МИНИСТЕРСТВО ОБРАЗОВАНИЯ И НАУКИ РОССИЙСКОЙ ФЕДЕРАЦИИ
Федеральное государственное бюджетное образовательное учреждение
высшего образования
«Чувашский государственный университет имени И. Н. Ульянова»

Факультет информатики и вычислительной техники

Кафедра математического и аппаратного обеспечения информационных систем

«УТВЕРЖДАЮ»
Проректор по учебной работе

_____ И.Е. Поверинов

31 августа 2017 г.

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ
«РАЗРАБОТКА И ЭКСПЛУАТАЦИЯ ЗАЩИЩЕННЫХ АВТОМАТИЗИРОВАННЫХ СИСТЕМ»

Специальность 10.05.03 «Информационная безопасность автоматизированных систем»

Квалификация (степень) выпускника Специалист по защите информации

Специализация Безопасность открытых информационных систем

Чебоксары – 2017

Рабочая программа основана на требованиях Федерального государственного образовательного стандарта высшего образования по специальности 10.05.03 «Информационная безопасность автоматизированных систем» (специализация «Безопасность открытых информационных систем»), утвержденного приказом Министерства образования и науки 01.12.2016 г. №1509

СОСТАВИТЕЛЬ (СОСТАВИТЕЛИ):

Доцент _____ В.П. Филиппов

ОБСУЖДЕНО:
на заседании кафедры математического и аппаратного обеспечения информационных систем 30.08.2017 г., протокол № 1

заведующий кафедрой _____ Д.В. Ильин

СОГЛАСОВАНО:
Методическая комиссия факультета информатики и вычислительной техники
«30» августа 2017г., протокол №1

Декан факультета _____ А.В. Щипцова

Директор научной библиотеки _____ Н.Д. Никитина

Начальник управления информатизации _____ И.П. Пивоваров

Начальник учебно-методического управления _____ В.И. Маколов

Оглавление

1. Цель и задачи обучения по дисциплине

Цель дисциплины изучение основных понятий, методологии и практических приемов проектирования, разработки и внедрения автоматизированных систем на предприятиях различных отраслей промышленности с учетом требований по обеспечению информационной безопасности.

Задачи дисциплины:

- приобретение обучаемыми необходимого объема знаний и практических навыков в области стандартизации и нормотворчества в области защиты автоматизированных систем;
- формирование у обучаемых целостного представления об организации и содержании процессов проектирования, разработки, внедрения и эксплуатации автоматизированных систем (АС) в защищенном исполнении.

2. Место дисциплины в структуре основной образовательной программы (ООП)

Дисциплина «Разработка и эксплуатация защищенных автоматизированных систем» (РиЭЗАС) является дисциплиной базовой части.

Изучение дисциплины «Разработка и эксплуатация защищенных автоматизированных систем» основывается на базе знаний, умений и владений, полученных обучающимися в ходе освоения дисциплин: Безопасность сетей ЭВМ, Управление информационной безопасностью, Техническая защита информации, Безопасность систем баз данных.

РиЭЗАС является базовым теоретическим и практическим основанием прохождения производственных и преддипломной практик, государственной итоговой аттестации.

3. Перечень планируемых результатов обучения по дисциплине, соотнесенных с планируемыми результатами освоения ООП

Процесс обучения по дисциплине направлен на формирование следующих компетенций:

- способность к самоорганизации и самообразованию (ОК-8);
- способность применять языки, системы и инструментальные средства программирования в профессиональной деятельности (ОПК-3);
- способность применять нормативные правовые акты в профессиональной деятельности (ОПК-6);
- способность к освоению новых образцов программных, технических средств и информационных технологий (ОПК-8).
- способностью создавать и исследовать модели автоматизированных систем (ПК-2);
- способность проводить анализ защищенности автоматизированных систем (ПК-3);
- способность разрабатывать модели угроз и модели нарушителя информационной безопасности автоматизированной системы (ПК-4);
- способность проводить анализ рисков информационной безопасности автоматизированной системы (ПК-5);
- способность проводить анализ, предлагать и обосновывать выбор решений по обеспечению эффективного применения автоматизированных систем в сфере профессиональной деятельности (ПК-6);
- способность участвовать в разработке защищенных автоматизированных систем в сфере профессиональной деятельности (ПК-9);
- способность применять знания в области электроники и схемотехники, технологий, методов и языков программирования, технологий связи и передачи данных при разработке программно-аппаратных компонентов защищенных автоматизированных систем в сфере профессиональной деятельности (ПК-10);
- способность участвовать в проектировании системы управления информационной безопасностью автоматизированной системы (ПК-12);

- способность участвовать в проектировании средств защиты информации автоматизированной системы (ПК-13);
- способность организовать разработку, внедрение, эксплуатацию и сопровождение автоматизированной системы с учетом требований информационной безопасности (ПК-20);
- способность обеспечить эффективное применение информационно-технологических ресурсов автоматизированной системы с учетом требований информационной безопасности (ПК-24);
- способность обеспечить эффективное применение средств защиты информационно-технологических ресурсов автоматизированной системы и восстановление их работоспособности при возникновении нештатных ситуаций (ПК-25);
- способность администрировать подсистему информационной безопасности автоматизированной системы (ПК-26);

профессионально-специализированных компетенций

- способность участвовать в проектировании, эксплуатации и совершенствовании системы управления информационной безопасностью открытой информационной системы (ПСК-4.3);
- способность формировать и эффективно применять комплекс мер (правила, процедуры, практические приемы, руководящие принципы, методы, средства) для обеспечения информационной безопасности открытых информационных систем (ПСК-4.5);

В результате обучения по дисциплине, обучающийся должен (ЗУН):

знать:

основные стандарты и нормативные документы в области разработки автоматизированных систем в защищенном исполнении (З1);

общий порядок проектирования, разработки и внедрения, а также стадии жизненного цикла автоматизированных систем (З2);

языки, системы и инструментальные средств используемые для создания защищенных автоматизированных систем и средства защиты информации (З3);

основные угрозы безопасности информации и модели нарушителя в автоматизированных системах (З4);

модели и фреймворки используемых для описания открытых систем (З5);

модели угроз и модели нарушителя информационной безопасности автоматизированной системы (З6);

терминологию и принципы риск-менеджмента (З7);

международные стандарты и методологии в области проектирования и анализа защищенных автоматизированных систем (З8);

принципы проектирования средств защиты информации автоматизированной системы (З9);

принципы проектирования системы управления информационной безопасностью открытой информационной системы (З10);

принципы работы средств защиты информационно-технологических ресурсов автоматизированной системы (З11);

архитектуру информационной безопасности автоматизированной системы (З12);

принципы проектирования системы управления информационной безопасностью открытой информационной системы (З13);

правила, процедуры, практические приемы, руководящие принципы, методы, средства для обеспечения информационной безопасности открытых информационных систем (З14);

уметь:

разрабатывать модели угроз и нарушителей информационной безопасности автоматизированных систем, формировать требования к подсистемам информационной безопасности автоматизированных систем различных типов (У1);

осуществлять подбор и комплексирование средств защиты для автоматизированных систем в защищенном исполнении, контролировать эффективность проектирования, разработки и внедрения автоматизированных систем (У2);

применять языки, системы и инструментальные средств используемые для создания защищенных автоматизированных систем и средства защиты информации (У3);

определять комплекс мер (правила, процедуры, практические приемы, руководящие принципы, методы, средства) для обеспечения информационной безопасности автоматизированных систем, составлять аналитические обзоры по вопросам обеспечения информационной безопасности автоматизированных систем (У4);

создавать и исследовать модели открытых систем (У5);

разрабатывать модели угроз и модели нарушителя информационной безопасности автоматизированной системы (У6);

проводить анализ рисков информационной безопасности автоматизированной системы (У7);

проектировать и анализировать структуру защищенных автоматизированных систем (У8);

реализовывать ключевые функции средств защиты информации автоматизированной системы (У9);

эксплуатировать систему управления информационной безопасностью открытой информационной системы (У10);

применять средства защиты информационно-технологических ресурсов автоматизированной системы (У11);

контролировать состояние подсистем информационной безопасности автоматизированной системы (У12);

эксплуатировать систему управления информационной безопасностью открытой информационной системы (У13);

формировать комплекс мер для обеспечения информационной безопасности открытых информационных систем (У14);

владеть навыками:

навыками разработки моделей угроз и моделей нарушителей, методами мониторинга и аудита, выявления угроз информационной безопасности автоматизированных систем (Н1);

создания защищенных автоматизированных систем и средств защиты информации (Н2);

навыками выбора и обоснования критериев эффективности функционирования защищенных автоматизированных информационных систем (Н3);

навыками участия в экспертизе состояния защищенности информации на объекте защиты (Н4).

приемами и методами создания и исследования открытых систем (Н5);

существующими моделями угроз и моделями нарушителя информационной безопасности автоматизированной системы (Н6);

методами оценки рисков информационной безопасности автоматизированной системы (Н7);

методологиями проектирования и анализа защищенных автоматизированных систем (Н8);

разработки средств защиты информации автоматизированной системы (Н9);

совершенствования системы управления информационной безопасностью открытой информационной системы (Н10);

навыками восстановления работоспособности средств защиты информации автоматизированной системы при возникновении нештатных ситуаций (Н11);

процедурами безопасности используемыми в подсистемах информационной безопасности автоматизированной системы (Н12);

совершенствования системы управления информационной безопасностью открытой информационной системы (Н13);

эффективного применения комплекса мер для обеспечения информационной безопасности открытых информационных систем (Н14).

4. Структура и содержание дисциплины

Образовательная деятельность по дисциплине проводится:

– в форме контактной работы обучающихся с педагогическими работниками организации и (или) лицами, привлекаемыми организацией к реализации образовательных программ на иных условиях (далее – контактная работа);

– в форме самостоятельной работы.

Контактная работа включает в себя занятия лекционного типа, занятия семинарского типа (семинары, практические занятия, лабораторные работы, практикумы), групповые и (или) индивидуальные консультации, в том числе в электронной информационно-образовательной среде.

Обозначения:

Л – лекции, л/р – лабораторные работы, п/р – практические занятия, КСР – контроль самостоятельной работы, СРС – самостоятельная работа студента, ИФР – интерактивная форма работы, К – контроль.

4.1. Содержание дисциплины

Содержание	Формируемые компетенции	Формируемые ЗУН
Раздел 1. Основные виды АС в защищенном исполнении	ОК-8,ОПК-3, ОПК-6, ОПК-8, ПК-2, ПК-3, ПК-4, ПК-5, ПК-6, ПК-9, ПК-10, ПК-12	З1-З10, У1-У10, Н1-Н10
1.1. Введение. Понятие автоматизированной системы		
1.2. Общий порядок проектирования систем в защищенном исполнении		
Раздел 2. Моделирование защищенных автоматизированных систем	ОК-8, ОПК-3, ОПК-6, ОПК-8, ПК-2, ПК-3, ПК-6, ПК-9, ПК-10, ПК-12, ПК-13, ПК-20, ПК-24, ПК-25, ПК-26, ПСК-4.3, ПСК-4.5	З3-З14, У3-У14, Н1-Н14
2.1. Модель угроз		
2.2. Модель нарушителя		
Раздел 3. Разработка защищенных автоматизированных систем	ОПК-3, ОПК-6, ОПК-8, ПК-2, ПК-3, ПК-4, ПК-6, ПК-9, ПК-10, ПК-12, ПК-13, ПК-20, ПК-24, ПК-25, ПК-26, ПСК-4.3, ПСК-4.5	З2-З14, У1-У14, Н1-Н14
3.1 Создание систем защиты ПДн		
3.2. Основные критерии средств защиты		
Экзамен, РГР	ОК-8; ОПК-3; ОПК-6; ОПК-8; ПК-2; ПК-3; ПК-4; ПК-5; ПК-6; ПК-9; ПК-10; ПК-12; ПК-13; ПК-20; ПК-24; ПК-25; ПК-26; ПСК-4.3; ПСК-4.5	З1-З14, У1-У14, Н1-Н14

4.2. Объем дисциплины, виды учебной работы обучающихся по очной форме обуче*ния*

Содержание	Всего, час	Контактная работа, час				СРС, час	ИФР, час	К, час
		Л	л/р	п/р	КСР			
Раздел 1. Основные виды АС в защищенном исполнении								

1.1. Введение. Понятие автоматизированной системы	12	2	2	4		4		
1.2. Общий порядок проектирования систем в защищенном исполнении	12	2	2	4		4		
Раздел 2. Моделирование защищенных автоматизированных систем								
2.1. Модель угроз	24	2	4	8		10		
2.2. Модель нарушителя	16	4	2	4		6		
Раздел 3. Разработка защищенных автоматизированных систем								
3.1 Создание систем защиты ПДн	18	4	2	4		8		
3.2. Основные критерии средств защиты	14	2	4	8				
РГР	10					10		
Экзамен	38				2			36
Итого	**144 4 з.е.**	**16**	**16**	**32**	**2**	**42**		**36**

5. Содержание разделов дисциплины
5.1. Лекции

Раздел 1. Основные виды АС в защищенном исполнении
1.1. Введение. Цели и задачи курса. Содержание дисциплины. Рекомендуемая литература. Основные понятия и определения. Понятие автоматизированной системы. Особенности автоматизированных систем в защищенном исполнении. Основные виды АС в защищенном исполнении.
1.2. Проектирование систем в защищенном исполнении. Общий порядок проектирования систем в защищенном исполнении. Стандарты (ГОСТ), регламентирующие порядок проектирования АС в защищенном исполнении. Руководящие документы Гостехкомиссии России (ФСТЭК России).
Раздел 2. Моделирование защищенных автоматизированных систем
2.1. Модели угроз. Понятие модели угроз.,Документы,ФСТЭК,России, регламентирующие порядок разработки моделей угроз в автоматизированных системах. Практические подходы к разработке моделей угроз.
2.2. Модели нарушителя. Понятие модели нарушителя. Документы ФСТЭК России, регламентирующие порядок разработки моделей нарушителя в автоматизированных системах. Практические подходы к разработке моделей
нарушителя.
Раздел 3. Разработка защищенных автоматизированных систем
3.1. Создание систем защиты персональных данных. Понятие персональных данных. Понятие ИСПДн. Федеральное законодательство в области защиты персональных данных и ведомственные нормативные акты (ФСТЭК России, ФСБ России). Требования к ИСПДн. Классификация АС. Обезличивание персональных данных. Типовые модели угроз и модели нарушителя. Практические рекомендации по разработке моделей угроз и моделей нарушителя.
3.2. Основные категории средств защиты ИСПДн. Рекомендации по выбору средств защиты. Сертификация средств защиты ИСПДн. Особенности лицензирования соответствующих видов деятельности. Аттестация ИСПДн. Проектирование АС в защищенном исполнение на примере ИСПДн 1 класса.
5.2. Лабораторные работы

№	Тема	Количество

		часов
Лабораторная работа №1.	Изучение средств обеспечения надежности защищенных АИС. Средства построения дисковых RAID-массивов	4
Лабораторная работа №2.	Изучение средств обеспечения надежности защищенных АИС. Средства восстановления разделов файловой системы	4
Лабораторная работа №3.	Изучение технических средства защиты АИС от несанкционированного доступа	4
Лабораторная работа №4.	Изучение программных средства защиты АИС от несанкционированного доступа	4
Итого		16

5.3. Практические задания

Практическое занятие №1.	Основные угрозы безопасности информации в автоматизированных системах. Модели нарушителя в автоматизированных системах.	2
Практическое занятие №2	Методы, способы и средства разработки автоматизированных систем и подсистем безопасности автоматизированных систем.	2
Практическое занятие №3.	Методы, способы и средства обеспечения отказоустойчивости автоматизированных систем. Методы обеспечения информационной безопасности АИС.	4
Практическое занятие №4.	Методы проектирования защищенных АИС. Структура и содержание технического задания.	4
Практическое занятие №5.	Основы проектирования комплексной защиты информационной безопасности от НСД. Технологии создания отказоустойчивых систем.	4
Практическое занятие №6.	Аттестация АИС по требованиям безопасности. Особенности эксплуатации АИС на объекте защиты. Порядок обеспечения защиты информации при эксплуатации АИС.	4
Практическое занятие №7.	Технические и программные средства защиты АИС от несанкционированного доступа. Методы проверки защищенных АИС. Содержание и порядок ведения эксплуатационной документации.	4
Практическое занятие №8.	Контрольно-измерительное оборудование, используемое при поиске неисправностей и ремонте аппаратных средств АИС.	4
Практическое занятие №9.	Аппаратно-программные средства диагностики АИС. Аппаратно-программные средства контроля функционирования отдельных элементов, узлов, блоков.	4
Итого		32

5.3. Вопросы для самостоятельной работы студента в соответствии с содержанием разделов дисциплины

Тема	Вопрос
1.1. Введение. Понятие автоматизированной системы	Особенности автоматизированных систем в защищенном исполнении
1.2. Общий порядок проектирования систем в защищенном исполнении	Стандарты (ГОСТ), регламентирующие порядок проектирования АС в защищенном исполнении
2.1. Модель угроз	Документы ФСТЭК,России, регламентирующие порядок разработки моделей угроз в автоматизированных системах
2.2. Модель нарушителя	Практические,подходы к разработке,моделей нарушителя
3.1 Создание систем защиты ПДн	Федеральное законодательство в области защиты персональных данных и ведомственные нормативные акты (ФСТЭК России, ФСБ России).
3.2. Основные критерии средств защиты	Рекомендации по выбору средств защиты. Сертификация средств защиты ИСПДн.
ИТОГО	

6. Образовательные технологии

В соответствии со структурой образовательного процесса по дисциплине применяются следующие технологии:

- диагностики;
- целеполагания;
- управления процессом освоения учебной информации;
- применения знаний на практике, поиска новой учебной информации;
- организации совместной и самостоятельной деятельности обучающихся (учебно-познавательной, научно-исследовательской, частично-поисковой, репродуктивной, творческой и пр.);
- контроля качества и оценивания результатов образовательной деятельности (технология оценивания качества знаний, рейтинговая технология оценки знаний и др.)

В соответствии с требованиями ФГОС ВО для реализации компетентностного подхода при обучении дисциплине предусмотрено широкое использование в учебном процессе активных и интерактивных методов проведения занятий:

При обучении дисциплине применяются следующие формы занятий:

- лекции, направленные на получение новых и углубление научно-теоретических знаний, в том числе вводная лекция, информационная лекция, обзорная лекция, лекция-консультация, проблемная лекция, лекции-дискуссии, лекции-беседы и др.;
- практические занятия, проводимые под руководством преподавателя в учебной аудитории, направленные на углубление и овладение определенными методами самостоятельной работы, могут включать коллективное обсуждение материала, дискуссии, решение и разбор конкретных практических ситуаций, компьютерные симуляции, тренинги и др.
- лабораторные занятия, проводимые под руководством преподавателя в учебной лаборатории с использованием компьютеров и учебного оборудования, направленные на закрепление и получение новых умений и навыков, применение знаний и умений, полученных на теоретических занятиях, при решении практических задач и др.

Все занятия обеспечены мультимедийными средствами (SMART доски, проекторы, экраны) для повышения качества восприятия изучаемого материала. В образовательном процессе широко используются информационно-коммуникационные технологии.

Самостоятельная работа студентов – это планируемая работа студентов, выполняемая по заданию при методическом руководстве преподавателя, но без его непосредственного участия. Формы самостоятельной работы студентов определяются содержанием учебной дисциплины, степенью подготовленности студентов. Они могут иметь учебный или учебно-исследовательский характер: анализ литературы по теме, подготовка к лабораторным работам, подготовка реферативных сообщений, разработка проекта и др.

Формами контроля самостоятельной работы выступают оценивание проверка отчётов по результатам выполненных заданий и лабораторных работ, РГР. Результаты самостоятельной работы учитываются при оценке знаний на экзамене.

7. Формы аттестации и оценочные материалы

Текущий контроль предназначен для проверки хода и качества усвоения учебного материала, стимулирования учебной работы обучающихся и совершенствования методики проведения занятий. Он проводится в ходе всех видов занятий в форме, избранной преподавателем.

Промежуточная аттестация имеет целью определить степень достижения учебных целей по учебной дисциплине и проводится в форме экзаменов. Принимается экзамен преподавателями, читающими лекции по данной учебной дисциплине в соответствии с перечнем основных вопросов, выносимых для контроля знаний обучающихся:

7.1. Вопросы и задачи к экзамену

1. Основные понятия и определения. Понятие автоматизированной системы.
2. Особенности автоматизированных систем в защищенном исполнении.
3. Основные виды АС в защищенном исполнении.
4. Общий порядок проектирования систем в защищенном исполнении. Стандарты (ГОСТ), регламентирующие порядок проектирования АС в защищенном исполнении.
5. Руководящие документы Гостехкомиссии России (ФСТЭК России).
6. Понятие модели угроз. Документы ФСТЭК России, регламентирующие порядок разработки моделей угроз в автоматизированных системах. Практические подходы к разработке моделей угроз.
7. Понятие модели нарушителя. Документы ФСТЭК России, регламентирующие порядок разработки моделей нарушителя в автоматизированных системах.
8. Практические подходы к разработке моделей нарушителя.
9. Понятие персональных данных. Понятие ИСПДн.
10. Федеральное законодательство в области защиты персональных данных и ведомственные нормативные акты (ФСТЭК России, ФСБ России).
11. Требования к ИСПДн. Классификация АС. Обезличивание персональных данных.
12. Типовые модели угроз и модели нарушителя.
13. Практические рекомендации по разработке моделей угроз и моделей нарушителя.
14. Рекомендации по выбору средств защиты. Сертификация средств защиты ИСПДн.
15. Особенности лицензирования соответствующих видов деятельности. Аттестация ИСПДн.
16. Проектирование АС в защищенном исполнение на примере ИСПДн 1 класса.

Примерные задачи:

1. Защиты информации в автоматизированных системах обработки данных (АСОД).
2. Надёжность информации.
3. Уязвимость информации.
4. Элементы и объекты защиты в АСОД.
5. Дестабилизирующие факторы АСОД.
6. Причины нарушения целостности информации.

7. Каналы несанкционированного получения информации (ПНЦИ) в АСОД (КНПИ).
8. Электронная цифровая подпись.
9. Криптографические стандарты DES и ГОСТ 28147-89.
10. Проблемы реализации методов криптографической защиты в АСОД.
11. Характеристики криптографических средств защиты.
12. Криптографические методы защиты информации.
13. Криптология и основные её развития.
14. Методы криптографического преобразования данных.
15. Шифрование заменой (подстановка).
16. Монофоническая замена.
17. Шифрование методом перестановки.
18. Шифрование методом гаммирования.
19. Шифрование с помощью аналитических преобразований.
20. Комбинированные методы шифрования.
21. Кодирование.
22. Каналы несанкционированного получения информации (ПНЦИ) в АСОД (КНПИ).
23. Преднамеренные угрозы безопасности АСОД.
24. Подтверждение подлинности пользователей и разграничение их доступа к компьютерным ресурсам.
25. Своевременное обнаружение несанкционированных действий пользователей.
26. Контроль правильности функционирования системы защиты.

Раздел 3. Разработка защищенных автоматизированных систем

27. Технология построение локальной сети Arcnet.
28. Технология построение локальной сети Token Ring.
29. Технология построение локальной сети Ethernet.
30. Технология построение локальной сети Fast Ethernet.
31. Технология построение локальной сети Gigabit Ethernet.
32. Технология построение локальной сети 100BASEVG - AnyLAN.
33. Технология построение локальной сети высокоскоростные (более 100Мбит/с) сети.
34. Технология построение локальной сети оптоволоконный интерфейс FDDI.
35. Технология построение локальной сети ATM (Asynchronous Transfer Mode).
36. Технология построение локальной сети Fibre Channel.
37. Функции и задачи защиты информации.
38. Функции непосредственной защиты информации.
39. Методы и системы защиты информации.
40. Подтверждение подлинности пользователей и разграничение их доступа к компьютерным ресурсам.
41. Контроль доступа к аппаратуре.
42. Использование простого пароля.
43. Использование динамически изменяющегося пароля.
44. Методы модификации схемы простых паролей.
45. Методы идентификации и установления подлинности субъектов и различных объектов.
46. Своевременное обнаружение несанкционированных действий пользователей.
47. Общие сведения о контроле информационной целостности.
48. Способы определения модификаций информации.
49. Организация контроля.
50. Особенности использования программ непосредственного контроля.
51. Регистрация действий пользователей.

52. Контроль правильности функционирования системы защиты.

Оценивание результатов экзамена

Экзаменационный билет для проведения промежуточной аттестации включают вопросы и задачи для проверки сформированности знаний, умений и навыков.

Общими критериями, определяющими оценку знаний, умений и навыков на экзамене, являются:

для оценки «отлично» - наличие глубоких и исчерпывающих знаний в объёме пройденного программного материала правильные и уверенные действия по применению полученных знаний на практике, грамотное и логически стройное изложение материала при ответе, знание дополнительно рекомендованной литературы;

для оценки «хорошо» - наличие твердых и достаточно полных знаний программного материала, незначительные ошибки при освещении заданных вопросов, правильны действия по применению знаний на практике, четкое изложение материала;

для оценки «удовлетворительно» - наличие твердых знаний пройденного материала, изложение ответов с ошибками, уверенно исправляемыми после дополнительных вопросов, необходимость наводящих вопросов, правильные действия по применению знаний на практике;

для оценки «неудовлетворительно» - наличие грубых ошибок в ответе, непонимание сущности излагаемого вопроса, неумение применять знания на практике, неуверенность и неточность ответов на дополнительные и наводящие вопросы.

7.2. Примерная тематика расчетно-графических работ

1. Информационные технологии, используемые в АИС.
2. Основные угрозы безопасности информации в автоматизированных системах.
3. Модели нарушителя в автоматизированных системах.
4. Методы, способы и средства разработки автоматизированных систем и подсистем безопасности автоматизированных систем.
5. Методы, способы и средства обеспечения отказоустойчивости автоматизированных систем.
6. Методы обеспечения информационной безопасности АИС.
7. Методы и этапы проектирования защищенных АИС.
8. Построение комплексной защиты АИС.
9. Основы проектирования комплексной защиты информационной безопасности от НСД.
10. Средства обеспечения надежности защищенных АИС.
11. Технологии создания отказоустойчивых систем.
12. Аттестация АИС по требованиям безопасности.
13. Особенности эксплуатации АИС на объекте защиты.
14. Требования и рекомендации по защите служебной тайны и персональных данных при работе АИС.
15. Порядок обеспечения защиты информации при эксплуатации АИС.
16. Технические и программные средства защиты АИС от несанкционированного доступа.
17. Организация технического обслуживания защищенных АИС.
18. Методы проверки защищенных АИС.
19. Средства диагностирования защищенных АИС.
20. Контрольно-измерительное оборудование, используемое при поиске неисправностей аппаратных средств АИС.

21. Технологическое оборудование для ремонта аппаратных средств АИС.
22. Диагностические программы и пакеты диагностических программ, их назначение, возможности и порядок использования.
23. Аппаратно-программные средства диагностики АИС.
24. Аппаратно-программные средства контроля функционирования отдельных элементов, узлов, блоков.

Оценивание расчетно-графической работы

Оценивание расчетно-графической работы осуществляется в соответствии с полнотой и качеством выполнения задания на работу, качеством защиты работы (ответы на вопросы, презентация и др.). Оценка работы отражает уровень сформированности соответствующих компетенций.

8. Учебно-методическое и информационное обеспечение дисциплины

Электронный каталог и электронные информационные ресурсы, предоставляемые научной библиотекой ФГБОУ ВО «Чувашский государственный университет имени И.Н. Ульянова» доступны по ссылке http://library.chuvsu.ru/

8.1. Рекомендуемая основная литература

(ежегодное обновление перечня и условия доступа представлены в Приложениях к рабочей программе)

№ п/п	Наименование
1.	Подольский В.И. Компьютерные информационные системы в аудите: учебное пособие / Подольский В.И., Щербакова Н.А., Комиссаров В.Л., В.Л. Комиссаров; Н.А. Щербакова; В.И. Подольский - Компьютерные информационные системы в аудите - Москва: ЮНИТИ-ДАНА, 2012. - 163 с.. - ISBN 5-238-01141-5. http://www.iprbookshop.ru/10498.html
2.	Емельянова Н. З. Основы построения автоматизированных информационных систем: [учебное пособие для среднего профессионального образования по специальности "Программированное обеспечение вычислительной техники и автоматизированных систем"] / Емельянова Н. З., Партыка Т. Л., Попов И. И. - Москва: Форум, Инфра-М, 2007. - 415с.
3.	Гайдамакин Н. А. Автоматизированные информационные системы, базы и банки данных: вводный курс : учебное пособие для вузов по специальностям "Компьютерная безопасность" и "Комплексное обеспечение информационной безопасности автоматизированных систем" / Гайдамакин Н. А. - Москва: Гелиос АРВ, 2002. - 367с.

8.2 Рекомендуемая дополнительная литература

(ежегодное обновление и условия доступа перечня представлены в Приложениях к рабочей программе)

№ п/п	Наименование
1.	Денисова Е.В. Автономные информационные системы обнаружения скрытых объектов: учебное пособие / Денисова Е.В., Легкий В.Н., В.Н. Легкий; Е.В. Денисова; ред. В.Н. Опарин - Новосибирск: Новосиб. гос. техн. ун-т, 2012. - 128 с. Режим доступа: http://www.iprbookshop.ru/45358.html
2.	Васильев В.И. Интеллектуальные системы защиты информации [Электронный

	ресурс]: учебное пособие/ Васильев В.И.— Электрон. текстовые данные.— М.: Машиностроение, 2013.— 172 с.— Режим доступа: http://www.iprbookshop.ru/18519.— ЭБС «IPRbooks»
3.	Громов Ю.Ю. Интеллектуальные информационные системы и технологии: учебное пособие / Громов Ю.Ю., Иванова О.Г., Алексеев В.В., Беляев М.П., Швец Д.П., Елисеев А.И., Д.П. Швец; А.И. Елисеев; М.П. Беляев; Ю.Ю. Громов; О.Г. Иванова; В.В. Алексеев - Тамбов: Тамбовский государственный технический университет, ЭБС АСВ, 2013. - 244 с. Режим доступа: http://www.iprbookshop.ru/63850.html

Нормативные правовые и методические документы в области защиты информации доступны по ссылке https://fstec.ru/component/tags/tag/informatsionnoe-soobshchenie

8.3. Программное обеспечение, профессиональные базы данных, информационно-справочные системы

Программное обеспечение, профессиональные базы данных, информационно-справочные системы, предоставляемые управлением информатизации ФГБОУ ВО «Чувашский государственный университет имени И.Н. Ульянова» доступны по ссылке http://ui.chuvsu.ru//*

8.3.1 Программное обеспечение

№ п/п	Наименование	Условия доступа/скачивания
1.	MS Office/ LibreOffice	лицензия университета/ свободное лицензионное соглашение (https://ru.libreoffice.org/)
2.	MS Windows/Linux (Ubuntu)	лицензия университета/ свободное лицензионное соглашение (http://ubuntu.ru/)
3.	AVG AntiVirus Free	https://www.avg.com/ru-ru/homepage#pc
4.	Avast Free Antivirus	http://avast-anti-virus.ru/?yclid=5762528100398929218
5.	Kaspersky Free	https://www.kaspersky.ru/free-antivirus
6.	360 Total Security	https://www.360totalsecurity.com/ru/
7.	Zabbix	https://www.zabbix.com/download
8.	Clonezilla	https://clonezilla.org/downloads.php
9.	rsync	https://rsync.samba.org/

8.3.2 Базы данных, информационно-справочные системы

№ п/п	Наименование программного обеспечения	Условия доступа/скачивания
1.	Гарант	из внутренней сети университета (договор)*
2.	Консультант +	
3.	Springer	
4.	База данных угроз безопасности информации	https://bdu.fstec.ru/

8.4. Рекомендуемые интернет-ресурсы и открытые онлайн курсы.

№ п/п	Наименование	Условия доступа
1.	ISO 27000 Международные стандарты управления информационной безопасностью.	http://iso27000.ru
2.	Информационная безопасность. Практика информационной	http://dorlov.blogspot.com

	безопасности.	
3.	Электронная безопасность	www.suritel.ru
4.	Код безопасности	СЗИ от НСД Secret Net, СКриптЗИ М-506А-XP, www.securitvcode.ru
5.	SecurityLab. Информационный портал по безопасности.	http://www.securitylab.ru
6.	Xgu.ru.	http://xgu.ru/wiki/
7.	Российская Государственная Библиотека	http://www.rsl.ru
8.	Государственная публичная научно-техническая библиотека России	http://www.gpntb.ru
9.	Фундаментальная библиотека Нижегородского государственного университета	http://www.unn.ru/library
10.	Научная библиотека Казанского государственного университета	http://lsl.ksu.ru
11.	Научная электронная библиотека	http://elibrary.ru
12.	Полнотекстовая библиотека учебных и учебно-методических материалов	http://window.edu.ru
13.	Электронно-библиотечная система IPRbooks	http://www.iprbookshop.ru

9. Материально-техническое обеспечение дисциплины

Учебные аудитории для лекционных занятий по дисциплине оснащены автоматизированным рабочим местом (АРМ) преподавателя, обеспечивающим тематические иллюстрации и демонстрации, соответствующие программе дисциплины в составе:

- ПЭВМ с доступом в интернет (операционная система, офисные программы, антивирусные программы);
- мультимедийный проектор с дистанционным управлением;
- мультимедийное звуковое оборудование;
- настенный экран;
- интерактивная доска SMART;
- телевизор SMART.

Учебные аудитории для практических, лабораторных и самостоятельных занятий по дисциплине оснащены АРМ преподавателя и пользовательскими АРМ по числу обучающихся, объединенных локальной сетью («компьютерный» класс), с возможностью подключения к сети Интернет и доступом к электронной информационно-образовательной среде ФГБОУ ВО «Чувашский государственный университет имени И.Н. Ульянова».

Учебная аудитория для лабораторных занятий в области защищенных автоматизированных систем, оснащена аппаратно-программными средствами управления доступом к данным, шифрования, средствами дублирования и восстановления данных, средствами мониторинга состояния автоматизированных систем, источниками бесперебойного и аварийного питания, средствами контроля и управления доступом в помещения, охранной и пожарной сигнализацией, климатическим контролем.

10. Средства адаптации преподавания дисциплины к потребностям лиц с ограниченными возможностями

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

– для лиц с нарушениями зрения: в печатной форме увеличенным шрифтом; в форме электронного документа; в форме аудиофайла (перевод учебных материалов в аудиоформат); в печатной форме на языке Брайля; индивидуальные консультации с привлечением тифлосурдопереводчика; индивидуальные задания и консультации.

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

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

11. Методические рекомендации по освоению дисциплины

В ходе лекционных занятий студенту рекомендуется вести конспектирование учебного материала. Следует обращать внимание на категории, формулировки, раскрывающие содержание тех или иных явлений и процессов, научные выводы и практические рекомендации, положительный опыт в ораторском искусстве. При составлении конспекта желательно оставлять в рабочих конспектах поля, на которых в дальнейшем можно делать пометки из рекомендованной литературы, дополняющие материал прослушанной лекции, а также подчеркивающие особую важность тех или иных теоретических положений. В ходе лекционных занятий рекомендуется задавать преподавателю уточняющие вопросы с целью уяснения теоретических положений, разрешения спорных ситуаций.

В ходе подготовки к практическим занятиям и лабораторным работам рекомендуется изучить основную литературу, ознакомиться с дополнительной литературой, новыми публикациями в периодических изданиях: журналах, газетах и т.д. основой для выполнения лабораторной работы являются разработанные кафедрой методические указания. Рекомендуется дорабатывать свой конспект лекций, делая в нем соответствующие записи из литературы, рекомендованной преподавателем и предусмотренной рабочей программой дисциплины. Желательно подготовить тезисы для выступлений по всем учебным вопросам, выносимым на практическое занятие. Готовясь к докладу или реферативному сообщению, рекомендуется обращаться за методической помощью к преподавателю, составить план-конспект своего выступления, продумать примеры с целью обеспечения тесной связи изучаемой теории с практикой. В процессе подготовки студент может дополнить список использованной литературы современными источниками, не представленными в списке рекомендованной литературы, и в дальнейшем использовать собственные подготовленные учебные материалы при написании курсового проекта.

Формы организации студентов на лабораторных работах и практических занятиях индивидуальная. При индивидуальной форме организации занятий каждый студент выполняет индивидуальное задание.

Если в результате выполнения лабораторной работы запланирована подготовка письменного отчета, то отчет о выполненной работе необходимо оформлять в соответствии с требованиями методических указаний. Качество выполнения лабораторных работ является важной составляющей оценки текущей успеваемости обучающегося.