Федеральное государственное бюджетное образовательное учреждение инклюзивного высшего образования

«МОСКОВСКИЙ ГОСУДАРСТВЕННЫЙ ГУМАНИТАРНО-ЭКОНОМИЧЕСКИЙ УНИВЕРСИТЕТ»

Факультет Прикладной математики и информатики

Кафедра Информационных технологий и прикладной математики

УТВЕРЖДАЮ
И.о. проректора по ООД
_____ Пузанкова Е.Н.
«30» августа 2019 г.

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ
ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ

образовательная программа направления подготовки
09.03.03 Прикладная информатика
блок Б1.О.20 «Дисциплины (модули)», обязательная часть

Профиль подготовки
Прикладная информатика в биоинформационных технологиях

Квалификация (степень) выпускника
Бакалавр

Форма обучения очная

Курс 2 семестр 3,4

Москва
2019

Рабочая программа составлена на основании федерального государственного образовательного стандарта высшего образования по направлению подготовки 09.03.03 «Прикладная информатика (уровень бакалавриата)», утвержденного приказом Министерства образования и науки Российской Федерации № 922 от 19 сентября 2017 г. Зарегистрировано в Минюсте России 12 октября 2017 г. №48531.

Составители рабочей программы: МГГЭУ, доцент кафедры ИТиПМ
место работы, занимаемая должность

_____ Белоглазов А.А. «21» августа 2019 г.
подпись Ф.И.О. Дата

Рецензент: МГГЭУ, профессор кафедры ИТиПМ
место работы, занимаемая должность

_____ Истомина Т.В. «22» августа 2019 г.
подпись Ф.И.О. Дата

Рабочая программа утверждена на заседании кафедры Информационных технологий и прикладной математики
(протокол №1 от « 26 » августа 2019 г.)

/Зав кафедрой ИТиПМ/ _____ Петрунина Е.В. «26» августа 2019 г.
подпись Ф.И.О. Дата

СОГЛАСОВАНО
Начальник
Учебного отдела

«27» августа 2019 г. _____ Дмитриева И.Г.
(дата) (подпись) (Ф.И.О.)

СОГЛАСОВАНО
Декан
факультета

«26» августа 2019 г. _____ Петрунина Е.В.
(дата) (подпись) (Ф.И.О.)

СОГЛАСОВАНО
Заведующий
библиотекой

«26» августа 2019 г. _____ Ахтырская В.А.
(дата) (подпись) (Ф.И.О.)

РАССМОТРЕНО
ОДОБРЕНО
УЧЕБНО-МЕТОДИЧЕСКИМ
СОВЕТОМ МГГЭУ
ПР № 8 «30» августа 19 г.

1. ОРГАНИЗАЦИОННО-МЕТОДИЧЕСКИЙ РАЗДЕЛ

1.1. Цель и задачи изучения учебной дисциплины (модуля)

Целью изучения дисциплины является подготовка студентов к освоению организационных, технических, алгоритмических и других методов и средств защиты компьютерной информации, ознакомление с законодательством и стандартами в этой области, с современными криптосистемами, изучение методов идентификации пользователей, борьбы с вирусами, изучение способов применения методов защиты информации при проектировании автоматизированных систем обработки информации и управления (АСОИУ).

Задачи:

- раскрытие основных принципов и методов построения систем информационной безопасности;
- определение основных этапов и базовых концептуальных подходов к созданию систем информационной в рамках исторического развития отечественной и зарубежной науки;
- ознакомление с нормативно-правовыми информационной безопасности автоматизированных систем обработки информации;
- ознакомление со способами и особенностями создания систем защиты компьютерных сетей на различных уровнях взаимодействия с окружением;
- приобретение студентами навыков аналитического и эмпирического исследования систем компьютерной защиты сетей;
- выработка целостного представления о различных аспектах строения и функционирования систем компьютерной защиты сетей на всех ее уровнях.

1.2. Требования к результатам освоения дисциплины

Изучение данной дисциплины направлено на формирование следующих компетенций:

Код и наименование компетенции	**Планируемые результаты обучения по дисциплине (модулю), характеризующие этапы формирования компетенций**
ОПК-3. Способен решать стандартные задачи профессиональной деятельности на основе информационной и библиографической культуры с применением информационно-коммуникационных технологий и с учетом основных требований информационной безопасности	ОПК-3.1. Знает принципы, методы и средства решения стандартных задач профессиональной деятельности на основе информационной и библиографической культуры с применением информационно-коммуникационных технологий и с учетом основных требований информационной безопасности.
	ОПК-3.2. Умеет решать стандартные задачи профессиональной деятельности на основе информационной и библиографической культуры с применением информационно-коммуникационных технологий и с учетом основных требований информационной безопасности.
	ОПК-3.3. Владеет навыками подготовки обзоров, аннотаций, составления рефератов, научных докладов, публикаций, и библиографии по научно-исследовательской работе с учетом требований информационной безопасности.
ПК-7. Способен проводить описание прикладных процессов и информационного обеспечения решения	ПК-7.1. Знает инструменты и методы моделирования информационных процессов; способы описания прикладных процессов и программных продуктов; строение современных операционных систем; принципы функционирования современных ИС; методологии ведения

прикладных задач	документооборота в организациях в сфере программного обеспечения.
	ПК-7.2. Умеет проектировать ИС и разрабатывать программные продукты для решения прикладных задач.
	ПК-7.3. Владеет навыками детального описания предметной области, информационных систем и программных продуктов в прикладных областях деятельности.

1.3. Место дисциплины (модуля) в структуре образовательной программы направления подготовки 09.03.03 Прикладная информатика (бакалавриат)

Учебная дисциплина «Информационная безопасность» относится к основной части блока Б1. Изучение учебной дисциплины «Информационная безопасность» базируется на знаниях, умениях и навыках, полученных обучающимися при изучении предшествующих курсов: «Вычислительные системы, сети и телекоммуникации», «Информатика». Изучение учебной дисциплины «Информационная безопасность» необходимо для освоения таких дисциплин, как «Операционные системы», «Администрирование в информационных системах».

2. СТРУКТУРА И СОДЕРЖАНИЕ ДИСЦИПЛИНЫ

2.1.Объем дисциплины и виды учебной работы в соответствии с формами обучения

Объем дисциплины «Информационная безопасность» составляет 7 з.е./ 252 часа:

Вид учебной работы	Всего, часов	Очная форма	
		Курс, часов	
	Очная форма	2 курс 3 сем.	2 курс 4 сем.
Аудиторная работа обучающихся с преподавателем (по видам учебных занятий), всего в том числе:	*114*	*46*	*68*
Лекции	42	18	24
Практические занятия	72	28	44
Лабораторные занятия			
Самостоятельная работа обучающихся	102	62	40
Промежуточная аттестация (подготовка и сдача), всего:			
Контрольная работа			
Курсовая работа			
Зачет		+	
Экзамен			36
Итого: Общая трудоемкость учебной дисциплины (в часах, зачетных единицах)	**252/7**	108/3	144/4

2.2. Содержание дисциплины по темам (разделам)

№ раздела	Наименование раздела, тема	Содержание раздела	Форма текущего контроля
1.	Введение в информационную безопасность (ИБ)	Основные понятия. Анализ угроз. Проблемы безопасности компьютерных сетей. Политика безопасности. Основные составляющие политики безопасности. Нормативно-правовое обеспечение ИБ. Стандарты ИБ. Принципы защиты	Устный опрос

		информационных систем (ИС).	
2.	Технологии защиты данных	Принципы криптозащиты. Криптографические алгоритмы. Симметричные и асимметричные системы шифрования. Технологии аутентификации. Биометрическая аутентификация.	Устный опрос, отчет по практической работе
3.	Технологии защиты вычислительных систем	Обеспечение безопасности операционных систем (ОС). Межсетевые экраны. Защита в виртуальных сетях VPN. Защита на уровнях модели OSI.	Устный опрос, отчет по практической работе
4.	Технологии обнаружения вторжений	Анализ защищенности. Обнаружение атак. Программные средства обнаружения вторжение. Защита удаленного доступа. Защита от вирусов и спама.	Устный опрос, отчет по практической работе
5.	Управление безопасностью	Задачи управления ИБ в информационных системах (ИС). Архитектура и функционирование систем управления ИБ в (ИС). Аудит и мониторинг безопасности (ИС). Обзор систем управления безопасностью.	Устный опрос, отчет по практической работе

2.3. Разделы дисциплин и виды занятий

№ п/п	Наименование темы дисциплины	Лекционные занятия	Практические занятия	Самостоятельная работа	Всего часов	Формы текущего контроля успеваемости
1.	Введение в ИБ Основные понятия. Анализ угроз. Проблемы безопасности компьютерных сетей.	8		30	38	Устный опрос
2.	Технологии защиты данных. Принципы криптозащиты. Криптографические алгоритмы.	10	26	32	68	Устный опрос, отчет по практической работе
	Зачет		2		2	
	Итого:	18	28	62	108	
3.	Технологии защиты вычислительных систем.	8	12	10	30	Устный опрос, отчет по практической работе
4.	Технологии обнаружения вторжений. Анализ защищенности.	8	14	14	36	Устный опрос, отчет по практической работе
5.	Управление безопасностью. Задачи управления ИБ в информационных системах	8	18	16	42	Устный опрос, отчет по практической работе

	(ИС).					
Экзамен					36	
Итого:		24	44	40	144	
Всего:		42	72	102	252	

2.4. Планы теоретических (лекционных) занятий

№	Наименование тем лекций	Кол-во часов в 3,4 семестрах
3 семестр		
РАЗДЕЛ 1. Введение в ИБ		
1.	Основные понятия. Анализ угроз. Проблемы безопасности компьютерных сетей. Политика безопасности. Основные составляющие политики безопасности. Нормативно-правовое обеспечение ИБ. Стандарты ИБ. Принципы защиты информационных систем (ИС).	8
РАЗДЕЛ 2. Технологии защиты данных		
1.	Принципы криптозащиты. Криптографические алгоритмы. Криптоанализ. Симметричные и асимметричные системы шифрования. Технологии электронно-цифровой подписи. Функции хэщирования. Технологии аутентификации. Биометрическая аутентификация.	10
4 семестр		
РАЗДЕЛ 3. Технологии защиты вычислительных систем		
1.	Обеспечение безопасности операционных систем (ОС). Межсетевые экраны. Нормативно-правовое обеспечение. Сертификация и стандартизация. Защита в виртуальных сетях VPN. Защита на уровнях модели OSI.	8
РАЗДЕЛ 4. Технологии обнаружения вторжений		
1.	Анализ защищенности. Обнаружение атак. Защита удаленного доступа. Защита от вирусов и спама.	8
РАЗДЕЛ 5. Управление безопасностью		
1.	Задачи управления ИБ в информационных системах (ИС). Архитектура и функционирование систем управления ИБ в (ИС). Аудит и мониторинг безопасности (ИС). Обзор систем управления безопасностью.	8

2.5. Планы практических (семинарских) занятий

№	Наименование тем практических занятий	Кол-во часов в 3,4 семестрах
3 семестр		
РАЗДЕЛ 2. Технологии защиты данных		
1.	Устройство и принцип работы шифровальной машины «Энигма». Методы защиты текстовой информации и их стойкость. Симметричные криптографический протоколы DES, 3DES, ГОСТ. Стандарт шифрования AES Rijndael. Генерация простых чисел в ассиметричных алгоритмах шифрования. Электронная цифровая подпись. Изучение программы защиты информации PGP. Корректирующие коды.	26
4 семестр		
РАЗДЕЛ 3. Технологии защиты вычислительных систем		
1.	Механизмы защиты в ОС Microsoft Windows. Захват и анализ сетевого трафика. Межсетевые экраны. Организация и защита VPN. Снифферы.	12
РАЗДЕЛ 4. Технологии обнаружения вторжений		

1.	Выявление сетевых атак путем анализа трафика. Системы обнаружения атак. Технологии терминального доступа. Аудит информационной безопасности компьютерных систем. Службы каталогов.	14
РАЗДЕЛ 5. Управление безопасностью		
1.	Создание и модификация виртуальной защищённой сети с помощью ПО.	18

2.6. Планы лабораторных работ – не предусмотрено.

2.7. Планы самостоятельной работы обучающегося по дисциплине (модулю)

№	Название разделов и тем	Виды самостоятельной работы	Трудоемкость	Формируемые компетенции	Формы контроля
1.	Введение в информационную безопасность (ИБ). Политика безопасности. Нормативно-правовое обеспечение ИБ. Международные стандарты в сфере ИБ. Сравнение.	Работа с источниками	30	ОПК-3 ПК-7	Устный опрос
2.	Технологии защиты данных. Симметричные криптопротоколы. Сравнение.	Работа с источниками	32	ОПК-3	Устный опрос
3.	Технологии защиты вычислительных систем. Межсетевые экраны. Стандартизация и сертификация.	Работа с источниками	10	ОПК-3 ПК-7	Устный опрос
4.	Технологии обнаружения вторжений. Средство анализа сетевого трафика Wireshark. Сканирование сети.	Работа с источниками	14	ОПК-3 ПК-7	Устный опрос
5.	Управление безопасностью. Средство анализа сетевого трафика Wireshark. Сканирование сети. Настраивание параметров безопасности сети с использованием ПО Wireshark.	Работа с источниками	16	ОПК-3 ПК-7	Устный опрос

3. ОСОБЕННОСТИ ОБУЧЕНИЯ ЛИЦ С ОВЗ (ПОДА)

Обучение лиц с ограниченными возможностями здоровья осуществляется с учетом индивидуальных психофизических особенностей, а для инвалидов также в соответствии с индивидуальной программой реабилитации инвалида.

Для получения обучающимися, имеющими ограниченные физические возможности, качественного образования должны выполняться следующие важные условия: обучающийся должен иметь возможность беспрепятственно посещать образовательное учреждение и использовать в своём обучении дистанционные образовательные технологии.

Для обучения и контроля обучающихся с нарушениями координации движений предусмотрено проведение тестирования с использованием компьютера.

Во время аудиторных занятий обязательно использование средств обеспечения наглядности учебного материала с помощью мультимедийного проектора. Скорость изложения материала должна учитывать ограниченные физические возможности студентов.

4. УЧЕБНО-МЕТОДИЧЕСКОЕ ОБЕСПЕЧЕНИЕ САМОСТОЯТЕЛЬНОЙ РАБОТЫ ОБУЧАЮЩИХСЯ

Учебно-методическое и информационное обеспечение дисциплины для организации самостоятельной работы студентов (содержит перечень основной литературы, дополнительной литературы, программного обеспечения и Интернет-ресурсы).

5. УЧЕБНО-МЕТОДИЧЕСКОЕ И ИНФОРМАЦИОННОЕ ОБЕСПЕЧЕНИЯ УЧЕБНОЙ ДИСЦИПЛИНЫ (МОДУЛЯ)

5.1 Перечень основной литературы

1. Информационная безопасность конструкций ЭВМ и систем : учеб. пособие / Е.В. Глинская, Н.В. Чичварин. — Москва : ИНФРА-М, 2019. — 118 с. + Доп. материалы [Электронный ресурс; Режим доступа: https://new.znanium.com]. — (Высшее образование: Бакалавриат). — www.dx.doi.org/10.12737/13571. - Текст : электронный. - URL: https://new.znanium.com/catalog/product/991792

2. Нестеров, С. А. Информационная безопасность : учебник и практикум для академического бакалавриата / С. А. Нестеров. — Москва : Издательство Юрайт, 2019. — 321 с. — (Университеты России). — ISBN 978-5-534-00258-4. — Текст : электронный // ЭБС Юрайт [сайт]. — URL: https://biblio-online.ru/bcode/434171.

5.2 Перечень дополнительной литературы

1. Защита информации : учеб. пособие / А.П. Жук, Е.П. Жук, О.М. Лепешкин, А.И. Тимошкин. - 2-е изд. - Москва : РИОР : ИНФРА-М, 2018. - 392 с. - (Высшее образование: Бакалавриат; Магистратура). — https://doi.org/10.12737/4868. - Текст : электронный. - URL: https://new.znanium.com/catalog/product/937469

2. Организационное и правовое обеспечение информационной безопасности : учебник и практикум для бакалавриата и магистратуры / Т. А. Полякова, А. А. Стрельцов, С. Г. Чубукова, В. А. Ниесов ; под редакцией Т. А. Поляковой, А. А. Стрельцова. — Москва : Издательство Юрайт, 2019. — 325 с. — (Бакалавр и магистр. Академический курс). — ISBN 978-5-534-03600-8. — Текст : электронный // ЭБС Юрайт [сайт]. — URL: https://biblio-online.ru/bcode/432966

3. Казарин, О. В. Надежность и безопасность программного обеспечения : учебное пособие для бакалавриата и магистратуры / О. В. Казарин, И. Б. Шубинский. — Москва : Издательство Юрайт, 2019. — 342 с. — (Бакалавр и магистр. Модуль). — ISBN 978-5-534-05142-1. — Текст : электронный // ЭБС Юрайт [сайт]. — URL: https://biblio-online.ru/bcode/441287

5.3 Программное обеспечение

1. Сетевой компьютерный класс, оснащенный современной техникой
2. Офисный программный пакет (например, Microsoft Office 2003 или более поздних версий).
3. Web-браузер Mozilla Firefox или Google Chrome
4. Экран для проектора

5.4 Электронные ресурсы

1. Открытый ПП SiLab.
2. Национальный открытый Университет «ИНТУИТ» www.intuit.ru
3. Энциклопедия Кругосвет. Универсальная научно-популярная онлайн-энциклопедия. www.krugosvet.ru
4. Электронная библиотека: https://biblio-online.ru/
5. Электронная библиотека: https://new.znanium.com/

6. МАТЕРИАЛЬНО-ТЕХНИЧЕСКОЕ ОБЕСПЕЧЕНИЕ УЧЕБНОЙ ДИСЦИПЛИНЫ (МОДУЛЯ)

№ п/п	Наименование оборудованных учебных кабинетов, лабораторий	Перечень оборудования и технических средств обучения
1	Лекционная аудитория	Персональный компьютер, мультимедийный проектор
2	Компьютерный класс	Персональные компьютеры (IBM PC-совместимые) под управлением ОС Microsoft Windows, компьютерная сеть, доступ в сеть Интернет. Интерактивная доска

7. ОЦЕНКА КОМПЕТЕНЦИЙ ПО ИЗУЧАЕМОЙ ДИСЦИПЛИНЕ

№	Критерии оценки	
	«незачтено»	**«зачтено»**
	ЗНАТЬ	
1	Студент не способен самостоятельно выделять главные положения в изученном материале дисциплины. Не знает основные понятия ИБ, анализ угроз., проблемы безопасности компьютерных сетей. Политика безопасности. Стандарты ИБ. Не знает принципы защиты информационных систем (ИС), криптографических методы защиты информации.	Студент самостоятельно выделяет главные положения в изученном материале. Знает основные понятия ИБ, анализ угроз, проблемы безопасности компьютерных сетей. Политика безопасности. Стандарты ИБ. Показывает глубокое знание и понимание принципов защиты информационных систем (ИС), криптографических методов защиты информации, знание стандартов шифрования электронная цифровая подписи,
	УМЕТЬ	
2	Студент испытывает затруднения при анализе угроз ИБ, политики безопасности ИС. Студент не умеет самостоятельно разрабатывать политику безопасности ИС	Студент умеет анализировать проблем безопасности компьютерных сетей. Политики безопасности. Стандарты ИБ. Студент умеет самостоятельно разрабатывать политику безопасности ИС,
	ВЛАДЕТЬ	
3	Студент не владеет навыками концептуально-понятийным аппаратом, научным языком и терминологией криптографических методов защиты текстовой информации стандартов шифрования, ЭЦП.	Студент владеет концептуально-понятийным аппаратом, научным языком и терминологией криптографических методов защиты текстовой информации. Стандартов шифрования, ЭЦП. Студент владеет знаниями всего изученного материала, владеет навыками

№	Критерии оценки			
	«неудовлетворительно»	**«удовлетворительно»**	**«хорошо»**	**«отлично»**
	ЗНАТЬ			
1	Студент не способен самостоятельно выделять главные положения в изученном	Студент усвоил основное содержание материала дисциплины, но имеет пробелы	Студент способен самостоятельно выделять главные положения в	Студент знает, понимает, выделяет главные положения в изученном материале и

	материале дисциплины. Не знает основные методы и средства решения стандартных задач профессиональной деятельности с учетом основных требований информационной безопасности, строение современных операционных систем; принципы функционирования современных ИС. Отсутствуют знания и понимание основ и методов обеспечения безопасности компьютерных сетей, политики безопасности, стандарты ИБ. принципы защиты информационных систем_	в усвоении материала. Имеет несистематизированные знания об основных методах и средствах решения стандартных задач профессиональной деятельности с учетом основных требований информационной безопасности, строение современных операционных систем; принципы функционирования современных ИС. Показывает поверхностное знание методов обеспечения безопасности компьютерных сетей, политики безопасности, стандарты ИБ. принципы защиты информационных систем	изученном материале. Знает основные методы и средства решения стандартных задач профессиональной деятельности с учетом основных требований информационной безопасности, строение современных операционных систем; принципы функционирования современных ИС. Показывает знание методов обеспечения безопасности компьютерных сетей, политики безопасности, стандарты ИБ, принципы защиты информационных систем.	способен дать краткую характеристику основным идеям проработанного материала дисциплины. Знает основные методы и средства решения стандартных задач профессиональной деятельности с учетом основных требований информационной безопасности, строение современных операционных систем; принципы функционирования современных ИС. Показывает глубокое знание и понимание основ и методов обеспечения безопасности компьютерных сетей, политики безопасности, стандарты ИБ. принципы защиты информационных систем, криптографические методы защиты информации. Знает архитектуру и функционирование систем управления ИБ в (ИС).
УМЕТЬ				
2	Студент не умеет решать задачи профессиональной деятельности на основе информационной культуры с применением информационно-	Студент испытывает затруднения решении задач профессиональной деятельности с учетом основных требований ИБ,	Студент умеет самостоятельно решать стандартные задачи профессиональной деятельности на основе информационной и	Студент умеет решать стандартные задачи профессиональной деятельности на основе информационной культуры с

	коммуникационных технологий и с учетом основных требований информационной безопасности. Не умеет проводить анализ защищенности ИС, обнаружение атак, защиту удаленного доступа, защиту от вирусов и спама.	Студент испытывает затруднения при проведении анализа защищенности ИС, обнаружении атак, защите удаленного доступа, защите от вирусов и спама	библиографической культуры с применением информационно-коммуникационных технологий и с учетом основных требований информационной безопасности. Студент может проводить анализ защищенности ИС, обнаружение атак, зашиту от вирусов и спама.	применением информационно-коммуникационных технологий и с учетом основных требований информационной безопасности. Умеет проводить анализ защищенности ИС, обнаружение атак, защиту удаленного доступа, защиту от вирусов и спама.
ВЛАДЕТЬ				
3	Студент не владеет навыками обеспечение безопасности ОС, управления ИБ в информационных системах (ИС). Не владеет знаниями об аудите и мониторинге безопасности (ИС). навыками управления безопасностью ИС, выявления сетевых атак путем анализа трафика., аудита информационной безопасности компьютерных систем	Студент владеет основными навыками обеспечение безопасности ОС, управления ИБ в информационных системах (ИС). Владеет знаниями об аудите и мониторинге безопасности (ИС).	Студент владеет знаниями всего изученного материала, владеет навыками обеспечение безопасности ОС, управления ИБ в информационных системах (ИС). (ИС). Навыками управления безопасностью ИС, выявления сетевых атак путем анализа трафика. Испытывает затруднения при проведении аудита информационной безопасности компьютерных систем	Студент владеет навыками обеспечение безопасности ОС, управления ИБ в информационных системах (ИС). Владеет знаниями об аудите и мониторинге безопасности (ИС). Навыками управления безопасностью ИС, выявления сетевых атак путем анализа трафика., аудита информационной безопасности компьютерных систем
	Компетенция или ее часть не сформирована	Компетенция или ее часть сформирована на базовом уровне	Компетенция или ее часть сформирована на среднем уровне	Компетенция или ее часть сформирована на высоком уровне

8. ОБРАЗОВАТЕЛЬНЫЕ ТЕХНОЛОГИИ

8.1. Интерактивные образовательные технологии, используемые в аудиторных занятиях и самостоятельной работе обучающихся – не предусмотрены.

9. ОЦЕНОЧНЫЕ СРЕДСТВА ДЛЯ ТЕКУЩЕГО КОНТРОЛЯ УСПЕВАЕМОСТИ И ПРОМЕЖУТОЧНОЙ АТТЕСТАЦИИ

9.1. Организация входного, текущего и промежуточного контроля обучения

Входное тестирование – не предусмотрено.
Текущий контроль – устный опрос, защита по практическим работам.
Промежуточная аттестация – зачет, экзамен.

9.2. Тематика рефератов, проектов, творческих заданий, эссе и т.п.

Не предусмотрено.

9.3. Курсовая работа

Не предусмотрено.

9.4. Вопросы к зачету

1. Основные понятия защиты информации и информационной безопасности
2. Анализ угроз информационной безопасности
3. Проблемы безопасности IP-сетей
4. Угрозы и уязвимости проводных корпоративных сетей
5. Угрозы и уязвимости беспроводных сетей
6. Способы обеспечения информационной безопасности
7. Основные понятия политики безопасности
8. Структура политики безопасности организации. Базовая политика безопасности. Специализированные политики безопасности. Процедуры безопасности
9. Роль стандартов информационной безопасности
10. Стандарты ISO/IEC 17799:2002 (BS 7799:2000)
11. Стандарт BSI
12. Международный стандарт ISO 15408 «Общие критерии безопасности информационных технологий»
13. Стандарты для беспроводных сетей
14. Стандарты информационной безопасности в Интернете
15. Отечественные стандарты безопасности информационных технологий
16. Основные понятия криптографической защиты информации
17. Симметричные криптосистемы шифрования
18. Асимметричные криптосистемы шифрования
19. Комбинированная криптосистема шифрования
20. Электронная цифровая подпись и функция хэширования
21. Управление криптоключами
22. Классификация криптографических алгоритмов
23. Симметричные алгоритмы шифрования. Блочные алгоритмы шифрования данных
24. Асимметричные криптоалгоритмы. Алгоритм шифрования RSA. Алгоритмы цифровой подписи
25. Аутентификация, авторизация и администрирование действий пользователей
26. Методы аутентификации, использующие пароли и PIN-коды

27. Строгая аутентификация
28. Биометрическая аутентификация пользователя
29. Угрозы безопасности ОС
30. Понятие защищенной ОС
31. Основные функции подсистемы защиты ОС
32. Идентификация, аутентификация и авторизация субъектов доступа
33. Разграничение доступа к объектам ОС
34. Аудит безопасности в ОС.

9.5. Вопросы к экзамену

1. Основные понятия защиты информации и информационной безопасности
2. Анализ угроз информационной безопасности
3. Анализ угроз сетевой безопасности.
4. Способы обеспечения информационной безопасности
5. Основные понятия политики безопасности.
6. Структура политики безопасности организации. Процедуры безопасности
7. Разработка политики безопасности.
8. Стандарты информационной безопасности
9. Основные понятия криптографической защиты информации
10. Симметричные криптосистемы шифрования
11. Асимметричные криптосистемы шифрования
12. Комбинированная криптосистема шифрования
13. Электронная цифровая подпись и функция хэширования
14. Управление криптоключами
15. Аутентификация, авторизация и администрирование действий пользователей
16. Безопасность КИС.
17. Безопасность облачных вычислений.
18. Обеспечение безопасности ОС.
19. Функции межсетевых экранов
20. Особенности функционирования
21. Схемы сетевой защиты на базе МЭ
22. Концепция построения виртуальных защищенных сетей VPN
23. VPN-решения для построения защищенных сетей
24. Протоколы формирования защищенных каналов на канальном уровне
25. Протоколы формирования защищенных каналов на сеансовом уровне
26. Защита беспроводных сетей
27. Архитектура средств безопасности IPSec. Защита передаваемых данных с помощью протоколов AH и ESP
28. Протокол управления криптоключами IKE
29. Основные схемы применения IPSec. Преимущества средств безопасности IPSec
30. Управление идентификацией и доступом
31. Организация защищенного удаленного доступа. Централизованный контроль удаленного доступа
32. Управление доступом по схеме однократного входа с авторизацией Single Sign-On (SSO)
33. Протокол Kerberos
34. Инфраструктура управления открытыми ключами PKI
35. Технология анализа защищенности
36. Технологии обнаружения атак
37. Компьютерные вирусы и проблемы антивирусной защиты.

38. Концепция адаптивного управления безопасностью

9.6. Контроль освоения компетенций

Вид контроля	**Контролируемые темы (разделы)**	**Компетенции, компоненты которых контролируются**
Устный опрос	*1,2,3,4,5*	*ОПК-3, ПК-7*
Отчет по практической работе	*2,3,4,5*	*ОПК-3, ПК-7*