ФЕДЕРАЛЬНОЕ ГОСУДАРСТВЕННОЕ БЮДЖЕТНОЕ ОБРАЗОВАТЕЛЬНОЕ УЧРЕЖДЕНИЕ ИНКЛЮЗИВНОГО ВЫСШЕГО ОБРАЗОВАНИЯ
«МОСКОВСКИЙ ГОСУДАРСТВЕННЫЙ ГУМАНИТАРНО ЭКОНОМИЧЕСКИЙ УНИВЕРСИТЕТ»

Факультет Прикладной математики и информатики
Кафедра Цифровых технологий

УТВЕРЖДАЮ
Проректор по учебно-методической работе
_____ Сахарчук Е.С.
«27» 04 2022г.

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ (МОДУЛЯ) КИБЕРПРЕСТУПНОСТЬ И КОМПЬЮТЕРНАЯ КРИМИНАЛИСТИКА

образовательная программа направления подготовки
09.04.03 "Прикладная информатика"
Б1.В.ДВ.02.02 «Дисциплины (модули)», Часть, формируемая участниками образовательных отношений, Дисциплины (модули) по выбору

Профиль подготовки
Прикладная информатика в информационной сфере

Квалификация (степень) выпускника:

Магистр

Форма обучения: очная

Курс 2 семестр 3

Москва 2022

Рабочая программа составлена на основании федерального государственного образовательного стандарта высшего образования направления 09.04.03 "Прикладная информатика", утвержденного приказом Министерства науки и высшего образования Российской Федерации № 916 от «19» сентября 2017 г.

Разработчик рабочей программы:
к.т.н., доцент кафедры цифровых технологий МГТЭУ
место работы, занимаемая должность

подпись	А.А. Белоглазов И.О. Фамилия	«14» 03 2022 г. Дата

Рабочая программа утверждена на заседании кафедры цифровых технологий
(протокол № 4 от «21» 03 2022 г.)

Декан факультета

«21» 03 2022 г. (дата)	(подпись)	Е.В. Петрунина (Ф.И.О.)

СОГЛАСОВАНО
Начальник
управления по социальной
работе

« » 2022 г. (дата)	(подпись)	(Ф.И.О.)

СОГЛАСОВАНО
Председатель
совета обучающихся

«14» 04 2022 г. (дата)	(подпись)	Корти Н. (Ф.И.О.)

Содержание

1. ОРГАНИЗАЦИОННО-МЕТОДИЧЕСКИЙ РАЗДЕЛ

1.1. Цель и задачи изучения учебной дисциплины (модуля)

Цель курса состоит в получении студентами прочных теоретических знаний и практических навыков в области проектирования систем обеспечения экологической безопасности.

Задачи дисциплины:

1) изучение методологических подходов и основных принципов расчетов и проектирования систем обеспечения безопасности, основ проектирования сооружений для очистки воздуха, сточных вод, переработки техногенных отходов;

2) освоение применения основных принципов создания систем экологической безопасности в профессиональной деятельности, выполнения расчетов основных технологических параметров систем обеспечения экологической безопасности техногенных объектов;

3) получение навыков использования методов фундаментальных и прикладных естественно-научных дисциплин в профессиональной деятельности.

Требования к результатам освоения дисциплины

Код и наименование компетенции	Код и наименование индикатора достижения компетенции
ПК-3 Способен разрабатывать и применять математические методы, системное и прикладное программное обеспечение для решения задач проектной деятельности	ПК-3.1. Знает языки программирования, библиотеки и пакеты программ; современные методы цифровой обработки изображений и средства компьютерной обработки информации.
	ПК-3.2. Умеет анализировать поставленную задачу и находить алгоритм ее решения; выбирать оптимальные системы программирования, наиболее подходящие для решения поставленной задачи.
	ПК-3.3. Владеет методами моделирования информационных процессов; навыками работы над проектом в составе группы научных специалистов.
ПК-7 Способен проектировать архитектуру ИС предприятий и организаций в прикладной области	ПК-7.1 Знает процесс подготовки информации к принятию управленческих решений систему сбора, обработки и подготовки информации по предприятию и его структурным подразделениям; виды и особенности архитектур и сервисов ИС предприятий и организаций в прикладной области; методы оценки экономической эффективности и качества информационных систем, в т.ч. для учета проектных рисков.
	ПК-7.2 Умеет формировать общий бюджет предприятия в разрезе его составных частей; подготовить релевантную информацию для принятия управленческого решения; выбирать методология и технологию проектирования архитектуры и сервисов информационной системы предприятий и организаций в прикладной области.
	ПК-7.3 Владеет навыками использования современных инструментальных средств при разработке ИС различного назначения; практическими навыками проектирования архитектуры информационных систем и сервисов на основе современных методов и технологий; навыками интегрирования компонентов и сервисов информационных систем; практическими навыками использования современных инструментальных средств, применяемых на стадиях жизненного цикла информационных систем различных классов.

ПК-9 Способен принимать эффективные проектные решения в условиях неопределенности и риска	ПК-9.1 Знает принципы, методы, положения, определения эффективности проектных решений в условиях неопределенности и риска; возможности современных инструментальных средств для анализа, моделирования, оценки информационных процессов предприятий прикладной области в условиях неопределенности и риска.
	ПК-9.2 Умеет решений в условиях неопределенности и риска; правильно использовать возможности современных инструментальных средств для анализа, моделирования, оценки информационных процессов предприятий прикладной области в условиях неопределенности и риска.
	ПК-9.3 Владеет навыками принятия эффективных проектных решений на основе приобретенных знаний и умений и их применения в условиях неопределенности и риска; навыками использования современных инструментальных средств при моделировании, оценке и оптимизации информационных процессов предприятий прикладной области; русскоязычной и англоязычной терминологией методов, моделей, инструментария в сфере информационных технологий.

1.2. **Место дисциплины (модуля) в структуре образовательной программы направления подготовки 09.04.03 «Прикладная информатика (уровень магистратуры)»**

Для успешного освоения дисциплины студент должен иметь базовую подготовку по информатике и математике в пределах программы средней школы, а также дисциплины младших курсов, такие как

- Математический анализ
- Теория вероятностей и математическая статистика
- Информационные операции и атаки в распределенных информационных системах

Дисциплины и практики, для которых освоение данной дисциплины (модуля) необходимо как предшествующее

- Разработка и эксплуатация защищенных автоматизированных систем
- Методы проектирования защищенных распределенных информационных систем
- Управление рисками в распределенных информационных системах

2. СТРУКТУРА И СОДЕРЖАНИЕ ДИСЦИПЛИНЫ

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

Объем дисциплины «Киберпреступность и компьютерная криминалистика» составляет 5 зачетных единиц/180 часов:

Вид учебной работы	Всего, часов	Очная форма
		Курс, часов
		2 курс, 3 сем.
Аудиторная работа обучающихся с преподавателем (по видам учебных занятий), всего в том числе:	*48*	*48*
Лекции	14	14
Практические занятия	34	34
Лабораторные занятия		
Самостоятельная работа обучающихся	132	132
Промежуточная аттестация (подготовка и сдача), всего:		
Контрольная работа		
Курсовая работа		
Зачет с оценкой	5	5

Экзамен		
Итого: Общая трудоемкость учебной дисциплины (в часах, зачетных единицах)	180\5	180\5

2.2. Содержание дисциплины по темам (разделам)

№ п/п	Наименование раздела (темы)	Содержание раздела (тематика занятий)	Формируемые компетенции (индекс)
1.	Основы криминалистики	Понятие, предмет и задачи криминалистики. Система криминалистики. Понятие и научные основы криминалистической идентификации. Криминалистическая диагностика. Предмет, система и задачи трасологии. Научные основы трасологии. Общие положения организации раскрытия и расследования преступлений.	ПК-3, ПК-7, ПК-9
2.	Объекты компьютерной криминалистики	Классификация информационных ресурсов, характеристика и основные свойства. Информационные ресурсы в современных условиях, требования к ним, надежность (достоверность) информации и защиты от несанкционированного доступа.	ПК-3, ПК-7, ПК-9
3.	Аппаратнокомпьютерная и программнокомпьютерная экспертизы	Криминалистическая характеристика компьютерных преступлений. Основные группы компьютерных преступлений. Виды компьютерно-технической экспертизы.	ПК-3, ПК-7, ПК-9
4.	Информационнокомпьтерная и компьютерно-сетевая экспертизы	Объект, предмет и основные задачи информационнокомпьютерной экспертизы. Основные вопросы, ставящиеся, перед экспертом для проведения информационно-компьютерной экспертизы. Объект, предмет и основные задачи компьютерно-сетевой экспертизы. Компьютерно-сетевая экспертиза как вид компьютернотехнических исследований.	ПК-3, ПК-7, ПК-9

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.	Основы криминалистики	2	2	33	72	Устный опрос
2.	Объекты компьютерной криминалистики	2	4	33	72	Устный опрос

3.	Аппаратнокомпьютерная и программнокомпьютерная экспертизы	4	14	33		Устный опрос
4.	Информационнокомпьтерная и компьютерно-сетевая экспертизы	6	14	33		Устный опрос
Зачет		5				
	Итого:	14	34	132	180\5	

Тема лекции. Вопросы, отрабатываемые на лекции	**Всего часов**
Лекция 1. Основы криминалистики.	2
Лекция 2 Объекты компьютерной криминалистики.	2
Лекция 3. Аппаратнокомпьютерная и программнокомпьютерная экспертизы	4
Лекция 4. Информационнокомпьтерная и компьютерно-сетевая экспертизы	6

2.4. Планы теоретических (лекционных) занятий

2.5. Планы практических (семинарских) занятий

Тема практического занятия. Вопросы, отрабатываемые на практическом занятии	**Всего часов**
Классификация криптографических методов	5
Асимметричные криптосистемы.	5
«Аппаратно-программные решения защиты информации в информационных системах»	7
«Математические методы обеспечения защиты от несанкционирован-ного доступа и конфиденциальности»	7
Разработка матрицы конфликтного взаимодействия для типовых ТКС.	5
«Криптография и криптоанализ в авторизации, аутентификации и в обмене информации»	5

2.6. Планы лабораторных работ – не предусмотрено.

Задания, вопросы, для самостоятельного изучения (задания)	**Всего Часов**
Характеристика и возможности оптических, акустических радиоэлектронных и материально-вещественных каналов утечки информации.	17
Основные параметры системы защиты информации.	17
Архитектура системы защиты информации (СЗИ). Этапы создания СЗИ. Виды обеспечения СЗИ. Принципы разработки СЗИ.	17
«Информационная безопасность в глобальном информационном пространстве Интернет.	17
Серверы доступа (брандмауэры) Cisco ASA5500. Средства обнаружения вторжений IDS 4200	17
Безопасная интеграция в Интернет. Программные и технологические решения»	17

3. ОСОБЕННОСТИ ОБУЧЕНИЯ ЛИЦ С ИНВАЛИДНОСТЬЮ И ОВЗ

В случае необходимости, обучающимся из числа лиц с ограниченными возможностями здоровья (по заявлению обучающегося) могут предлагаться следующих варианты восприятия учебной информации с учетом их индивидуальных психофизических особенностей, в том числе с применением электронного обучения и дистанционных технологий:

1) для лиц с нарушениями зрения: в печатной форме увеличенным шрифтом; в форме электронного документа; в форме аудиофайла (перевод учебных материалов в

аудиоформат); индивидуальные консультации с привлечением сурдопереводчика; индивидуальные задания и консультации.

2) для лиц с нарушениями слуха: в печатной форме; в форме электронного документа; видеоматериалы с субтитрами; индивидуальные консультации с привлечением сурдопереводчика; индивидуальные задания и консультации.

3) для лиц с нарушениями опорно-двигательного аппарата: в печатной форме; в форме электронного документа; в форме аудиофайла; индивидуальные задания и консультации

4. УЧЕБНО-МЕТОДИЧЕСКОЕ ОБЕСПЕЧЕНИЕ САМОСТОЯТЕЛЬНОЙ РАБОТЫ ОБУЧАЮЩИХСЯ

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

В распоряжении преподавателей и обучающихся имеется основное необходимое материально-техническое оборудование, Интернет-ресурсы, доступ к полнотекстовым электронным базам, книжный фонд библиотеки Московского государственного гуманитарно-экономического университета.

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

5.1 Перечень основной литературы

1. Галатенко, Владимир Антонович.и Основы информационной безопасности : учеб. пособие для студентов вузов, обуч. по специальности 351400 "Прикл.информ." / Галатенко, Владимир Антонович. - 4-е изд. - М. : Изд-во Интернет-Ун-та Информ. Технологий: БИНОМ. Лаб. знаний, 2016, 2008, 2006. - 205 с. - (Основы информационных технологий). - Рекомендовано УМО. - ISBN 978-5-94774-821-5 :230-00.Местонахождение: Университетская библиотека ONLINE, IPRbooks URL:http://biblioclub.ru/index.php?page=book&id=233063, http://www.iprbookshop.ru/52209.html

2. Мельников, Владимир Павлович. Информационная безопасность и защита информации : учеб. пособие для студентов вузов, обуч. по специальности "Информ. системы и технологии" / Мельников, Владимир Павлович, С. А. Клейменов ; под ред. С.А.Клейменова. - 5-е изд., стер. - М. : Академия, 2011, 2010. - 330,[6] с. - (Высшее профессиональное образование. Информатика и вычислительная техника). - Допущено УМО. - ISBN 978-5-7695-7738-3 : 401-06. Местонахождение: Научная библиотека ДГУ

3. Бабаш, Александр Владимирович. Информационная безопасность : лаб. практикум; учеб. пособие / Бабаш, Александр Владимирович, Е. К. Баранов. - 2-е изд., стер. - И. : Кнорус, 2016, 2011. - 306-00. Местонахождение: Университетская библиотека ONLINE URL: http://biblioclub.ru/index.php?page=book&id=90539 (Дата обращения 10.12.2017 г).

4. Сергеева, Ю.С.Защита информации. : Конспект лекций. Учебное пособие / Ю. С. Сергеева ; Сергеева Ю. С. - М. : А-Приор, 2011. - 128. - (Конспект лекций). - ISBN 978-5-384-00397-7. Местонахождение: Российская государственная библиотека (РГБ) URL: http://нэб.рф/catalog/000199_000009_006559182

5. Прохорова, О.В. Информационная безопасность и защита информации : учебник / О.В. Прохорова ; Министерство образования и науки РФ, Федеральное государственное бюджетное образовательное учреждение высшего профессионального образования «Самарский государственный архитектурно-строительный университет». - Самара : Самарский государственный архитектурно-строительный университет, 2014. - 113 с. : табл., схем., ил. - Библиогр. в кн. - ISBN 978-5-9585-0603-3 ; То же [Электронный ресурс]. - URL: http://biblioclub.ru/index.php?page=book&id=438331

6. Инструментальный контроль и защита информации : учебное пособие / Н.А. Свинарев, О.В. Ланкин, А.П. Данилкин и др. ; Министерство образования и науки РФ, ФГБОУ ВПО «Воронежский государственный университет инженерных технологий». - Воронеж : Воронежский государственный университет инженерных технологий, 2013. - 192 с. : табл., ил. - Библиогр. в кн. - ISBN 978-5-00032-018-1 ; То же [Электронный ресурс]. - URL: http://biblioclub.ru/index.php?page=book&id=255905

7. Бурькова, Е.В. Физическая защита объектов информатизации : учебное пособие / Е.В. Бурькова ; Министерство образования и науки Российской Федерации, Оренбургский Государственный Университет, Кафедра вычислительной техники и защиты информации. - Оренбург : Оренбургский государственный университет, 2017. - 158 с. : табл., схем. - Библиогр. в кн. - ISBN 978-5-7410-1697-8 ; То же [Электронный

ресурс]. - URL: http://biblioclub.ru/index.php?page=book&id=481730

Перечень дополнительной литературы

1. Алешников С.И. Математические методы защиты информации. Часть 4. Вычислительный практикум по эллиптическим кривым и криптографии на эллиптических кривых [Электронный ресурс] : практическое пособие / С.И. Алешников, Ю.Ф. Болтнев. — Электрон. текстовые данные. — Калининград: Балтийский федеральный университет им. Иммануила Канта, 2007. — 58 с. — 978-588874-803-9. — Режим доступа: http://www.iprbookshop.ru/23795.html

2. Алешников С.И. Математические методы защиты информации. Часть 5. Методы алгебраических кривых [Электронный ресурс] : учебное пособие / С.И. Алешников, Е.С. Алексеенко. — Электрон. текстовые данные. — Калининград: Балтийский федеральный университет им. Иммануила Канта, 2010. — 158 с. — 9785- 9971-0073-5. — Режим доступа: http://www.iprbookshop.ru/23796.html

3. Алешников С.И. Математические методы защиты информации. Часть 3. Вычислительный практикум по числовым полям и криптографии в квадратичных полях [Электронный ресурс] : практическое пособие / С.И. Алешников, Е.В. Козьминых. — Электрон. текстовые данные. — Калининград: Балтийский федеральный университет им. Иммануила Канта, 2006. — 97 с. — 588874-689-4. — Режим доступа: http://www.iprbookshop.ru/23851.html

4. Бескид П.П. Криптографические методы защиты информации. Часть 2. Алгоритмы, методы и средства обеспечения конфиденциальности, подлинности и целостности информации [Электронный ресурс] : учебное пособие / П.П. Бескид, Т.М. Тагарникова. — Электрон. текстовые данные. — СПб. : Российский государственный гидрометеорологический университет, 2010. — 104 с. — 2227-8397. — Режим доступа: http://www.iprbookshop.ru/17926.html

Программное обеспечение

Текстовый редактор
Microsoft Windows
Microsoft Office
7-Zip
AcrobatReader

5.4. Электронные ресурсы

1. Федеральная служба по техническому и экспортному контролю (ФСТЭК России) www.fstec.ru

2. Информационно-справочная система по документам в области технической защиты информации www.fstec.ru

3. Образовательные порталы по различным направлениям образования и тематике http://depobr.gov35.ru/

4. Справочно-правовая система «Консультант Плюс» www.consultant.ru

5. Справочно-правовая система «Гарант» » www.garant.ru

6. Федеральный портал «Российское образование www.edu.ru

7. Федеральный правовой портал «Юридическая Россия» http://www.law.edu.ru/

8. Российский биометрический портал www.biometrics.ru

9. Федеральный портал «Информационно- коммуникационные технологии в образовании» htpp\\:www.ict.edu.ru

10. Сайт Научной электронной библиотеки www.elibrary.ru

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

7. ОЦЕНКА КОМПЕТЕНЦИЙ ПО ИЗУЧАЕМОЙ ДИСЦИПЛИНЕ

№	**Критерии оценки**			
	«неудовлетворительно»	**«удовлетворительно»**	**«хорошо»**	**«отлично»**
	ЗНАТЬ			
1	Студент не усвоил следующие знания: правовую и нормативную базу корпоративных информационных систем отраслей; информационную структуру и информационные ресурсы сетей отраслей как объекта защиты;	Студент усвоил основное содержание материала дисциплины, но имеет пробелы в усвоении материала. Имеет несистематизированные знания по темам: основные устройства и системы защиты объектов и информации; основные типы методов, устройств и систем технической	Студент способен самостоятельно выделять главные положения в изученном материале. Знает: правовую и нормативную базу корпоративных информационных систем отраслей; информационную структуру и информационные ресурсы сетей отраслей как объекта	Студент усвоил основное содержание материала дисциплины :правовую и нормативную базу корпоративных информационных систем отраслей; информационную структуру и информационные ресурсы сетей отраслей как объекта защиты; основные

		разведки; методы защиты автоматизированных систем обработки данных от несанкционированного доступа к информации, в том числе: специальные технические средства опознавания пользователя ПЭВМ;	защиты; основные устройства и системы защиты объектов и информации; основные типы методов, устройств и систем технической разведки; методы защиты автоматизированных систем обработки данных от несанкционированного доступа к информации, в том числе: специальные технические средства опознавания пользователя ПЭВМ; специальное программное обеспечение по защите информации ПЭВМ;	устройства и системы защиты объектов и информации; основные типы методов, устройств и систем технической разведки; методы защиты автоматизированных систем обработки данных от несанкционированного доступа к информации, в том числе: специальные технические средства опознавания пользователя ПЭВМ; специальное программное обеспечение по защите информации ПЭВМ; основные типы методов, устройств и систем технической разведки;
УМЕТЬ				
2	Студент не умеет создавать простейшие статические webдокуграфическом многооконном режиме, так и в режиме командной строки (консоли); использовать уровни защиты информации; использовать криптографические методы защиты информации;	Студент испытывает затруднения при использовании уровней защиты информации; использовании криптографических методов защиты информации; Не умеет: использовать протоколы взаимной аутентификации объектов сетей; использовать методы организации систем защиты информации ;	Студент умеет использовать уровни защиты информации; использовать криптографические методы защиты информации; использовать протоколы взаимной аутентификации объектов сетей; использовать методы организации систем защиты информации ; применять современные	Студент умеет использовать уровни защиты информации; использовать криптографические методы защиты информации; использовать протоколы взаимной аутентификации объектов сетей; использовать методы организации систем защиты информации ; применять современные

		применять современные системные программные средства, технологии и инструментальные средства;	системные программные средства, технологии и инструментальные средства;	системные программные средства, технологии и инструментальные средства; - размещать сценарии PHP на HTML - странице; - использовать графические программы для создания чертежей структуры web - сайта; - использовать графические редакторы для обработки изображений, размещаемых на web -сайте
ВЛАДЕТЬ				
3	Студент не владеет следующими знаниями: DataGridView; навыками работы с межсетевыми экранами и пакетами антивирусных программ; навыками самостоятельного проектирования систем защиты информации.	Студент владеет DataGridView; навыками работы с межсетевыми экранами и пакетами антивирусных программ; навыками самостоятельного проектирования систем защиты информации.	Студент владеет DataGridView; навыками работы с межсетевыми экранами и пакетами антивирусных программ; навыками самостоятельного проектирования систем защиты информации. с техническими средствами разведки, защиты информации и противодействия коммерческой разведке; - навыками работы в системе Windows;	Студент владеет DataGridView; навыками работы с межсетевыми экранами и пакетами антивирусных программ; навыками самостоятельного проектирования систем защиты информации. с техническими средствами разведки, защиты информации и противодействия коммерческой разведке; - навыками работы в системе Windows; навыками разработки статических и динамических страниц сети Internet - навыками программирования

				на языке PHP
	Компетенции или их части не сформированы.	Компетенции или их части сформированы на базовом уровне.	Компетенции или их части сформированы на среднем уровне.	Компетенции или их части сформированы на высоком уровне.

8. ОБРАЗОВАТЕЛЬНЫЕ ТЕХНОЛОГИИ

Интерактивные образовательные технологии, используемые в аудиторных занятиях и самостоятельной работе обучающихся

Семестр	Вид занятия (Л, ПР, ЛР)	Используемые интерактивные образовательные технологии	Количество часов
3	Л	Лекция-беседа, ТСО (мультимедийный проектор, презентации PowerPoint)	14
	ПР	Практикум на ЭВМ, проблемный метод, взаимообучение	34
	ЛР	Не предусмотрены	
	КР	Устный опрос	
	Сам.работа	ЭБС, дистанционные консультации, взаимообучение в студенческой среде	132
Итого:			180

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 отчетов по практическим работам, работа на компьютерах в парах, презентация в режиме диалога, работа в парах.

Промежуточная аттестация – зачет с оценкой.

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

Не предусмотрены.

9.3. Курсовая работа

Не предусмотрено.

9.4. Вопросы к экзамену

1. Понятие информации и информационной безопасности.
2. Информация, сообщения, информационные процессы как объекты информационной безопасности.

3. Обзор защищаемых объектов и систем.
4. Понятие «угроза информации». Понятие «риска информационной безопасности».
5. Примеры преступлений в сфере информации и информационных технологий.
6. Сущность функционирования системы защиты информации.
7. Защита человека от опасной информации и от неинформированности в области информационной безопасности.
8. Целостность, доступность и конфиденциальность информации.
9. Классификация информации по видам тайны и степеням конфиденциальности.
10. Понятия государственной тайны и конфиденциальной информации.
11. Жизненные циклы конфиденциальной информации в процессе ее создания,
обработки, передачи.
12. Цели и задачи защиты информации.
13. Основные понятия в области защиты информации.
14. Элементы процесса менеджмента ИБ.
15. Модель интеграции информационной безопасности в основную деятельность организации.
16. Понятие Политики безопасности.
17. Понятие угрозы безопасности информации
18. Системная классификация угроз безопасности информации
19. Каналы и методы несанкционированного доступа к информации
20. Уязвимости. Методы оценки уязвимости информации
21. Анализ существующих методик определения требований к защите информации
22. Параметры защищаемой информации и оценка факторов, влияющих на требуемый уровень защиты информации
23. Виды мер и основные принципы защиты информации
24. Организационная структура системы защиты информации
25. Законодательные акты в области защиты информации
26. Российские и международные стандарты, определяющие требования к защите информации
27. Система сертификации РФ в области защиты информации. Основные правила и документы системы сертификации РФ в области защиты информации
28. Основные механизмы защиты информации.
29. Система защиты информации.
30. Меры защиты информации, реализуемые в автоматизированных (информационных) системах
31. Программные и программно-аппаратные средства защиты информации
32. Инженерная защита и техническая охрана объектов информатизации
33. Организационно-распорядительная защита информации. Работа с кадрами и
внутриобъектовый режим.

34. Принципы построения организационно-распорядительной системы

9.6. Контроль освоения компетенций

Вид контроля	**Контролируемые темы (разделы)**	**Компетенции, компоненты которых контролируются**
Устный опрос	*1-4*	ПК-3,ПК-7,ПК-8

ЛИСТ РЕГИСТРАЦИИ ИЗМЕНЕНИЙ

№ п/п	Номер и дата протокола заседания кафедры	Перечень измененных пунктов	Подпись заведующего кафедрой