МИНОБРНАУКИ РОССИИ
ФЕДЕРАЛЬНОЕ ГОСУДАРСТВЕННОЕ БЮДЖЕТНОЕ ОБРАЗОВАТЕЛЬНОЕ УЧРЕЖДЕНИЕ ВЫСШЕГО ОБРАЗОВАНИЯ
«ВОРОНЕЖСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ ИНЖЕНЕРНЫХ ТЕХНОЛОГИЙ»

УТВЕРЖДАЮ
Проректор по учебной работе

ДОКУМЕНТ ПОДПИСАН
ЭЛЕКТРОННОЙ ПОДПИСЬЮ

Сертификат: 00A29CA99D98126F4EB57F6F989D713C88
Владелец: Василенко Виталий Николаевич
Действителен: с 07.07.2022 до 30.09.2023

_____ Василенко В.Н.

«25» мая 2023

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ

Разработка и эксплуатация автоматизированных систем в защищенном исполнении

(наименование в соответствии с РУП)

Специальность

10.05.03 Информационная безопасность автоматизированных систем
(шифр и наименование направления подготовки/специальности)

Специализация

Безопасность открытых информационных систем
(наименование профиля/специализации)

Квалификация выпускника
специалист по защите информации
(в соответствии с Приказом Министерства образования и науки РФ от 12 сентября 2013 г. N 1061 "Об утверждении перечней специальностей и направлений подготовки высшего образования" (с изменениями и дополнениями)

1. Цели и задачи дисциплины

Целью освоения дисциплины «Разработка и эксплуатация автоматизированных систем в защищенном исполнении» является формирование компетенций обучающегося в области профессиональной деятельности и сфере профессиональной деятельности:

- 06 Связь, информационные и коммуникационные технологии (в сфере обеспечения безопасности информации в автоматизированных системах).

Дисциплина направлена на решение задач профессиональной деятельности проектного типа.

Программа составлена в соответствии с требованиями Федерального государственного образовательного стандарта высшего образования по специальности 10.05.03 Информационная безопасность автоматизированных систем.

2. Перечень планируемых результатов обучения, соотнесенных с планируемыми результатами освоения образовательной программы

В результате освоения дисциплины в соответствии с предусмотренными компетенциями обучающийся должен:

№ п/п	Код компетенции	Наименование компетенции	Код и наименование индикатора достижения компетенции
1	ОПК-11	Способен разрабатывать компоненты систем защиты информации автоматизированных систем	ИД1$_{ОПК-11}$ – обладает способностью проводить анализ защищённости автоматизированных систем

Код и наименование индикатора достижения компетенции	Результаты обучения (показатели оценивания)
ИД1$_{ОПК-11}$ – обладает способностью проводить анализ защищённости автоматизированных систем	Знает особенности проведения анализ защищённости автоматизированных систем
	Умеет проводить анализ защищённости автоматизированных систем
	Владеет способностью проводить анализ защищённости автоматизированных систем

3. Место дисциплины в структуре ОП ВО

Дисциплина относится к части, формируемой участниками образовательных отношений Блока 1 ООП. Дисциплина является обязательной к изучению.

Изучение дисциплины основано на знаниях, умениях и навыках, полученных при изучении обучающимися дисциплины «Микропроцессоры и микроконтроллеры» и прохождении обучающимися учебной (ознакомительной) практики.

Дисциплина является предшествующей для прохождения производственной (преддипломной) практики, подготовки к процедуре защиты и защиты выпускной квалификационной работы.

4. Объем дисциплины и виды учебных занятий

Общая трудоемкость дисциплины составляет 9 зачетных единиц.

Виды учебной работы	**Всего ак. ч**	**Распределение трудоемкости по семестрам, ак. ч**	
		9 семестр	**А семестр**
Общая трудоемкость дисциплины	**324**	**144**	**180**
Контактная работа, *в т.ч. аудиторные занятия:*	**203,6**	**91,6**	**112**
Лекции	66	30	36
в том числе в форме практической подготовки	–	–	–
Лабораторные работы	66	30	36
в том числе в форме практической подготовки	–	–	–

Практические занятия (ПЗ)	66	30	36
в том числе в форме практической подготовки	–	–	–
Консультации текущие	3,3	1,5	1,8
Консультации перед экзаменом	2	–	2
Вид аттестации (зачет, экзамен)	0,3	0,1	0,2
Самостоятельная работа:	**86,6**	**52,4**	**34,2**
Проработка материалов по лекциям, учебникам, учебным пособиям	17,6	7,4	10,2
Подготовка к практическим и лабораторным занятиям	27	15	12
Подготовка доклада	30	30	–
Домашнее задание	12	–	12
Подготовка к экзамену (контроль)	**33,8**	**–**	**33,8**

5. Содержание дисциплины, структурированное по темам (разделам) с указанием отведенного на них количества академических часов и видов учебных занятий

5.1 Содержание разделов дисциплины

№ п/п	Наименование разделов дисциплины	Содержание раздела	Трудоемкость раздела, ак. ч
1	Теоретические основы построения защищенных автоматизированных систем	Системный подход к построению защищенных автоматизированных систем. Понятие сложной системы. Управление и информация, самоорганизация. Основные принципы системного подхода при создании сложных систем; Понятие качества и эффективности. Методические вопросы оценки эффективности сложных систем. Функциональная и обеспечивающая часть сложной системы. Технология функционирования сложной системы.	74,4
2	Угрозы безопасности автоматизированных систем	Угрозы безопасности локальных и распределённых автоматизированных систем. Проектирование автоматизированных систем. Цели и задачи проектирования. Структуризация предметной области. Классификация объектов проектирования. Жизненный цикл автоматизированной системы. Этапы проектирования системы. Организация работ, функции заказчиков и разработчиков. Разработка компонентов систем защиты информации автоматизированных систем.	74
3	Проектирование защищенных автоматизированных систем	Проектирование и построение системы защиты автоматизированных систем. Практические методы реализации моделей безопасности. Ядра безопасности. Мониторинг взаимодействий в системе. Архитектура защищенных систем. Принципы построения защищенных информационных систем. Технологический цикл реализации защищенной системы обработки и хранения информации. Реализация систем контроля доступа; способы представления информации о правах доступа.	65
4	Методы обеспечения безопасности защищенных автоматизированных систем	Методология оценки защищенности изделий и продуктов информационных технологий. Критерии оценки безопасности информационных технологий. Контекст безопасности. Профиль защиты и задание по безопасности. Функциональные требования безопасности. Функциональные классы, семейства и компоненты безопасности. Требования доверия к безопасности. Классы, семейства и компоненты доверия. Оценочный уровень доверия. Критерии оценки профиля защиты и задания по безопасности.	71,2

5.2 Разделы дисциплины и виды занятий

№ п/п	Наименование раздела дисциплины	Лекции, ак. ч	ЛР, ак. ч	ПЗ, ак. ч	СР, ак. ч

1	Теоретические основы построения защищенных автоматизированных систем	16	16	16	26,4
2	Угрозы безопасности автоматизированных систем	16	16	16	26
3	Проектирование защищенных автоматизированных систем	16	16	16	17
4	Методы обеспечения безопасности защищенных автоматизированных систем	18	18	18	17,2
	Консультации текущие	3,3			
	Консультации перед экзаменом	2			
	Зачет, экзамен	0,3			

5.2.1 Лекции

№ п/п	Наименование раздела дисциплины	Тематика лекционных занятий	Трудоемкость, ак. ч
1	Теоретические основы построения защищенных автоматизированных систем	Системный подход к построению защищенных автоматизированных систем. Понятие сложной системы. Управление и информация, самоорганизация. Основные принципы системного подхода при создании сложных систем; Понятие качества и эффективности. Методические вопросы оценки эффективности сложных систем. Функциональная и обеспечивающая часть сложной системы. Технология функционирования сложной системы.	16
2	Угрозы безопасности автоматизированных систем	Угрозы безопасности локальных и распределённых автоматизированных систем. Проектирование автоматизированных систем. Цели и задачи проектирования. Структуризация предметной области. Классификация объектов проектирования. Жизненный цикл автоматизированной системы. Этапы проектирования системы. Организация работ, функции заказчиков и разработчиков.	16
3	Проектирование защищенных автоматизированных систем	Проектирование и построение системы защиты автоматизированных систем. Практические методы реализации моделей безопасности. Ядра безопасности. Мониторинг взаимодействий в системе. Архитектура защищенных систем. Принципы построения защищенных информационных систем. Технологический цикл реализации защищенной системы обработки и хранения информации. Реализация систем контроля доступа; способы представления информации о правах доступа.	16

4	Методы обеспечения безопасности защищенных автоматизированных систем	Методология оценки защищенности изделий и продуктов информационных технологий. Критерии оценки безопасности информационных технологий. Контекст безопасности. Профиль защиты и задание по безопасности. Функциональные требования безопасности. Функциональные классы, семейства и компоненты безопасности. Требования доверия к безопасности. Классы, семейства и компоненты доверия. Оценочный уровень доверия. Критерии оценки профиля защиты и задания по безопасности.	18
	Консультации текущие		3,3
	Консультации перед экзаменом		2
	Зачет, экзамен		0,3

5.2.2 Практические занятия

№ п/п	Наименование раздела дисциплины	Тематика практических занятий	Трудоемкость, ак. ч
1	Теоретические основы построения защищенных автоматизированных систем	Проектирование моделей данных с помощью CASE-системы ERWIN для построения защищенных АС	16
2	Угрозы безопасности автоматизированных систем	Безопасность в системах с распределенными базами данных	8
		Организация защищённых соединений при удалённом доступе.	8
3	Проектирование защищенных автоматизированных систем	Защита информационных воздействий по протоколу IPSec при использовании Windows 2003 Server.	8
		Обеспечение аутентичности удаленных пользователей посредством применения протоколов CHAP и EAP при организации модемных соединений.	8
4	Методы обеспечения безопасности защищенных автоматизированных систем	Настройка клиент-серверного взаимодействия по протоколу защиты данных	8
		Установка центра сертификации, генерация и отзыв сертификатов в операционной системе Windows	10

5.2.3 Лабораторный практикум

№ п/п	Наименование раздела дисциплины	Тематика лабораторных занятий	Трудоемкость, ак. ч
1	Теоретические основы построения защищенных автоматизированных систем	Создание моделей основных видов АС в защищенном исполнении	16

2	Угрозы безопасности автоматизированных систем	Разработка модели угроз и нарушителя для организации	16
3	Проектирование защищенных автоматизированных систем	Проектирование системы защиты персональных данных для основных видов АС	16
4	Методы обеспечения безопасности защищенных автоматизированных систем	Проектирование АС в защищенном исполнение на примере ИСПДн 1 класса	18

5.2.4 Самостоятельная работа обучающихся (СРО)

№ п/п	Наименование раздела дисциплины	Вид СРО	Трудоемкость, час
1	Теоретические основы построения защищенных автоматизированных систем	Проработка материалов по лекциям, учебникам, учебным пособиям	3,4
		Подготовка к практическим и лабораторным занятиям	8
		Подготовка доклада с визуальным представлением средствами PowerPoint	15
2	Угрозы безопасности автоматизированных систем	Проработка материалов по лекциям, учебникам, учебным пособиям	4
		Подготовка к практическим и лабораторным занятиям	7
		Подготовка доклада с визуальным представлением средствами PowerPoint	15
3	Проектирование защищенных автоматизированных систем	Проработка материалов по лекциям, учебникам, учебным пособиям	5
		Подготовка к практическим и лабораторным занятиям	6
		Домашнее задание	6
4	Методы обеспечения безопасности защищенных автоматизированных систем	Проработка материалов по лекциям, учебникам, учебным пособиям	5,2
		Подготовка к практическим и лабораторным занятиям	6
		Домашнее задание	6

6. Учебно-методическое и информационное обеспечение дисциплины

Для освоения дисциплины обучающийся может использовать:

6.1. Основная литература

1. Давидюк, Н. В. Разработка автоматизированных систем обработки информации в защищенном исполнении : учебное пособие / Н. В. Давидюк. – Санкт-Петербург : Интермедия, 2020. – 48 с. – ISBN 978-5-4383-0194-3. – Текст : электронный // Лань : электронно-библиотечная система. – URL: https://e.lanbook.com/book/161365

2. Бабушкин, В. М. Разработка защищенных программных средств информатизации производственных процессов предприятия : учебное пособие / В. М. Бабушкин. – Казань : КНИТУ-КАИ, 2020. – 256 с. – ISBN 978-5-7579-2463-2. – Текст : электронный // Лань : электронно-библиотечная система. – URL: https://e.lanbook.com/book/193486

3. Тугов, В. В. Проектирование автоматизированных систем управления : учебное пособие для вузов / В. В. Тугов, А. И. Сергеев, Н. С. Шаров. – 3-е изд., стер. – Санкт-

Петербург : Лань, 2022. – 172 с. – ISBN 978-5-8114-8987-9. – Текст : электронный // Лань : электронно-библиотечная система. – URL: https://e.lanbook.com/book/186064

4. Потехин, Д. С. Разработка программно-аппаратного обеспечения информационных и автоматизированных систем : учебное пособие / Д. С. Потехин, И. Е. Тарасов. – Москва : РТУ МИРЭА, 2022. – 131 с. – Текст : электронный // Лань : электронно-библиотечная система. – URL: https://e.lanbook.com/book/240098

6.2. Дополнительная литература

1. Пономаренко, Д. А. Основы проектирования автоматизированных систем : учебное пособие / Д. А. Пономаренко, Н. И. Безгачин. – 2-е изд., испр. и доп. – Мурманск : МГТУ, 2016. – 154 с. – ISBN 978-5-86185-889-2. – Текст : электронный // Лань : электронно-библиотечная система. – URL: https://e.lanbook.com/book/142630

2. Гвоздева, Т. В. Проектирование информационных систем. Стандартизация, техническое документирование информационных систем : учебное пособие для спо / Т. В. Гвоздева, Б. А. Баллод. – 2-е изд., стер. – Санкт-Петербург : Лань, 2021. – 216 с. – ISBN 978-5-8114-8414-0. – Текст : электронный // Лань : электронно-библиотечная система. – URL: https://e.lanbook.com/book/176672

3. Гвоздева, Т. В. Проектирование информационных систем: технология автоматизированного проектирования. Лабораторный практикум : учебное пособие / Т. В. Гвоздева, Б. А. Баллод. – 2-е изд., стер. – Санкт-Петербург : Лань, 2020. – 156 с. – ISBN 978-5-8114-5147-0. – Текст : электронный // Лань : электронно-библиотечная система. – URL: https://e.lanbook.com/book/133477

4. Лукьянец, О. Ф. Формализация технологических знаний при разработке автоматизированных систем : учебное пособие / О. Ф. Лукьянец, С. Е. Каминский, О. М. Деев. – Москва : МГТУ им. Н.Э. Баумана, 2014. – 136 с. – ISBN 978-5-7038-3771-9. – Текст : электронный // Лань : электронно-библиотечная система. – URL: https://e.lanbook.com/book/58416

6.3 Перечень учебно-методического обеспечения для самостоятельной работы обучающихся

1. Разработка и эксплуатация защищенных автоматизированных систем [Электронный ресурс]: методические указания для самостоятельной работы для студентов, обучающихся по направлению 10.05.03 «Информационная безопасность автоматизированных систем», очной формы обучения / А. В. Скрыпников**,** Е. В. Чернышова ; ВГУИТ, Кафедра информационной безопасности. - Воронеж : ВГУИТ, 2016. - 20 с. http://biblos.vsuet.ru/ProtectedView/Book/ViewBook/1731

2. Методические указания для обучающихся по освоению дисциплин (модулей) в ФГБОУ ВО ВГУИТ [Электронный ресурс] : методические указания для обучающихся на всех уровнях высшего образования / М. М. Данылив, Р. Н. Плотникова; ВГУИТ, Учебно-методическое управление. - Воронеж : ВГУИТ, 2016. – Режим доступа : http://biblos.vsuet.ru/MegaPro/Web/SearchResult/MarcFormat/100813

6.4 Перечень ресурсов информационно-телекоммуникационной сети «Интернет», необходимых для освоения дисциплины

Наименование ресурса сети «Интернет»	Электронный адрес ресурса
«Российское образование» - федеральный портал	*https://www.edu.ru/*
Научная электронная библиотека	*https://elibrary.ru/defaultx.asp?*
Национальная исследовательская компьютерная сеть России	*https://niks.su/*
Информационная система «Единое окно доступа к образовательным ресурсам»	*http://window.edu.ru/*
Электронная библиотека ВГУИТ	*http://biblos.vsuet.ru/megapro/web*
Сайт Министерства науки и высшего образования РФ	*https://minobrnauki.gov.ru/*
Портал открытого on-line образования	*https://npoed.ru/*
Электронная информационно-образовательная среда ФГБОУ ВО	*https://education.vsuet.ru/*

6.5 Перечень информационных технологий, используемых при осуществлении образовательного процесса по дисциплине, включая перечень программного обеспечения и информационных справочных систем

При изучении дисциплины используется программное обеспечение, современные профессиональные базы данных и информационные справочные системы: ЭИОС университета, в том числе на базе программной платформы «Среда электронного обучения 3KL», автоматизированная информационная база «Интернет-тренажеры», «Интернет-экзамен» и др.

При освоении дисциплины используется лицензионное и открытое про-граммное обеспечение – ОС Microsoft Windows, ОС ALT Linux, Microsoft Office Professional Plus, VMWare Player, Oracle VM VirtualBox.

Блок управления комплекса радиоконтроля и поиска радиопередающих устройств «ОМЕГА» (переносной), МУ защиты ресурсов сети от внутренних и внешних атак CISCO ASA5505-KB, переносной комплекс для автоматизации измерений при проведении исследований и контроля технических средств ЭВТ «НАВИГАТОР-ПЗГ»; средство активной защиты информации от утечки за счет побочных электромагнитных излучений и наводок «СОНАТА-Р3.1»; система защиты речевой информации «Соната-АВ-4Б» (Центральный блок питания и управления + Размыкатели в составе СВАЗ Соната АВ); профессиональный обнаружитель скрытых видеокамер СОКОЛ-М (переносной); портативный обнаружитель закладок Protect1203 (переносной); устройство активной защиты информации «ВЕТО-М»; электронный замок Samsung SHS-2920. Страж NT вер.3.0 Сертификат ФСТЭК № 2145 30.07.2013 г.; Ревизор 1XP Сертификат ФСТЭК № 989 08.02.2015 г.; Ревизор 2XP Сертификат ФСТЭК № 990 08.02.2015 г.; Фикс 2.0.2 Сертификат ФСТЭК №1548 15.01.2015 г.; Ревизор сети вер.3.0 Сертификат ФСТЭК №3413 02.06.2015 г.; СЗИ Панцирь К Сертификат ФСТЭК №1973 09.12.2015 г.; СЗИ Dallas Lock 8.0 К Сертификат ФСТЭК №2720 25.09.2015; СЗИ Dallas Lock 8.0 С Сертификат ФСТЭК №2945 16.08.2013.

7 Материально-техническое обеспечение дисциплины (модуля)

Необходимый для реализации образовательной программы перечень материально-технического обеспечения включает:

- лекционные аудитории (оборудованные видеопроекционным оборудованием для презентаций; средствами звуковоспроизведения; экраном; имеющие выход в Интернет);
- помещения для проведения лабораторных и практических занятий (оборудованные учебной мебелью);
- библиотеку (имеющую рабочие места для студентов, оснащенные компьютерами с доступом к базам данных и Интернет);
- компьютерные классы.

Обеспеченность процесса обучения техническими средствами полностью соответствует требованиям ФГОС по специальности 10.05.03. Материально-техническая база приведена в лицензионных формах и расположена во внутренней сети по адресу http://education.vsuet.ru.

Аудитории для проведения лекционных, практических и лабораторных занятий, текущего контроля и промежуточной аттестации:

Учебная аудитория № 401 для проведения лекционных занятий, текущего контроля и	Комплект мебели для учебного процесса – 80 шт. Переносной проектор Acer. Аудио-визуальная система лекци-	Microsoft Windows 8.1, Microsoft Office 2007 Standart, Microsoft Office 2007 Russian Academic OPEN No Level #44822753

промежуточной аттестации	онных аудиторий (мультимедийный проектор EpsonEB-X18, настенный экран ScreenMedia)	от 17.11.2008 http://eopen.microsoft.com
Учебная аудитория. № 332а для проведения для проведения	Комплекты мебели для учебного процесса. ПЭВМ – 12 (компьютер Core i5-4570), стенды – 5 шт.	ОС Alt Linux (Альт Образование 8.2) Geany. Lazarus. Qt Creator. Quanta Plus. Веб-редактор Bluefish. Среда разработки Code::Blocks. Офисный пакет Libre Office 5.4: Base, Calc, Draw, Impress, Math, Writer. Персональная бухгалтерия HomeBank. Словарь Star Dict. iTest. VM Maxima. Кумир. Avidemux. Audacios. Brasero. Cheese. SMPlayer. Медиаплеер Parole. Редактор тегов Easy TAG. Stath Studio. Pinta. Веб-браузер Mozilla Firefox. Графический редактор. FP – free Pascal.

Аудитория для самостоятельной работы обучающихся, курсового и дипломного проектирования

Учебная аудитория № 424 для самостоятельной работы обучающихся, курсового и дипломного проектирования	Ауд. 424: Комплекты мебели для учебного процесса. ПЭВМ – 12: рабочая станция Регард РДЦБ.; стенды – 3	ОС Alt Linux (Альт Образование 8.2) Geany. Lazarus. Qt Creator. Quanta Plus. Веб-редактор Bluefish. Среда разработки Code::Blocks. Офисный пакет Libre Office 5.4: Base, Calc, Draw, Impress, Math, Writer. Персональная бухгалтерия HomeBank. Словарь Star Dict. iTest. VM Maxima. Кумир. Avidemux. Audacios. Brasero. Cheese. SMPlayer. Медиаплеер Parole. Редактор тегов Easy TAG. Stath Studio. Pinta. Веб-браузер Mozilla Firefox. Графический редактор. FP – free Pascal.

Дополнительно самостоятельная работа обучающихся может осуществляться при использовании:

Читальные залы библиотеки.	Компьютеры со свободным доступом в сеть Интернет и Электронными библиотечными и информационно справочными системами.	Microsoft Office Professional Plus 2010 Microsoft Open License Microsoft Office Professional Plus 2010 Russian Academic OPEN 1 License No Level #48516271 от17.05.2011 г. http://eooen.microsoft.com Microsoft Office 2007 Standart, Microsoft Open License Microsoft Office 2007 Russian Academic OPEN No Level #44822753 от 17.11.2008 http://eopen.microsoft.com Microsoft Windows XP, Microsoft Open License Academic OPEN No Level #44822753 от 17.11.2008 http://eopen.microsoft.com. Adobe Reader XI, (бесплатное ПО) httos://acrobat.adobe.com/ru/ru/acrobat/odfreader/volume-distribution.html

8 Оценочные материалы для промежуточной аттестации обучающихся по дисциплине

Оценочные материалы (ОМ) для дисциплины включают:

- перечень компетенций с указанием индикаторов достижения компетенций, этапов их формирования в процессе освоения образовательной программы;

- описание шкал оценивания;

- типовые контрольные задания или иные материалы, необходимые для оценки знаний, умений, навыков;

- методические материалы, определяющие процедуры оценивания знаний, умений, навыков и (или) опыта деятельности.

ОМ представляются отдельным комплектом и **входят в состав рабочей программы дисциплины.**

Оценочные материалы формируются в соответствии с П ВГУИТ «Положение об оценочных материалах».

ОЦЕНОЧНЫЕМАТЕРИАЛЫ

ДЛЯ ПРОМЕЖУТОЧНОЙ АТТЕСТАЦИИ

по дисциплине

Разработка и эксплуатация автоматизированных систем в защищенном исполнении

1 Перечень компетенций с указанием этапов их формирования

№ п/п	Код компетенции	Формулировка компетенции	Код и наименование индикатора достижения компетенции
1	ОПК-11	Способен разрабатывать компоненты систем защиты информации автоматизированных систем	ИД1опк-11 – обладает способностью проводить анализ защищённости автоматизированных систем

Код и наименование индикатора достижения компетенции	Результаты обучения (показатели оценивания)
ИД1опк-11 – обладает способностью проводить анализ защищённости автоматизированных систем	Знает особенности проведения анализ защищённости автоматизированных систем
	Умеет проводить анализ защищённости автоматизированных систем
	Владеет способностью проводить анализ защищённости автоматизированных систем

№ п/п	Перечень компетенций		Этапы формирования компетенций		
	Код компетенции	Содержание компетенции (результат освоения)	В результате изучения учебной дисциплины обучающийся должен:		
			знать	уметь	владеть
1	ОПК-11	Способен разрабатывать компоненты систем защиты информации автоматизированных систем	особенности проведения анализ защищённости автоматизированных систем	проводить анализ защищённости автоматизированных систем	способностью проводить анализ защищённости автоматизированных систем

2 Паспорт фонда оценочных средств по дисциплине

№ п/п	Разделы дисциплины	Индекс контролируемой компетенции (или ее части)	Оценочные средства		Технология/процедура оценивания (способ контроля)
			наименование	№№ заданий	
1	Теоретические основы построения защищенных автоматизированных систем	ОПК-11	Тест	1-12	Компьютерное тестирование Процентная шкала. 0-100 %; 0-59,99% - неудовлетворительно; 60-74,99% - удовлетворительно; 75- 84,99% -хорошо; 85-100% - отлично.
			Собеседование (вопросы для зачета)	61-63	Проверка преподавателем Отметка в системе «зачтено – не зачтено»
			Собеседование (задания для лабораторной работы)	71-74	Компьютерное тестирование Процентная шкала. 0-100 %; 0-59,99% - неудовлетворительно; 60-74,99% - удовлетворительно; 75- 84,99% -хорошо; 85-100% - отлично.
			Собеседование (задания для практических рбои)	87-89	Компьютерное тестирование Процентная шкала. 0-100 %; 0-59,99% - неудовлетворительно; 60-74,99% - удовлетворительно; 75- 84,99% -хорошо; 85-100% - отлично.
			Домашнее задание	98-101	Проверка преподавателем Отметка в системе «зачтено – не зачтено»
2	Угрозы безопасности автоматизированных систем.	ОПК-11	Тест	13-29	Компьютерное тестирование Процентная шкала. 0-100 %; 0-59,99% - неудовлетворительно; 60-74,99% - удовлетворительно; 75- 84,99% -хорошо; 85-100% - отлично.
			Собеседование (вопросы для зачета)	64-66	Проверка преподавателем Отметка в системе «зачтено – не зачтено»
			Собеседование (задания для лабораторной работы)	75-78	Компьютерное тестирование Процентная шкала. 0-100 %; 0-59,99% - неудовлетворительно; 60-74,99% - удовлетворительно; 75- 84,99% -хорошо; 85-100% - отлично.
			Собеседование (задания для практических рбои)	90-91	Компьютерное тестирование Процентная шкала. 0-100 %; 0-59,99% - неудовлетворительно; 60-74,99% - удовлетворительно; 75- 84,99% -хорошо; 85-100% - отлично.
			Домашнее задание	102-104	Проверка преподавателем Отметка в системе «зачтено – не зачтено»
3	Проектирование за-	ОПК-11	Тест	30-40	Компьютерное тестирование Процентная шкала. 0-100 %;

	щищенных автоматизированных систем.				0-59,99% - неудовлетворительно; 60-74,99% - удовлетворительно; 75- 84,99% -хорошо; 85-100% - отлично.
			Собеседование (вопросы для зачета)	67-69	Проверка преподавателем Отметка в системе «зачтено – не зачтено»
			Собеседование (задания для лабораторной работы)	79-83	Компьютерное тестирование Процентная шкала. 0-100 %; 0-59,99% - неудовлетворительно; 60-74,99% - удовлетворительно; 75- 84,99% -хорошо; 85-100% - отлично.
			Собеседование (задания для практических рбои)	92-93	Компьютерное тестирование Процентная шкала. 0-100 %; 0-59,99% - неудовлетворительно; 60-74,99% - удовлетворительно; 75- 84,99% -хорошо; 85-100% - отлично.
			Домашнее задание	105-109	Проверка преподавателем Отметка в системе «зачтено – не зачтено»
4	Методы обеспечения безопасности защищенных автоматизированных систем	ОПК-11	Тест	41-60	Компьютерное тестирование Процентная шкала. 0-100 %; 0-59,99% - неудовлетворительно; 60-74,99% - удовлетворительно; 75- 84,99% -хорошо; 85-100% - отлично.
			Собеседование (вопросы для зачета)	69-70	Проверка преподавателем Отметка в системе «зачтено – не зачтено»
			Собеседование (задания для лабораторной работы)	84-86	Компьютерное тестирование Процентная шкала. 0-100 %; 0-59,99% - неудовлетворительно; 60-74,99% - удовлетворительно; 75- 84,99% -хорошо; 85-100% - отлично.
			Собеседование (задания для практических рбои)	94-97	Компьютерное тестирование Процентная шкала. 0-100 %; 0-59,99% - неудовлетворительно; 60-74,99% - удовлетворительно; 75- 84,99% -хорошо; 85-100% - отлично.
			Домашнее задание	110-113	Проверка преподавателем Отметка в системе «зачтено – не зачтено»

3 Оценочные материалы для промежуточной аттестации.

Типовые контрольные задания или иные материалы, необходимые для оценки знаний, умений, навыков и (или) опыта деятельности, характеризующих этапы формирования компетенций в процессе освоения образовательной программы

Для оценки знаний, умений, навыков студентов по дисциплине применяется бальнорейтинговая система оценки сформированности компетенций студента.

Бально-рейтинговая система оценки осуществляется в течение всего семестра при проведении аудиторных занятий и контроля самостоятельной работы. Показателями ОМ являются: текущий опрос в виде собеседования на лабораторных работах, практических занятиях, тестовые задания в виде решения контрольных работ на практических работах и самостоятельно (домашняя контрольная работа) и сдачи курсовой работы по предложенной преподавателем теме. Оценки выставляются в соответствии с графиком контроля текущей успеваемости студентов в автоматизированную систему баз данных (АСУБД) «Рейтинг студентов».

Обучающийся, набравший в семестре более 60 % от максимально возможной бально-рейтинговой оценки работы в семестре получает зачет автоматически.

Студент, набравший за текущую работу в семестре менее 60 %, т.к. не выполнил всю работу в семестре по объективным причинам (болезнь, официальное освобождение и т.п.) допускается до зачета, однако ему дополнительно задаются вопросы на собеседовании по разделам, выносимым на зачет.

Аттестация обучающегося по дисциплине проводится в форме тестирования и предусматривает возможность последующего собеседования (экзамена). Зачет проводится в виде тестового задания.

Каждый вариант теста включает 15 контрольных заданий, из них:

- 5 контрольных заданий на проверку знаний;
- 5 контрольных заданий на проверку умений;
- 5 контрольных заданий на проверку навыков;

В случае неудовлетворительной сдачи зачета студенту предоставляется право повторной сдачи в срок, установленный для ликвидации академической задолженности по итогам соответствующей сессии. При повторной сдаче зачета количество набранных студентом баллов на предыдущем зачете не

3.1 Тесты *(тестовые задания)*

3.1.1 Шифр и наименование компетенции

ОПК-11 - Способен разрабатывать компоненты систем защиты информации автоматизированных систем

№ задания	Тестовое задание
1.	Перечислите разделение информации по степени важности: Ответ: 1) жизненно важная незаменимая информация;2) важная информация; 3) полезная информация; 4) несущественная информация.
2.	Защищенность информации это: 1) процесс создания и использования в автоматизированных системах специальных механизмов, поддерживающих установленный статус её защищенности. **2) поддержание на заданном уровне тех параметров находящейся в автоматизированной системе информации, которые характеризуют установленный статус её хранения, обработки и использования.** 3) организованная совокупность средств, методов и мероприятий, используемых для регулярной обработки информации в процессе решения определенного круга прикладных задач. 4) организационно-технический комплекс электронных средств, специального математического и программного обеспечения, предназначенный для повышения эффективности управления путем автоматизации процессов сбора, обработки, хранения и выдачи инфор-

	мации, необходимой для выработки управляющих воздействий, передачи команд (сигналов), решения расчетных информационных задач.
3.	Перечислите группы лиц, связанных с обработкой информации. Ответ: 1) держатель; 2) источник; 3) нарушитель.
4.	Автоматизированная система это **1**) поддержание на заданном уровне тех параметров находящейся в автоматизированной системе информации, которые характеризуют установленный статус её хранения, обработки и использования **2) организованная совокупность средств, методов и мероприятий, используемых для регулярной обработки информации в процессе решения определенного круга прикладных задач.** 3) процесс создания и использования в автоматизированных системах специальных механизмов, поддерживающих установленный статус её защищенности. 4) целенаправленное регулярное применение в автоматизированных системах средств и методов, а также осуществление мероприятий с целью поддержания заданного уровня защищенности информации по всей совокупности показателей и условий, являющихся существенными с точки зрения обеспечения безопасности информации
5.	Защита информации это: 1) поддержание на заданном уровне тех параметров находящейся в автоматизированной системе информации, которые характеризуют установленный статус её хранения, обработки и использования. **2) процесс создания и использования в автоматизированных системах специальных механизмов, поддерживающих установленный статус её защищенности.** 3) организованная совокупность средств, методов и мероприятий, используемых для регулярной обработки информации в процессе решения определенного круга прикладных задач. 4) результат отражения и обработки в человеческом сознании многообразия внутреннего и окружающего мира; это сведения об окружающих человека предметах, явлениях природы, деятельности других людей и т. д., а также сведения о его внутреннем состоянии
6.	Перечислите три базовых принципа, которые должна обеспечивать информационная безопасность Ответ: 1) Конфиденциальность; 2) Целостность; 3) доступность.
7.	Система – это 1) **множество элементов находящихся в отношениях или связях друг с другом, образующие целостность или органическое единство.** 2) выделение совокупности функций (целенаправленных действий) системы и ее компонентов направленное на достижение определённой цели. 3) понимание системы как нерасчленимого целого, взаимодействующего с внешней средой. 4) любая часть системы, вступающая в определенные отношения с другими частями (подсистемами, элементами)
8.	Компонент это 1) множество элементов находящихся в отношениях или связях друг с другом, образующие целостность или органическое единство. 2) выделение совокупности функций (целенаправленных действий) системы и ее компонентов направленное на достижение определённой цели. 3) понимание системы как нерасчленимого целого, взаимодействующего с внешней средой. **4) любая часть системы, вступающая в определенные отношения с другими частями (подсистемами, элементами)**
9.	Функциональные представление систем это 1) множество элементов находящихся в отношениях или связях друг с другом, образующие целостность или органическое единство. **2) выделение совокупности функций (целенаправленных действий) системы и ее компонентов направленное на достижение определённой цели.** 3) понимание системы как нерасчленимого целого, взаимодействующего с внешней средой. 4) любая часть системы, вступающая в определенные отношения с другими частями (подсистемами, элементами)
10.	Макроскопическое представление это 1) множество элементов находящихся в отношениях или связях друг с другом, образующие целостность или органическое единство. 2) выделение совокупности функций (целенаправленных действий) системы и ее компонентов направленное на достижение определённой цели. **3) понимание системы как нерасчленимого целого, взаимодействующего с внешней средой.**

	4) любая часть системы, вступающая в определенные отношения с другими частями (подсистемами, элементами).
11.	Что означает термин ПРАВОВЫЕ МЕРЫ ЗАЩИТЫ ИНФОРМАЦИИ? Выберите один ответ: **1) Это действующие в стране законы, указы и другие нормативные акты, регламентирующие правила обращения с информацией и ответственность за их нарушения.** 2) Это традиционно сложившиеся в стране или обществе нормы поведения и правила обращения с информацией. 3) Это меры, регламентирующие процессы функционирования системы обработки данных, использования её ресурсов. 4) Это действующие в стране законы, регламентирующие процессы функционирования системы обработки данных, использования её ресурсов
12.	Что означает термин БЕЗОПАСНОСТЬ ИНФОРМАЦИИ Выберите один ответ: 1)Потенциально возможное событие, действие, процесс или явление, которое может привести к нарушению конфиденциальности, целостности, доступности информации, а также неправомерному её тиражированию. 2)Свойство системы, в которой циркулирует информация, характеризующееся способностью обеспечивать своевременный беспрепятственный доступ к информации субъектов, имеющих на это надлежащие полномочия. **3)Защищенность информации от нежелательного её разглашения, искажения, утраты или снижения степени доступности информации, а также незаконного её тиражирования.** 4) целенаправленное регулярное применение в автоматизированных системах средств и методов, а также осуществление мероприятий с целью поддержания заданного уровня защищенности информации по всей совокупности показателей и условий, являющихся существенными с точки зрения обеспечения безопасности информации.
13.	Угроза – это **1) потенциально возможное событие, явление или процесс, которое посредством воздействия на компоненты информационной системы может привести к нанесению ущерба.** 2) это любая характеристика или свойство информационной системы, использование которой нарушителем может привести к реализации угрозы. 3) это любое действие нарушителя, которое приводит к реализации угрозы путём использования уязвимостей информационной системы. 4) множество элементов находящихся в отношениях или связях друг с другом, образующие целостность или органическое единство.
14.	Уязвимость это 1) потенциально возможное событие, явление или процесс, которое посредством воздействия на компоненты информационной системы может привести к нанесению ущерба. **2) это любая характеристика или свойство информационной системы, использование которой нарушителем может привести к реализации угрозы.** 3) это любое действие нарушителя, которое приводит к реализации угрозы путём использования уязвимостей информационной системы. 4) множество элементов находящихся в отношениях или связях друг с другом, образующие целостность или органическое единство.
15.	Атака – это 1) потенциально возможное событие, явление или процесс, которое посредством воздействия на компоненты информационной системы может привести к нанесению ущерба. 2) это любая характеристика или свойство информационной системы, использование которой нарушителем может привести к реализации угрозы. **3) это любое действие нарушителя, которое приводит к реализации угрозы путём использования уязвимостей информационной системы**. 4) множество элементов находящихся в отношениях или связях друг с другом, образующие целостность или органическое единство.
16.	Все угрозы условно можно разделить на две большие группы. Перечислите их. Ответ: 1) угрозы утечки информации по техническим каналам связи; 2) угрозы несанкционированного доступа к информации.
17.	К техническим каналам утечки видовой информации относятся: Выберите один или несколько вариантов ответа. **1) Наблюдение за объектами.** **2) Съёмка объектов.**

	3) Съёмка документов. 4) Прослушивание объектов.
18.	Дать определение защите от несанкционированного доступа (Защита от НСД) Ответ: предотвращение или существенное затруднение НСД.
19.	Какие программы относятся к программам Конструкторы вирусов? Выберите один ответ: 1) Это программы, наносящие какие-либо разрушительные действия, т.е. в зависимости от определенных условий или при каждом запуске уничтожающие информацию на дисках, приводящие систему к зависанию и т.п. 2) Это программы, которые на первый взгляд являются стопроценными вирусами, но неспособны размножаться по причине ошибок. Например, вирус, который при заражении "забывает" поместить в начало файлов команду передачи управления на код вируса. **3)Это утилита, предназначенная для изготовления новых компьютерных вирусов. Они позволяют генерировать исходные тексты вирусов (ASM-файлы), объектные модули и/или непосредственно зараженные файлы.** 4)Главной функцией подобного рода программ является шифрование тела вируса и генерация соответствующего расшифровщика
20.	Что необходимо сделать при обнаружении загрузочного вируса? Выберите один ответ: **1) Компьютер от сети отключать не следует, так как вирусы этого типа по сети не распространяются.** 2) Компьютер необходимо отключить от сети и проинформировать системного администратора. 3) Вместо отключения компьютера от сети достаточно на период «лечения» убедиться в том, что соответствующий редактор неактивен. 4) Все вышеперечисленные варианты.
21.	В чем заключается принцип работы загрузочного вируса? Выберите один ответ: **1) Вирусы записывают себя либо в загрузочный сектор диска, либо в сектор, содержащий системный загрузчик винчестера, либо меняет указатель на активный boot-сектор** 2) Вирусы либо различными способами внедряются в выполняемые файлы, либо создают файлы-двойники, либо используют особенности организации файловой системы 3) Вирусы заражают файлы-документы и электронные таблицы популярных редакторов 4) Вирусы используют для своего распространения протоколы или команды компьютерных сетей и электронной почты
22.	Что необходимо сделать при обнаружении макровируса? Выберите один ответ: 1) Компьютер необходимо отключить от сети и проинформиравать системного администратора 2) Компьютер от сети отключать не следует, так как вирусы этого типа по сети не распространяются. **3) Вместо отключения компьютера от сети достаточно на период «лечения» убедиться в том, что соответствующий редактор неактивен** 4) Все вышеперечисленные операции.
23.	В чем заключается принцип работы файлового вируса? Выберите один ответ: **1) Вирусы либо различными способами внедряются в выполняемые файлы, либо создают файлы-двойники, либо используют особенности организации файловой системы**. 2) Записывают себя либо в загрузочный сектор диска, либо в сектор, содержащий системный загрузчик винчестера, либо меняют указатель на активный boot-сектор. 3) Вирусы заражают файлы-документы и электронные таблицы популярных редакторов. 4)Вирусы используют для своего распространения протоколы или команды компьютерных сетей и электронной почты.
24.	Теневое копирование выводимых данных: Выберите один ответ: 1) Обеспечивает сохранение всей информации выводимой на экран. **2) Обеспечивает создание в системе дубликатов данных, выводимых на отчуждаемые носители информации.** 3) Обеспечивает сохранение всей информации передаваемой по сетевым ресурсам. 4) Обеспечивает сохранение информации создаваемой в текстовых редакторах

25.	При выборе модели злоумышленника следует: Выберите один ответ: **1) Учитывать квалификацию злоумышленника, его оснащенность (возможности) и официальный статус в компьютерной системе.** 2) Учитывать параметры средств ведения информационной разведки, которые может применить злоумышленник. 3) Знать психологию поведения злоумышленника. 4) Знать программные средства которые он использует.
26.	Основными способами несанкционированного доступа к компьютерной информации являются следующие: Выберите один ответ: **1) Преодоление программных средств защиты, несанкционированное копирование информации, внедрение программных закладок и компьютерных вирусов.** 2) Подслушивание, визуальное наблюдение, хищение документов и машинных носителей информации, подкуп и шантаж сотрудников. 3) Использование ошибок и небрежность пользователей, перехват побочных электромагнитных излучений. 4) Применение технических средств разведки
27.	Какие средства защиты фиксируют факт проникновения злоумышленника в компьютерную систему? Выберите один ответ: **1) Функция аудита безопасности компьютерной системе.** 2) Средства охранно-пожарной сигнализации. 3) Пломбы, наклейки, замки на аппаратуре компьютерной системы. 4) Средства биометрической идентификации
28.	Для защиты от несанкционированного изменения структуры компьютерной системы в процессе эксплуатации следует обеспечить: Выберите один ответ: 1) Использование современных технологий программирования, наличие автоматизированных контрольно-испытательных стендов, наличие трансляторов для обнаружения закладок. 2) Применение стандартных блоков, контроль адекватности, контроль процесса разработки, сертификацию готового продукта. **3) Охрану помещений, разграничение доступа к оборудованию, противодействие внедрению вредоносных программ.** 4) Все вышеперечисленные методы.
29.	Для увеличения времени преодоления защиты злоумышленником при построении системы защиты информации следует учитывать принцип Выберите один ответ: **1) Многоуровневой структура СЗИ.** 2) Параллельной разработки компьютерной системы и СЗИ. 3) Иерархической системы управления СЗИ. 4)Блочной архитектуры защищенной компьютерной системы
30.	Совокупность аппаратных и программных средств для подготовки и создания образца печатной продукции готового для тиражирования – это Выберите один ответ: **1) настольная издательская система.** 2) геоинформационная система. 3)реляционная база данных. 4) операционная система.
31.	В чем заключается криптографическое преобразование информации? Выберите один ответ: **1) В преобразовании информации с помощью специальных алгоритмов либо аппаратных решений и кодов ключей, т.е. в приведении её к неявному виду.** 2) В создании некоторой физической замкнутой преграды вокруг объекта защиты с организацией контролируемого доступа лиц, связанных с объектом защиты по своим функциональным обязанностям. 3) В разделении информации, циркулирующей в объекте защиты, на части и организации доступа к ней должностных лиц в соответствии с их функциональными обязанностями и полномочиями. 4) В том, что из числа допущенных к ней должностных лиц выделяется группа, которой предоставляется доступ только при одновременном предъявлении.
32.	Основными этапами классификации АС являются:

	Выберите один или несколько вариантов ответа. **1) разработка и анализ исходных данных;** **2) выявление основных признаков АС, необходимых для классификации;** **3) сравнение выявленных признаков АС с классифицируемыми;** **4) присвоение АС соответствующего класса защиты информации от НСД;** 5) Аккредитация АС.
33.	Система взаимодействующих элементов, связанных между собой по выделенным или коммутируемым линиям для обеспечения локальной или удаленной связи (голосовой, визуальной, обмена данными и т.п.) и для обмена сведениями между пользователями, имеющими общие интересы, это… Выберите один ответ: **1) Сеть** 2) Портал 3) Блог 4) Протокол
34.	Сервер - это: Выберите один ответ: **1) компьютер, предоставляющий в доступ пользователям какие-либо ресурсы.** 2) компьютер, имеющий подключение к сети Интернет. 3) переносной компьютер. 4) рабочая станция. 5) компьютер с модемом, подключенный к телефонной линии.
35.	Буфер обмена принадлежит: Выберите один ответ: 1) графическому редактору Microsoft Paint. 2) текстовому редактору Microsoft Word. **3)операционной системе Microsoft Windows.** 4)электронным таблицам Microsoft Excel. 5)ни одному из выше перечисленного.
36.	Механизм замкнутой программной среды: Выберите один ответ: 1) Позволяет производить блокировку работы пользователя при НСД. 2) Позволяет осуществлять кодирование файлов и папок. 3) Позволят производить разграничение доступа пользователя к настройкам операционной системы. **4) Позволяет явно указать с какими программами пользователь может работать**
37.	Принимает ли участие служба безопасности в разработке проектов по новым информационным системам? Выберите один ответ: 1) Инициирует разработку проектов. 2) Нет 3) Возглавляет разработку проектов. **4) Да**
38.	Одной из основных функций систем виртуальной частной сети (VPN) является: Выберите один ответ: 1) Шифрования данных в сетевом пакете. **2) Сокрытия информации заголовка сетевого пакета.** 3) Использование выделенной линии связи. 4) Сокрытия факта передачи информации по цифровым сетям связи
39.	Для контроля целостности программной структуры в процессе эксплуатации используется: Выберите один ответ: 1) Сравнение параметров рабочих программных файлов с дистрибутивами. 2)Проверка списка файлов программного обеспечения. **3)Контрольное суммирование, хэш-функция.** 4) Резервное копирование
40.	Функция proxy-сервера межсетевого экрана предназначена для: Выберите один ответ: 1) Фильтрации на транспортном уровне запросов на установление виртуальных соединений. 2) Централизованного управления всеми межсетевыми экранами организации. **3) Скрытия от внешних абонентов истинных внутренних адресов защищаемой локальной сети**. 4) Фильтрации пакетов служебных протоколов, служащих для диагностики и управления ра-

	ботой сетевых устройств.
41.	Аутентификация – это 1) **процесс, в ходе которого на основании пароля, ключа или какой-либо иной информации, пользователь подтверждает, что является именно тем, за кого себя выдаёт**. 2) процесс, в ходе которого выясняются права доступа, привилегии, свойства и характеристики пользователя на основании его имени, логина или какой-либо другой информации о нём. 3) это совокупность целенаправленных действий, включающих в себя оценку ситуации и состояния объектов управления, выбор управляющих воздействий и их реализацию (планирование и внедрение мер обеспечения безопасности). 4) это любое действие нарушителя, которое приводит к реализации угрозы путём использования уязвимостей информационной системы.
42.	Идентификация – это 1) процесс, в ходе которого на основании пароля, ключа или какой-либо иной информации, пользователь подтверждает, что является именно тем, за кого себя выдаёт. **2) процесс, в ходе которого выясняются права доступа, привилегии, свойства и характеристики пользователя на основании его имени, логина или какой-либо другой информации о нём.** 3) это совокупность целенаправленных действий, включающих в себя оценку ситуации и состояния объектов управления, выбор управляющих воздействий и их реализацию (планирование и внедрение мер обеспечения безопасности). 4) это любое действие нарушителя, которое приводит к реализации угрозы путём использования уязвимостей информационной системы.
43.	Управление – это 1) процесс, в ходе которого на основании пароля, ключа или какой-либо иной информации, пользователь подтверждает, что является именно тем, за кого себя выдаёт. 2) процесс, в ходе которого выясняются права доступа, привилегии, свойства и характеристики пользователя на основании его имени, логина или какой-либо другой информации о нём. **3) это совокупность целенаправленных действий, включающих в себя оценку ситуации и состояния объектов управления, выбор управляющих воздействий и их реализацию (планирование и внедрение мер обеспечения безопасности).** 4) это любое действие нарушителя, которое приводит к реализации угрозы путём использования уязвимостей информационной системы.
44.	Защита информации в VPN (виртуальных частных сетях) обеспечивается с помощью: Выберите один ответ: 1) Межсетевых экранов и шифрования трафика. 2) Физической защиты информационных линий связи. 3) Журналирования событий безопасности. **4) Инкапсуляции и декапсуляции сетевых пакетов**.
45.	Информационное право составляет: Выберите один ответ: **1) нормативную базу информационного общества.** 2) государственную политику. 3)нормативную базу аграрного общества. 4)нормативную базу доиндустриального общества
46.	Применение векторной графики по сравнению с растровой: Выберите один ответ: 1) не меняет способы кодирования изображения 2) увеличивает объем памяти, необходимой для хранения изображения 3) не влияет на объем памяти, необходимой для хранения изображения, и на трудоемкость редактирования изображения **4) сокращает объем памяти, необходимой для хранения изображения, и облегчает редактирование последнего**
47.	Объединение компьютеров в сеть Выберите один ответ: 1) Объединяет угрозы каждого подключаемого компьютера. **2) Увеличивает количество угроз информации компьютерной системе.** 3) Не влияет на количество угроз информации компьютерной системе. 4) Уменьшает количество угроз информации компьютерной системе
48.	Межсетевой экран применяется для: Выберите один ответ:

	1) Организации шифрованного сетевого соединения. **2) Разграничения доступа между двумя сетями с различными требованиями по обеспечению безопасности.** 3) Контроля почтового трафика и Web-трафика. 4) Обнаружения сетевых атак или подозрительных намерений злоумышленника
49.	Какой принцип управления межсетевым экраном предпочтительнее в компьютерной системе, обрабатывающей конфиденциальную информацию? Выберите один ответ: 1) Контроля сетевых соединений. 2) Разрешено все, что не запрещено. **3) Запрещено все, что не разрешено**. 4) Выборочной фильтрации трафика.
50.	Какой этап построения системы защиты информации заканчивается выработкой технического задания? Выберите один ответ: 1) Этап эскизного проектирования. 2) Этап производства опытного образца. 3) Этап опытно-конструкторской разработки. **4) Этап научно-исследовательской разработки**.
51.	Что относится к основным механизмам защиты компьютерной системы от несанкционированного доступа? Выберите один ответ: 1) Дублирование информации, создание отказоустойчивых компьютерных систем, блокировка ошибочных операций. 2) Антивирусное ПО, защита от аварий и стихийных бедствий. **3) Идентификация и аутентификация пользователей, разграничение доступа, шифрование, физическая защита компонент компьютерной системы.** 4) Сегментация сетей с помощью коммутаторов и межсетевых экранов, шифрование информации.
52.	Кто должен анализировать и очищать журнал аудита безопасности компьютерной системы? Выберите один ответ: 1) Пользователь. 2) Начальник. 3) Администратор. **4) Аудитор.**
53.	Почему система защиты информации должна иметь несколько уровней (рубежей) перекрывающих друг друга? Выберите один ответ: **1) Чтобы злоумышленник последовательно «взламывал» все уровни защиты.** 2) Для построения блочной архитектуры защищенной компьютерной системы 3) За передним уровнем не видно последующего. 4) Чтобы обеспечить иерархическую систему управления
54.	В каком случае внедрение решений по защите информации происходит быстрее: Выберите один ответ: 1) В случае дружеских отношений с директором. 2) При наличии большого количества свободных денег в организации. 3) В случае рассмотрения Советом безопасности организации вопросов защиты информации. **4) В случае прямого подчинения службы информационной безопасности руководителю организации.**
55.	как оценить эффективность службы информационной безопасности? Выберите один ответ: **1) По журналу фиксации и анализа инцидентов.** 2) Со слов администратора безопасности. 3) Используя технологии управления рисками. 4) Из доклада начальника службы информационной безопасности.
56.	Контроль целостности предназначен для: Выберите один ответ: 1) Выявления вредоносного программного обеспечения. **2) Слежения за неизменностью контролируемых объектов:** 3) Выявления нештатного подключения внешних устройств. 4) Выявления НСД

57.	Какие основные способы разграничения доступа применяются в компьютерных системах? Выберите один ответ: 1) Парольное разграничение доступа и иерархическое. **2) Дискреционный и мандатный.** 3) По специальным спискам и многоуровневый. 4) По группам пользователей и специальным разовым разрешениям
58.	Под экспериментальным подходом к оценке эффективности системы защиты информации понимается Выберите один ответ: 1) Организация процесса определения эффективности СЗИ путем математического моделирования. 2) Организация процесса определения эффективности существующих СЗИ путем анализа работоспособности средств и механизмов системы защиты информации специалистами отдела безопасности. **3) Организация процесса определения эффективности существующих СЗИ путем попыток преодоления защитных механизмов системы специалистами, выступающими в роли злоумышленников.** 4) Организация процесса определения эффективности существующих СЗИ путем анализа работоспособности средств и механизмов системы защиты информации специалистами ФСТЭК.
59.	Системы обнаружения атак предназначены для: Выберите один ответ: 1) Предотвращения атаки на компьютерную систему в режиме реального времени. 2) Ведения базы данных совершенных атак в локальной сети. 3) Сообщения об атаке на компьютерную систему администратору в процессе ее совершения. **4) Обнаружения совершенных атак для проведения расследования инцидента**.
60.	Что такое аудит безопасности компьютерной системы? Выберите один ответ: 1) Инструмент политики безопасности, позволяющий наблюдать динамические изменения технического состояния аппаратных компонентов компьютера (температура материнской платы, скорость вращения вентилятора на процессоре и т.д.). 2) Инструмент политики безопасности, позволяющий контролировать процесс загрузки системных драйверов. 3) Инструмент политики безопасности, направленный на проверку реализованных в автоматизированной информационной системе процедур обеспечения безопасности с целью оценки их эффективности и корректности. **4) Инструмент политики безопасности, позволяющий отслеживать действия пользователей и системные события и регистрировать их в журнале**

Критерии и шкалы оценки:

Процентная шкала **0-100 %; отметка в системе**

«неудовлетворительно, удовлетворительно, хорошо, отлично»

0-59,99% - неудовлетворительно;

60-74,99% - удовлетворительно;

75- 84,99% -хорошо;

85-100% - отлично.

3.2 Собеседование (вопросы к устному ответу для зачета)

3.2.1 Шифр и наименование компетенции

ОПК-11 - Способен разрабатывать компоненты систем защиты информации автоматизированных систем.

61.	**История развития, назначение и роль автоматизированных систем.** Ответ: АИС - это человеко-машинная система, обеспечивающая автоматизированную подготовку, поиск и обработку информации в рамках интегрированных сетевых, компьютерных и коммуникационных технологий для оптимизации экономической и другой деятельности в различных сферах управления. Существуют основные 4 этапа развития автоматизированных систем: 1 этап. Первые информационные системы появились в 50-х гг. В эти годы они были предназначены для обработки счетов и расчета зарплаты, а реализовывались на электромеханических бухгалтерских счетных машинах. Это приводило к некоторому сокращению затрат и времени на подготовку бумажных документов. 2 этап. 60-е гг. знаменуются изменением отношения к информационным системам. Информация, полученная из них, стала применяться для периодической отчетности по многим параметрам. Для этого организациям требовалось компьютерное оборудование широкого назначения, способное обслуживать множество функций, а не только обрабатывать счета и считать зарплату, как было ранее. 3 этап. В 70-х - начале 80-х гг. информационные системы начинают широко использоваться в качестве средства управленческого контроля, поддерживающего и ускоряющего процесс принятия решений. 4 этап. К концу 90-х начала 2000 гг. концепция использования информационных систем вновь изменяется. Они становятся стратегическим источником информации и используются на всех уровнях организации любого профиля. Информационные системы этого периода, предоставляя вовремя нужную информацию, помогают организации достичь успеха в своей деятельности, создавать новые товары и услуги, находить новые рынки сбыта, обеспечивать себе достойных партнеров, организовывать выпуск продукции по низкой цене и многое другое.
62.	**Этапы развития информационных систем.** Ответ: Первые ИС появились в 50-х гг. В эти годы они были предназначены для обработки счетов и расчета зарплаты, а реализовывались на электромеханических бухгалтерских счетных машинах. Это приводило к некоторому сокращению затрат и времени на подготовку бумажных документов. 60-е гг. знаменуются изменением отношения к ИС. Информация, полученная из них, стала применяться для периодической отчетности по многим параметрам. Для этого организациям требовалось компьютерное оборудование широкого назначения, способное обслуживать множество функций, а не только обрабатывать счета и считать з/пл. В 70-х - начале 80-х ИС начинают широко использоваться в качестве средства управленческого контроля, поддерживающего и ускоряющего процесс принятия решений. К концу 80-х гг. концепция использования ИС вновь изменяется. Они становятся стратегическим источником информации и используются на всех уровнях организации любого профиля. ИС этого периода, предоставляя вовремя нужную информацию, помогают организации достичь успеха в своей деятельности, создавать новые товары и услуги, находить новые рынки сбыта, обеспечивать себе достойных партнеров, организовывать выпуск продукции по низкой цене и многое другое.
63.	**Классификация автоматизированных систем.** Ответ: Классификация АС производится в соответствии с РД «Автоматизированные системы. Защита от несанкционированного доступа к информации. Классификация автоматизированных систем и требования по защите информации». Настоящий руководящий документ устанавливает классификацию автоматизированных систем, подлежащих защите от несанкционированного доступа к информации, и требования по защите информации в АС различных классов. Основными этапами классификации АС являются: 1) разработка и анализ исходных данных; 2) выявление основных признаков АС, необходимых для классификации; 3) сравнение выявленных признаков АС с классифицируемыми; 4) присвоение АС соответствующего класса защиты информации от НСД. Необходимыми исходными данными для проведения классификации конкретной АС являются: 1) перечень защищаемых информационных ресурсов АС и их уровень конфиденциальности; 2) перечень лиц, имеющих доступ к штатным средствам АС, с указанием их уровня полномочий; 3) матрица доступа или полномочий субъектов доступа по отношению к защищаемым информацион-

	ным ресурсам АС; 4) режим обработки данных в АС. К числу определяющих признаков, по которым производится группировка АС в различные классы, относятся: 1) наличие в АС информации различного уровня конфиденциальности; 2) уровень полномочий субъектов доступа АС на доступ к конфиденциальной информации; 3) режим обработки данных в АС.
64.	**Основные понятия и определения теории сложных систем.** Ответ: Общая теория систем (ОТС) - раздел науки, изучающий самые фундаментальные понятия и аспекты систем: различные явления, отвлекаясь от их конкретной природы и основываясь лишь на формальных взаимосвязях между различными составляющими и на характере их изменения под влиянием внешних условий. При этом результаты всех наблюдений объясняются лишь взаимодействием их компонентов, например, характером их организации и функционирования, а не с помощью непосредственного обращения к природе вовлеченных в явления механизмов (будь они физическими, биологическими, экологическими, социологическими или концептуальными). Для ОТС объектом исследования является не «физическая реальность», а «система», т. е. абстрактная формальная взаимосвязь между основными признаками и свойствами.
65.	**Классификация систем. Функциональная и обеспечивающая часть сложной системы.** Ответ: Система может быть охарактеризована одним или несколькими признаками и соответственно ей может быть найдено место в различных классификациях, каждая из которых может быть полезной при выборе методологии исследования. Сложные системы можно классифицировать на основные группы : 1) По содержанию (характеру происхождения) различают реальные (материальные), объективно существующие, и абстрактные (концептуальные, идеальные), являющиеся продуктом мышления; 2) Реальные системы делятся на естественные (природные системы) и искусственные (антропогенные); 3) По степени сложности системы подразделяются на сложные и простые; 4) По характеру взаимодействия с внешней средой системы подразделяются на открытые и замкнутые(закрытые); 5) По возможности изменения характеристик состояния различают статические и динамические системы; 6) По виду связи между элементами системы классифицируются на детерминированные и стохастические; 7) По характеру функций различают специальные, многофункциональные и универсальные системы; 8)По характеру развития систем различают стабильные и развивающиеся; 9) По степени организованности системы подразделяются на хорошо организованные и плохо организованные (диффузные); 10) По сложности поведения различают автоматические, решающие, самоорганизующиеся, предвидящие, превращающиеся системы; 11) По характеру структуры управления системы могут быть централизованные и децентрализованные; 12) По назначению системы бывают производящими, управляющими и обслуживающими.
66.	**Понятие качества и эффективности сложных систем.** Ответ: Качество сложных системы — это совокупность свойств системы, обусловливающих возможность ее использования для удовлетворения определенных в соответствии с ее назначением потребностей. Эффективность сложных систем - это свойство системы выполнять поставленную цель в заданных условиях использования и с определенным качеством. Показатели эффективности характеризуют степень приспособленности системы к выполнению поставленных перед нею задач и являются обобщающими показателями оптимальности функционирования ИС, зависящими от локальных показателей: надежность, достоверность, безопасность.
67.	**Классификация угроз безопасности АС.** Ответ: 1) По природе возникновения; 2) По степени преднамеренности проявления; 3) По непосредственному источнику угроз; 4) По положению источника угроз; 5) По степени зависимости от активности АС; 6) По степени воздействия на АС; 7) По этапам доступа пользователей или программ к ресурсам АС; 8) По способу доступа к ресурсам АС; 9) По текущему месту расположения информации, хранимой и обрабатываемой в АС; 10) По цели реализации угрозы.
68.	**Методы анализа защищенности АС.** Ответ: 1) изучения исходных данных по АС; 2) оценки рисков, связанных с осуществлением угроз безопасности в отношении ресурсов АС; 3) ручного анализа конфигурационных файлов маршрутизаторов и прокси - серверов, почтовых и DNS-серверов, других критических элементов сетевой инфраструктуры; 4) сканирования внешних сетевых адресов локальной сети; 5) сканирования ресурсов локальной сети изнутри; 6) анализа конфигурации серверов и рабочих станций при помощи специализированных программных агентов.
69.	**Цели и задачи проектирования АС.**

	Ответ: Целями проектирование систем защиты информации заключается в том, чтобы для заданной автоматизированной системы (АС) или ее проекта, создать оптимальные механизмы обеспечения защиты информации и механизмы управления ими. Задачей проектирования систем защиты (АС) является организованные возможности средств, методов и мероприятий, осуществляемых в автоматизированных системах с целью полного или частичного осуществления одной или нескольких функций защиты в одной или нескольких зонах защиты
70.	**Показатели и критерии эффективности** Ответ: Показатели эффективности отражают степень достижения целей предприятия (подразделения, сотрудника) в соотношении к затраченным ресурсам или времени. Такими показателями являются рентабельность, оборачиваемость, производительность труда, капиталоемкость и т.д. Критерий эффективности – это показатель, который позволяет каждой операции, процессу или проекту установить в соответствие число, равное эффективности операции или проекта. То есть, критерий эффективности позволяет из множества альтернативных вариантов выбирать тот, который обеспечивает максимизацию добавленной стоимости системы.

Критерии и шкалы оценки:

- оценка «зачтено» выставляется студенту, если он активно участвует в собеседовании и обсуждении, подготовил аргументы в пользу решения, предложил альтернативы, выслушивал мнения других;

- оценка «не зачтено», если студент выполнял роль наблюдателя, не внес вклада в собеседование и обсуждение.

3.3 Собеседование (вопросы к защите лабораторных работ)
3.3.1 Шифр и наименование компетенции

ОПК-11 - Способен разрабатывать компоненты систем защиты информации автоматизированных систем

№ задания	Формулировка вопроса
71.	Основные средства и способы обеспечения информационной безопасности в автоматизированных Системах
72.	Принципы построения систем защиты информации
73.	Понятие и классификация угроз безопасности автоматизированных систем
74.	Базовая модель угроз безопасности информации
75.	Методика оценки угроз безопасности Информации
76.	Последовательность стадий и содержание этапов разработки автоматизированных систем в защищенном исполнении
77.	Содержание этапов проектирования автоматизированных систем в защищенном исполнении
78.	Требования по защите сведений о создаваемой АС
79.	Модели данных, систем и процессов защиты информации в автоматизированных системах
80.	Технологии автоматизированного проектирования автоматизированных информационных систем
81.	Оценка защищенности АС на основе отечественных стандартов и нормативно- методических документов ФСТЭК России
82.	Понятие и архитектура распределенных автоматизированных систем
83.	Особенности способов и средств защиты информации в распределенных автоматизированных системах
84.	Состав и содержание организационных и технических мер по защите информационных систем персональных данных
85.	Порядок обеспечения защиты информации при эксплуатации АС
86.	Общие обязанности администратора информационной безопасности автоматизированной системы

Процентная шкала 0-100 %;
85-100% - отлично (практическое задание выполнено в установленный срок с использованием рекомендаций преподавателя; показан высокий уровень знания изученного материала по заданной теме, проявлен творческий подход, умение глубоко анализировать проблему и делать обобщающие практико-ориентированные выводы; работа выполнена без ошибок и недочетов или допущено не более одного недочета);
75- 84,99% - хорошо (практическое задание выполнено в установленный срок с использованием рекомендаций преподавателя; показан хороший уровень владения изученным материалом по заданной теме, работа выполнена полностью, но допущено в ней: а) не более одной негрубой ошибки и одного недочета; б) или не более двух недочетов);
60-74,99% - удовлетворительно (практическое задание выполнено в установленный срок с частичным использованием рекомендаций преподавателя; продемонстрированы минимальные знания по основным темам изученного материала; выполнено не менее половины работы или допущены в ней а) не более двух грубых ошибок, б) не более одной грубой ошибки и одного недочета, в) не более двух-трех негрубых ошибок, г) одна негрубая ошибка и три недочета, д) при отсутствии ошибок, 4-5 недочетов);
0-59,99% - неудовлетворительно (число ошибок и недочетов превосходит норму, при которой может быть выставлена оценка «удовлетворительно» или если правильно выполнено менее половины задания; если обучающийся не приступал к выполнению задания или правильно выполнил не более 10 процентов всех заданий).

3.4 Собеседование (вопросы к защите практических работ)
3.4.1 Шифр и наименование компетенции

ОПК-11 - Способен разрабатывать компоненты систем защиты информации автоматизированных систем

№ задания	Формулировка задания
87.	Определить уровень базовый уровень защищенности ИС ПДн по следующим исходным данным: - обработка ПДн сотрудников организации; - категории биометрических и иных персональных данных; - объем обработки менее 100000 субъектов персональных данных; - возможны угрозы 2 типа.
88.	Определить состав и содержание организационных и технических мер по защите ИС ПДн в соответствии с уровнем защищенности, руководствуясь последовательностью действий: - определить базовый набор мер для третьего уровня защищенности ПДн; - адаптировать базовый набор мер, с учетом характеристик распределенной информационной системы; - подготовить предложения для уточнения адаптированного базового набора мер для различных вариантов ИС ПДн. Подобрать необходимый для заданного уровня защищенности ПДн состав средств защиты информации.
89.	Разработать структуру технического задания на создание автоматизированной системы в защищенном исполнении. Составить технический паспорт на автоматизированную систему в защищенном исполнении, включающий: - общие сведения об автоматизированной системе; - состав оборудования автоматизированной системы (состав основных и вспомогательных средств и систем); - состав средств защиты информации.
90.	Разработать перечень сведений конфиденциального характера предприятия, с учетом видов информации ограниченного доступа (коммерческая тайна, персональные данные), и требуемых этапов разработки подобного перечня. Для сформированного перечня определить состав объектов защиты

91.	Разработать модель системы (элемента системы) защиты информации, используя один из методов: - специальные методы неформального моделирования. - декомпозицию общей задачи на частные задачи. - прием макромоделирования
92.	Разработать основные положения Методики анализа и оценки рисков информационной безопасности в соответствии с выбранной областью действия системы управления информационной безопасностью и активами. В содержание Методики анализа и оценки рисков информационной безопасности включить: - порядок инвентаризации активов; - порядок оценки ценности активов, шкалы оценки ценности; - порядок определения угроз и уязвимостей активов, определения вероятности их возникновения; - порядок оценки рисков информационной безопасности; - порядок формирования мер по обработке рисков.
93.	Разработать программу проведения аудита первой стороны, включающую: - внутренние требования системы управления информационной безопасностью; - состав проверяемых подразделений; - вид аудиторской проверки; - метрики оценки эффективности аудита
94.	Разработать модель реализации преднамеренного инцидента информационной безопасности, с учетом: - перечня злоумышленников; - целей злоумышленников; - методов и средств реализации информационного воздействия; - действий злоумышленников; - объектов информационного воздействия; - результатов информационного воздействия
95.	Найти ключевые точки сообщения с окружающим программно-аппаратным обеспечением (адреса памяти, файлы на диске, сетевые ресурсы) сервиса, используя средства мониторинга активности приложения. Предложить список мер по программной защите приложения от внешних атак на данные точки сообщения
96.	Используя средства агрессивного сканирования портов, сымитировать атаку на распределенную информационную систему в кабинете. Оценить успешность атаки, построить оценку защищенности сети по полученным данным.
97.	На основе заданной схемы незащищенной корпоративной ЛВС предприятия разработать схему защищенной сети с использованием следующих средств активной защиты: файрволл, интерактивный детектор атак. Привести конфигурацию файрволла для заданного перечня сервисов.

Процентная шкала 0-100 %;
85-100% - отлично (практическое задание выполнено в установленный срок с использованием рекомендаций преподавателя; показан высокий уровень знания изученного материала по заданной теме, проявлен творческий подход, умение глубоко анализировать проблему и делать обобщающие практико-ориентированные выводы; работа выполнена без ошибок и недочетов или допущено не более одного недочета);
75- 84,99% - хорошо (практическое задание выполнено в установленный срок с использованием рекомендаций преподавателя; показан хороший уровень владения изученным материалом по заданной теме, работа выполнена полностью, но допущено в ней: а) не более одной негрубой ошибки и одного недочета; б) или не более двух недочетов);
60-74,99% - удовлетворительно (практическое задание выполнено в установленный срок с частичным использованием рекомендаций преподавателя; продемонстрированы минимальные знания по основным темам изученного материала; выполнено не менее половины работы или допущены в ней а) не более двух грубых ошибок, б) не более одной грубой ошибки и одного недочета, в) не более двух-трех негрубых ошибок, г) одна негрубая

ошибка и три недочета, д) при отсутствии ошибок, 4-5 недочетов);
0-59,99% - неудовлетворительно (число ошибок и недочетов превосходит норму, при которой может быть выставлена оценка «удовлетворительно» или если правильно выполнено менее половины задания; если обучающийся не приступал к выполнению задания или правильно выполнил не более 10 процентов всех заданий).

3.4. Домашнее задание, реферат

ОПК-11 - Способен разрабатывать компоненты систем защиты информации автоматизированных систем,

№ задания	Формулировка задания
98.	ГОСТ Р 50922-2006 — Защита информации. Основные термины и определения.
99.	ГОСТ Р ИСО/МЭК 15408-1-2008 — Информационная технология. Методы и средства обеспечения безопасности. Критерии оценки безопасности информационных технологий. Часть 1. Введение и общая модель
100.	ГОСТ Р ИСО/МЭК 15408-2-2008 — Информационная технология. Методы и средства обеспечения безопасности. Критерии оценки безопасности информационных технологий. Часть 2. Функциональные требования безопасности.
101.	ГОСТ Р ИСО/МЭК 15408-3-2008 — Информационная технология. Методы и средства обеспечения безопасности. Критерии оценки безопасности информационных технологий. Часть 3. Требования доверия к безопасности.
102.	ГОСТ Р ИСО/МЭК 15408 — «Общие критерии оценки безопасности информационных технологий»
103.	ГОСТ Р ИСО/МЭК 17799 — «Информационные технологии. Практические правила управления информационной безопасностью». Прямое применение международного стандарта с дополнением — ISO/IEC 17799:2005
104.	ГОСТ Р ИСО/МЭК 27001 — «Информационные технологии. Методы безопасности. Система управления безопасностью информации. Требования». Прямое применение международного стандарта — ISO/IEC 27001:2005.
105.	ГОСТ Р 51898-2002 — Аспекты безопасности. Правила включения в стандарты
106.	Защищенная автоматизированная система
107.	Модели угроз информационной безопасности
108.	Модель нарушителя информационной безопасности
109.	Персональные данные. Особенности хранения и передачи
110.	Понятие и требования к ИСПДн
111.	Практические подходы к разработке моделей нарушителя
112.	Понятие персональных данных. Понятие ИСПДн.
113.	Федеральное законодательство в области защиты персональных данных и ведомственные нормативные акты (ФСТЭК России, ФСБ России).

Критерии и шкалы оценки:
- оценка «зачтено» выставляется студенту, если домашнее задание является самостоятельным, оригинальным текстом, в котором прослеживается авторская позиция, продуманная система аргументов, а также наличествует обоснованные выводы; используются термины, понятия по дисциплине, в рамках которой выполняется работа; полностью соответствует выбранной теме, цели и задачам; текст домашнего задания логически выстроен, имеет четкую структуру; работа соответствует всем техническим требованиям; домашнее задание выполнено в установленный срок.
- оценка «не зачтено», выставляется студенту, если домашнее задание не является самостоятельным, оригинальным текстом, в котором не прослеживается авторская позиция, не продумана система аргументов, а также отсутствуют обоснованные выводы; не используются термины, понятия по дисциплине, в рамках которой выполняется работа; не соответствует выбранной теме, цели и задачам; текст домашнего задания композиционно не выстроен; работа не соответствует техническим требованиям; домашнее задание не выполнено в установленный срок.

4. Методические материалы, определяющие процедуры оценивания знаний, умений, навыков и (или) опыта деятельности, характеризующих этапы формирования компетенций

Процедуры оценивания в ходе изучения дисциплины знаний, умений и навыков, характеризующих этапы формирования компетенций, регламентируются положениями:
- П ВГУИТ 2.4.03 Положение о курсовых экзаменах и зачетах;
- П ВГУИТ 4.1.02 Положение о рейтинговой оценке текущей успеваемости.

Для оценки знаний, умений, навыков обучающихся по дисциплине применяется рейтинговая система. Итоговая оценка по дисциплине определяется на основании определения среднеарифметического значения баллов по каждому заданию.

Зачет по дисциплине выставляется в зачетную ведомость по результатам работы в семестре после выполнения всех видов учебной работы, предусмотренных рабочей программой дисциплины (с отметкой «зачтено») и получении по результатам тестирования по всем разделам дисциплины не менее 60 %.

5. Описание показателей и критериев оценивания компетенций на различных этапах их формирования, описание шкал оценивания для каждого результата обучения по дисциплине/практике

Результаты обучения по этапам формирования компетенций	Предмет оценки (продукт или процесс)	Показатель оценивания	Критерии оценивания сформированности компетенций	Шкала оценивания	
				Академическая оценка или баллы	Уровень освоения компетенции
ОПК-11– Способен разрабатывать компоненты систем защиты информации автоматизированных систем.					
ЗНАЕТ	Знает методы проведения анализ защищённости автоматизированных систем	Изложение основных методик анализа защищённости автоматизированных систем	Изложены основные методики анализа защищённости авто аматизированных систем	Зачтено/ 60-100; Удовлетворительно /60-74,9	Освоена (базовый)
				Хорошо/75-84,9; Отлично/85-100.	Освоена (повышенный)
			Не изложены основные методики анализа защищённости авто аматизированных систем	Не зачтено / 0-59,99	Не освоена (недостаточный)
УМЕТЬ	Защита практических работ (собеседование), решение тестовых заданий	Применять методики анализ защищённости автоматизированных систем	Самостоятельно разрабатывать основные методики анализа защищённости авто аматизированных систем	Зачтено/ 60-100; Удовлетворительно /60-74,99;	Освоена (базовый)
				Хорошо/75-84,99; Отлично/85-100.	Освоена (повышенный)
			Не правильно разрабатывать основные методики анализа защищённости авто аматизированных систем	Не зачтено/ 0-59,99	Не освоена (недостаточный)
ВЛАДЕТЬ	Домашнее задание	Демонстрировать навыки проведения анализ защищённости автоматизированных систем	Приведена демонстрация навыков разработки основных методик анализа защищённости автоаматизированных систем	Зачтено/ 60-100	Освоена (повышенный)
			Не приведена демонстрация навыков анализа защищённости авто аматизированных систем	Не зачтено/ 0-59,99	Не освоена (недостаточный)