл.1-4	Лабораторные работы; тест
4.	Криптографические методы защиты информации. Криптографические алгоритмы Стойкость криптосистемы. Стандарты криптографической защиты DES и ГОСТ. Несимметричные системы шифрования.	2	-	12	8	[1]:гл.7 [4] ч.2, гл.12	[7]:гл. 5 [6]:гл.4.7	Лабораторные работы;тест
5.	Технические каналы утечки информации. Определение и основные виды каналов и источников утечки. Контроль информации в каналах связи. Способы предотвращения утечки информации по техническим каналам. Защита информации в каналах связи. Защита	4	-	12	7,8	[1]:гл.10 [2]:гл.1,4 [3], гл.1	[6]:гл.5 [7]:гл.7,8	Лабораторные работы;тест

	информации от утечки по каналу побочных электромагнитных излучений и наводок.							
	<b>Всего часов:</b>	16	-	36	53,8			

## СОДЕРЖАНИЕ РАБОЧЕЙ ПРОГРАММЫ

дисциплины Основы информационной безопасности сетей и систем связи на 2 сессию 5 курса

заочная

форма обучения

<b>Вид работы</b>	<b>Объем дисциплины</b>
Общая трудоемкость дисциплины (ЗЕТ / часов)	3/108
Учебных часов на контактную работу с преподавателем:	
лекций	4
практических/ семинарских	-
лабораторных	12
других (групповая, индивидуальная консультация и иные виды учебной деятельности, предусматривающие работу обучающихся с преподавателем) (ФКР)	0,2
Учебных часов на самостоятельную работу обучающихся (СР)	87,8
Учебных часов на подготовку к экзамену/зачету/дифференцированному зачету (Контроль)	4

Форма(ы) контроля:

зачет \_\_\_\_\_ 2 \_\_\_\_\_ сессия 5 курса

№ 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 самостоятель ной работе студентов	Форма текущего контроля успеваемости (коллоквиумы, контрольные работы, компьютерные тесты и т.п.)
		ЛК	ПР/СЕМ	ЛР	СРС			
1	2	4	5	6	7	8	9	10
1.	Информационное общество и информационная безопасность. Определение угрозы и уязвимости информации. Системная классификация угроз. Количественная оценка угроз. Понятие информационного риска.	4	-	-	16	[1]:гл.1-3 [4]:ч.1; ч.2,гл.5	[6]:гл.1 [5]:гл.1	тест
2.	Организационно-правовое обеспечение защиты информации. Доктрина информационной безопасности Российской Федерации. Концепция правового обеспечения защиты информации. Опыт законодательного регулирования информатизации за рубежом.	4	-	-	16	[1]:гл.11 [3]:гл.3,5 [4] ч.1, гл.6,7 [4] ч.2, гл.8	[5]:гл.1-5	тест
3.	Защита информации от несанкционированного доступа. Правила разграничения доступа. Модели разграничения доступа. Проблемы опознавания пользователя. Характеристики устройств аутентификации	2	-	4	18	[1]:гл.5 [2]:гл.4.11 [4]: ч.2, гл.3	[6]:гл.2 [7] гл.1-4	Лабораторные работы ; тест
4.	Криптографические методы защиты информации. Криптографические алгоритмы Стойкость криптосистемы. Стандарты криптографической защиты DES и ГОСТ. Несимметричные системы шифрования.	2	-	4	18	[1]:гл.7 [4] ч.2, гл.12	[7]:гл. 5 [6]:гл.4.7	Лабораторные работы ; тест
5.	Технические каналы утечки информации. Определение и основные виды каналов и источников утечки. Контроль информации в каналах связи. Способы предотвращения утечки информации по техническим каналам. Защита информации в каналах связи. Защита	4	-	4	19,8	[1]:гл.10 [2]:гл.1,4 [3], гл.1	[6]:гл.5 [7]:гл.7,8	Лабораторные работы ; тест

	информации от утечки по каналу побочных электромагнитных излучений и наводок.							
	<b>Всего часов:</b>	2	-	12	87,8			

## Рейтинг – план дисциплины

Основы информационной безопасности сетей и систем связи

специальность Инфокоммуникационные технологии и системы связи  
курс 4, семестр 7

Виды учебной деятельности студентов	Балл за конкретное задание	Число заданий за семестр	Баллы	
			Минимальный	Максимальный
<b>Модуль I Информационное общество и информационная безопасность.</b>				
<b>Текущий контроль</b>				
1. Устный опрос	10	2	0	20
<b>Рубежный контроль</b>				
1. Письменное тестирование	25	1	0	25
<b>Модуль II Технические аспекты информационной безопасности</b>				
<b>Текущий контроль</b>				
1. Выполнение лабораторных работ	2	6	0	12
2. Выполнение расчетов, оформление и защита отчетов по лабораторным работам	3	6	0	18
<b>Рубежный контроль</b>				
1. Письменное тестирование	25	1	0	25
<b>Поощрительные баллы</b>				
1. Участие в студенческих научных конференциях, выставках, конкурсах.	10	1	0	10
<b>Посещаемость (баллы вычитаются из общей суммы набранных баллов)</b>				
1. Непосещение лекционных занятий			0	-6
2. Непосещение практических занятий			0	-10
<b>Итоговый контроль</b>				
1. Зачет	0	1	0	0