МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ РОССИЙСКОЙ ФЕДЕРАЦИИ
Федеральное государственное бюджетное образовательное
учреждение инклюзивного высшего образования

**«Российский государственный
университет социальных технологий»**

(ФГБОУ ИВО «РГУ СоцТех»)

УТВЕРЖДАЮ

Проректор по образовательной деятельности

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ (МОДУЛЯ)
Проектирование систем обеспечения информационной безопасности
образовательная программа направления подготовки
09.04.03 «Прикладная информатика»
Б1.В.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 2024

Содержание

1. **ОРГАНИЗАЦИОННО-МЕТОДИЧЕСКИЙ РАЗДЕЛ**
2. **СТРУКТУРА И СОДЕРЖАНИЕ ДИСЦИПЛИНЫ (МОДУЛЯ)**
3. **ОСОБЕННОСТИ ОБУЧЕНИЯ ИНВАЛИДОВ И ЛИЦ С ОВЗ**
4. **УЧЕБНО-МЕТОДИЧЕСКОЕ ОБЕСПЕЧЕНИЕ САМОСТОЯТЕЛЬНОЙ РАБОТЫ ОБУЧАЮЩИХСЯ**
5. **ОБРАЗОВАТЕЛЬНЫЕ ТЕХНОЛОГИИ**
6. **ОЦЕНОЧНЫЕ СРЕДСТВА ДЛЯ ТЕКУЩЕГО КОНТРОЛЯ УСПЕВАЕМОСТИ И ПРОМЕЖУТОЧНОЙ АТТЕСТАЦИИ**
7. **УЧЕБНО-МЕТОДИЧЕСКОЕ И ИНФОРМАЦИОННОЕ ОБЕСПЕЧЕНИЕ УЧЕБНОЙ ДИСЦИПЛИНЫ (МОДУЛЯ)**
8. **МАТЕРИАЛЬНО-ТЕХНИЧЕСКОЕ ОБЕСПЕЧЕНИЕ УЧЕБНОЙ ДИСЦИПЛИНЫ (МОДУЛЯ)**

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-5 Способен исследовать применение различных научных подходов к автоматизации информационных процессов и информатизации предприятий и организаций	ПК-5.1 Знает различные научные подходы к автоматизации информационных процессов и информатизации предприятий и организаций; процесс подготовки информации к принятию управленческих решений; тенденции развития автоматизации управления промышленными предприятиями.
	ПК-5.2 Умеет провести алгоритмизацию конкретной управленческой задачи; применять различные научные подходы к автоматизации информационных процессов и информатизации предприятий и организаций.
	ПК-5.3 Владеет навыками применения типовых подходов, применяемых при анализе, планировании и оперативном управлении деятельностью промышленного предприятия; навыками исследования применения различных научных подходов к автоматизации информационных процессов и информатизации предприятий и организаций на основе приобретенных знаний и умений и их применения в нетипичных ситуациях.
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-8 Способен проектировать информационные процессы и системы с использованием инновационных инструментальных средств адаптировать современные ИКТ к задачам прикладных ИС	ПК-8.1 Знает принципы, методы, положения, определения проектирования информационных процессов и систем с использованием инновационных инструментальных средств; подходы и методы к проектированию информационных процессов и систем с использованием инновационных инструментальных средств; подходы к адаптации современных ИКТ к задачам прикладных ИС.
	ПК-8.2 Умеет разрабатывать, проектировать, тестировать, администрировать информационные процессы и системы с использованием инновационных инструментальных средств; принимать решения по информатизации предприятий и организаций прикладной области в условиях неопределенности и риска; интегрировать компоненты и сервисы информационных систем; проводить моделирование информационных систем; проектировать информационные системы.
	ПК-8.3 Владеет навыками адаптации современных ИКТ к задачам прикладных ИС на основе приобретенных знаний и умений и их применения в нетипичных ситуациях; практическими навыками проектирования информационных процессов и систем с использованием инновационных инструментальных средств; практическими навыками адаптации современных ИКТ к задачам прикладных ИС; навыками выбора технологии проектирования информационных систем.
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 принимать эффективные проектные решения 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
- Моделирование систем и процессов
- Методология и технология проектирования информационных систем
- Техническая защита информации

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

- Архитектура сетевой безопасности и управление процессом обеспечения безопасности

2. СТРУКТУРА И СОДЕРЖАНИЕ ДИСЦИПЛИНЫ

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

Объем дисциплины «Проектирование систем обеспечения информационной безопасности» составляет 4 зачетных единиц/144 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:	*42*	*42*
Лекции	8	8
Практические занятия	34	34
Лабораторные занятия		
Самостоятельная работа обучающихся	102	102
Промежуточная аттестация (подготовка и сдача), всего:		
Контрольная работа		
Курсовая работа		
Зачет	2	2
Экзамен		
Итого: Общая трудоемкость учебной дисциплины (в часах, зачетных единицах)	144\4	144\4

2.2. Содержание дисциплины по темам (разделам)

№ п/п	Наименование раздела (темы)	Содержание раздела (тематика занятий)	Формируемые компетенции (индекс)

1.	Основные принципы создания программно-аппаратных средств обеспечения информационной безопасности (ПАСОИБ)	Основные понятия и определения в области создания ПАСОИБ Нормативно-правовая база создания ПАСОИБ Классификация ПАСОИБ Функциональные возможности ПАСОИБ Принцип разработки ПАСОИБ Концепция диспетчера доступа Основные этапы проектирования ПАСОИБ	ПК-5,ПК-7,ПК-8,ПК-9
2.	Основные методы и средства реализации отдельных функциональных требований по защите информации и данных	Классификация функциональных требований по защите информации и данных Методы обеспечения идентификации и аутентификации Методы криптографической защиты Методы и средства хранения ключевой информации Методы и средства ограничения доступа к компонентам информационных систем Методы аудита безопасности Методы обеспечения целостности системы защиты	ПК-5,ПК-7,ПК-8,ПК-9
3	Аппаратно-программные решения защиты информации в информационных системах	Классификация аппаратных средств защиты программ Классификация программных средств защиты программ Структура ПО Способы встраивания средств защиты в ПО Способы определения незаконного использования ПО Основные принципы обеспечения безопасности программ	ПК-5,ПК-7,ПК-8,ПК-9
4	Программно-аппаратные средства защиты информации в сетях передачи данных	Информационная безопасность в глобальном информационном пространстве Интернет. Безопасная интеграция в Интернет. Программные и технологические решения Классификация программно-аппаратных средств защиты информации в сетях передачи данных Принципы построения и функционирования межсетевых экранов Основные принципы защиты информации при передаче по каналам связи	ПК-5,ПК-7,ПК-8,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.	Основные принципы создания программно-аппаратных средств обеспечения информационной безопасности (ПАСОИБ)	2	8	24	24	Устный опрос
2.	Основные методы и средства реализации отдельных функциональных требований по	2	10	26	38	Устный опрос

	защите информации и данных					
3.	Архитектура системы защиты информации (СЗИ). Этапы создания СЗИ. Виды обеспечения СЗИ. Принципы разработки СЗИ.			13	13	Устный опрос
4.	Аппаратно-программные решения защиты информации в информационных системах	2	8	13	23	Устный опрос
5.	Программно-аппаратные средства защиты информации в сетях передачи данных	2	8	26	36	Устный опрос
Зачет		2				
	Итого:	8	34	102	144\4	

2.4. Планы теоретических (лекционных) занятий

Тема лекции. Вопросы, отрабатываемые на лекции	**Всего часов**
Лекция 1. Основные принципы создания программно-аппаратных средств обеспечения информационной безопасности (ПАСОИБ) План-вопросы • Основные понятия и определения в области создания ПАСОИБ • Нормативно-правовая база создания ПАСОИБ • Классификация ПАСОИБ • Функциональные возможности ПАСОИБ	2
Лекция 2 Основные методы и средства реализации отдельных функциональных требований по защите информации и данных. План – вопросы • Классификация функциональных требований по защите информации и данных • Методы обеспечения целостности системы защиты	2
Лекция 3. Аппаратно-программные решения защиты информации в информационных системах План-вопросы • Классификация аппаратных средств защиты программ • Классификация программных средств защиты программ	2
Лекция 4. . Программно-аппаратные средства защиты информации в сетях передачи данных План-вопросы • Информационная безопасность в глобальном информационном пространстве Интернет. Безопасная интеграция в Интернет. Программные и технологические решения • Классификация программно-аппаратных средств защиты информации в сетях передачи данных • Основные принципы защиты информации при передаче по каналам связи	2

2.5. Планы практических (семинарских) занятий

Тема практического занятия. Вопросы, отрабатываемые на практическом занятии	Всего часов
Основные принципы создания программно-аппаратных средств обеспечения информационной безопасности (ПАСОИБ) - Принцип разработки ПАСОИБ - Концепция диспетчера доступа - Основные этапы проектирования ПАСОИБ	8
Основные методы и средства реализации отдельных функциональных требований по защите информации и данных - Методы обеспечения идентификации и аутентификации - Методы криптографической защиты - Методы и средства хранения ключевой информации - Методы и средства ограничения доступа к компонентам информационных систем - Методы аудита безопасности	10
Аппаратно-программные решения защиты информации в информационных системах - Способы встраивания средств защиты в ПО - Способы определения незаконного использования ПО - Основные принципы обеспечения безопасности программ	8
Программно-аппаратные средства защиты информации в сетях передачи данных - Принципы построения и функционирования межсетевых экранов - Разработка матрицы конфликтного взаимодействия для типовых ТКС - Криптография и криптоанализ в авторизации, аутентификации и в обмене информации	8

2.6. Планы лабораторных работ – не предусмотрено.

Задания, вопросы, для самостоятельного изучения (задания)	Всего часов
Основные принципы создания программно-аппаратных средств обеспечения информационной безопасности (ПАСОИБ)	24
Основные методы и средства реализации отдельных функциональных требований по защите информации и данных	26
Архитектура системы защиты информации (СЗИ). Этапы создания СЗИ. Виды обеспечения СЗИ. Принципы разработки СЗИ.	13
Аппаратно-программные решения защиты информации в информационных системах	13
Программно-аппаратные средства защиты информации в сетях передачи (Информационная безопасность в глобальном информационном пространстве Интернет. Серверы доступа (брандмауэры) Cisco ASA5500. Средства обнаружения вторжений IDS 4200 Безопасная интеграция в Интернет. Программные и технологические решения)	26

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. Конфликтно-активное управление проектами развития систем обеспечения информационной безопасности инфокоммуникационных сетей : монография / В.И. Новосельцев, С.С. Кочедыков, Д.Е. Орлова, К.А. Плющик ; под ред. В.И. Новосельцева. — Москва : ИНФРА-М, 2023. — 235 с. — (Научная мысль). — DOI 10.12737/1921360. - ISBN 978-5-16-018194-3. - Текст : электронный. - URL: https://znanium.com/catalog/product/1921360
2. Енютина, Т. А. Расчет и проектирование систем обеспечения безопасности : учебное пособие / Т. А. Енютина, Л. В. Кулагина. - Красноярск : Сибирский федеральный университет, 2022. - 190 с. - ISBN 978-5-7638-4599-0. - Текст : электронный. - URL: https://znanium.com/catalog/product/2092915
3. Расчет и проектирование систем обеспечения безопасности : учебное пособие / В. В. Коростовенко, Т. А. Стрекалова, В. А. Гронь, А. В. Галайко. - Красноярск : Сибирский федеральный университет, 2022. - 108 с. - ISBN 978-5-7638-4625-6. - Текст : электронный. - URL: https://znanium.com/catalog/product/2091877

5.2 Перечень дополнительной литературы

1. Царегородцев А.В. Анализ рисков в процессах обеспечения информационной безопасности жизненного цикла финансовых автоматизированных информационных систем – М.: ИНФРА-М, 2024 -198 с. https://znanium.ru/catalog/document?id=436066
2. Привалов, А. А. Обеспечение информационной безопасности, проектирования, создания, модернизации объектов информации на базе компьютерных систем в защищенном исполнении : учебно-методическое пособие к курсовой работе / А. А. Привалов. - Москва : РУТ (МИИТ), 2018. - 48 с. - Текст : электронный. - URL: https://znanium.com/catalog/product/1895288
3. Дербин, Е. А. Информационное противоборство: концептуальные основы обеспечения информационной безопасности : учебное пособие / Е.А. Дербин, А.В. Царегородцев. — Москва : ИНФРА-М, 2024. — 267 с. — (Высшее образование). — DOI 10.12737/2084342. - ISBN 978-5-16-019050-1. - Текст : электронный. - URL: https://znanium.ru/catalog/product/2084342

5.3. **Программное обеспечение**

Текстовый редактор
Microsoft Windows
Microsoft Office
7-Zip
AcrobatReader

5.3 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. Федеральный портал «Российское образование www.edu.ru
6. Федеральный правовой портал «Юридическая Россия» http://www.law.edu.ru/
7. Российский биометрический портал www.biometrics.ru
8. Федеральный портал «Информационно- коммуникационные технологии в образовании» htpp\\:www.ict.edu.ru
9. Сайт Научной электронной библиотеки www.elibrary.ru
10. Электронная библиотека «Знаниум»: https://znanium.com
11. Электронная библиотека «Юрайт»: https://urait.ru

12. Электронно-библиотечная система «Лань»: https://e.lanbook.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

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 разведки; методы защиты автоматизированных систем обработки данных от несанкционированного доступа к информации, в том числе: специальные технические средства	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 защиты; основные устройства и системы защиты объектов и информации; основные типы методов, устройств и систем технической разведки; методы защиты	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 устройства и системы защиты объектов и информации; основные типы методов, устройств и систем технической разведки; методы защиты автоматизированных

		опознавания пользователя ПЭВМ;	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;	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 ; применять современные системные программные средства, технологии и инструментальные средства;	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 системные программные средства, технологии и инструментальные средства;	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 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

1	Л	Лекция-беседа, ТСО (мультимедийный проектор, презентации PowerPoint)	8
	ПР	Практикум на ЭВМ, проблемный метод, взаимообучение	34
	ЛР	Не предусмотрены	
	КР	Устный опрос	
	Сам.работа	ЭБС, дистанционные консультации, взаимообучение в студенческой среде	102
Итого:			144

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

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

Не предусмотрены.

9.3. Курсовая работа

Не предусмотрено.

9.4. Вопросы к зачету

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. Информация ограниченного доступа, государственная тайна, конфиденциальная информация, санкционированный и несанкционированный доступ к информации
6. Информационная безопасность, конфиденциальность информации, доступность информации, целостность ресурса или компонента системы
7. Примеры преступлений в сфере информации и информационных технологий.
8. Сущность функционирования системы защиты информации.
9. Защита человека от опасной информации и от неинформированности в области информационной безопасности.
10. Целостность, доступность и конфиденциальность информации.
11. Классификация информации по видам тайны и степеням конфиденциальности.
12. Понятия государственной тайны и конфиденциальной информации.
13. Жизненные циклы конфиденциальной информации в процессе ее создания, обработки, передачи.
14. Цели и задачи защиты информации.

15. Основные понятия в области защиты информации.
16. Угрозы безопасности ИС. Непреднамеренное воздействие и атака на компьютерную систему.
17. Комплекс средств защиты информации.
18. Модель интеграции информационной безопасности в основную деятельность организации.
10. Понятие Политики безопасности.
11. Понятие угрозы безопасности информации
12. Системная классификация угроз безопасности информации
13. Каналы и методы несанкционированного доступа к информации
14. Уязвимости. Методы оценки уязвимости информации
15. Анализ существующих методик определения требований к защите информации
16. Параметры защищаемой информации и оценка факторов, влияющих на требуемый уровень защиты информации
17. Виды мер и основные принципы защиты информации
18. Организационная структура системы защиты информации
19. Законодательные акты в области защиты информации
20. Российские и международные стандарты, определяющие требования к
21. защите информации
22. Основные механизмы защиты информации.
23. Меры защиты информации, реализуемые в автоматизированных (информационных) системах
24. Программные и программно-аппаратные средства защиты информации
25. Инженерная защита и техническая охрана объектов информатизации
26. Организационно-распорядительная защита информации. Работа с кадрами и внутри объектовый режим.
27. Методы криптографической защиты
28. Методы аудита безопасности
29. Архитектура системы защиты информации (СЗИ). Этапы создания СЗИ. Виды обеспечения СЗИ. Принципы разработки СЗИ.
30. Принципы построения и функционирования межсетевых экранов
31. Матрица конфликтного взаимодействия для типовых ТКС
32. Криптография и криптоанализ в авторизации, аутентификации и в обмене информации
33. Аппаратно-программные решения защиты информации в информационных системах

9.6. Контроль освоения компетенций

Вид контроля	**Контролируемые темы (разделы)**	**Компетенции, компоненты которых контролируются**
Устный опрос	*1-4*	ПК-5,ПК-7,ПК-8,ПК-9

1.

ЛИСТ РЕГИСТРАЦИИ ИЗМЕНЕНИЙ

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