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

Основы информационной безопасности

(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 «Основы информационной безопасности» 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 научно-исследовательского, проектного, контрольно-аналитического, эксплуатационного типов.

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

№ п/п	Код компетенции	Формулировка компетенции	Код и наименование индикатора достижения компетенции
1	ОПК-1	Способен оценивать роль информации, информационных технологий и информационной безопасности в современном обществе, их значение для обеспечения объективных потребностей личности, общества и государства;	$ИД2_{ОПК-1}$ – обладает способностью применять достижения современных информационных технологий и информационной безопасности для обеспечения объективных потребностей личности, общества и государства

Код и наименование индикатора достижения компетенции	Результаты обучения (показатели оценивания)
$ИД2_{ОПК-1}$ – обладает способностью применять достижения современных информационных технологий и информационной безопасности для обеспечения объективных потребностей личности, общества и государства	Знает: цели, задачи, принципы и основные направления обеспечения информационной безопасности государства; основные термины по проблематике информационной безопасности; методологию создания систем защиты информации
	Умеет: выбирать и анализировать показатели качества и критерии оценки систем и отдельных методов и средств защиты информации; пользоваться современной научно-технической информацией по исследуемым проблемам и задачам личности, общества и государства
	Владеет: навыками разработки политики информационной безопасности автоматизированных систем; навыками формальной постановки и решения задачи обеспечения информационной безопасности компьютерных систем

3. Место дисциплины в структуре ООП ВО

Дисциплина «Основы информационной безопасности» относится к обязательной части Блока 1 ООП. Дисциплина является обязательной к изучению.

Изучение дисциплины основано на знаниях, умениях и навыках, полученных при изучении обучающимися дисциплины «Информатика» и прохождении практики «Учебная практика, ознакомительная»

Дисциплина является предшествующей для следующих дисциплин:

«Организационное и правовое обеспечение информационной безопасности»,

«Теория информации», прохождения практики «Производственная практика, преддипломная практика», подготовки к процедуре защиты и защиты выпускной квалификационной работы.

4. Объем дисциплины и виды учебной работы

Общая трудоемкость дисциплины составляет 4 зачетные единицы.

Виды учебной работы	Всего ак. ч	Распределение трудоемкости по семестрам, ак. ч
		3 семестр
Общая трудоемкость дисциплины	**144**	**144**
Контактная работа в т. ч. аудиторные занятия:	**63,7**	**63,7**
Лекции	30	30
в том числе в форме практической подготовки	–	–
Практические занятия	30	30
в том числе в форме практической подготовки	-	-
Консультации текущие	1,5	1,5
Консультации перед экзаменом	2	2
Вид аттестации – экзамен	0,2	0,2
Самостоятельная работа:	**46,5**	**46,5**
Проработка материалов по лекциям, учебникам, учебным пособиям	16,5	16,5
Подготовка к практическим занятиям	10	10
Подготовка доклада с презентацией	10	10
Расчетно-практическая работа	10	10
Контроль (подготовка к экзамену)	**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 раздела дисциплины	Содержание раздела *(указываются темы и дидактические единицы)*	Трудоемкость раздела, акад. ч
1	Введение в проблему информационной безопасности. Основные понятия защиты информации.	Понятие информационной безопасности. Основные составляющие. Терминология информационной безопасности. Распространение объектно-ориентированного подхода на информационную безопасность.	36
2	Законодательные основы информационной безопасности. Стандарты и спецификации в области информационной безопасности.	Законодательное регулирование информационной безопасности. Рассмотрение международных и национальных стандартов и спецификаций в области информационной безопасности. «Оранжевая книга» как оценочный стандарт. Механизмы безопасности. Классы безопасности. Рассмотрение руководящих документов ФСТЭК России.	36
3	Угрозы информационной безопасности. Подходы к построению систем защиты информации.	Угрозы информационной безопасности. Административный, процедурный, программно-технический уровни обеспечения информационной безопасности. Идентификация, аутентификация и управление доступом. Криптографические методы защиты информации.	34,5
	Консультации текущие		1,5
	Консультации перед экзаменом		2
	Экзамен		0,2

5.2 Разделы дисциплины и виды занятий

№ п/п	Наименование раздела дисциплины	Лекции, ак. ч	Практические занятия, ак. ч	СРО, ак. ч
1	Введение в проблему информационной безопасности. Основные понятия защиты информации.	10	10	16
2	Законодательные основы информационной безопасности. Стандарты и спецификации в области информационной безопасности.	10	10	16
3	Угрозы информационной безопасности. Подходы к построению систем защиты информации.	10	10	14,5
	Консультации текущие	1,5		
	Консультации перед экзаменом	2		
	Экзамен	0,2		

5.2.1 Лекции

№ п/п	Наименование раздела дисциплины	Тематика лекционных занятий	Трудоемкость, ак. ч
1	Введение в проблему информационной безопасности. Основные понятия защиты информации.	Понятие информационной безопасности. Основные составляющие. Важность проблемы. Терминология и основные понятия защиты информации. Распространение объектно-ориентированного подхода на информационную безопасность.	10
2	Законодательные основы информационной безопасности. Стандарты и спецификации в области информационной безопасности.	Законодательный уровень информационной безопасности. Мировые стандарты в области информационной безопасности. Российские стандарты в области информационной безопасности. Спецификации в области информационной безопасности. Особенности нормотворческой деятельности в области информационной безопасности.	10
3	Угрозы информационной безопасности. Подходы к построению систем защиты информации.	Угрозы информационной безопасности. Административный уровень информационной безопасности. Управление рисками. Процедурный уровень информационной безопасности. Основные программно-технические меры обеспечения информационной безопасности. Идентификация, аутентификация и управление доступом. Криптографические методы защиты информации.	10

5.2.2 Практические занятия

№ п/п	Наименование раздела дисциплины	Тематика практических занятий	Трудоемкость, ак. ч.
1	Введение в проблему информационной безопасности. Основные понятия защиты информации	Метод анализа конкретных ситуаций Администрирование, политика и компоненты системы безопасности	10
2	Законодательные основы информационной безопасности. Стандарты и спецификации в области информационной безопасности	Разработка приказов (инструкций) регламентирующих сферу информационной безопасности на предприятии.	10
3	Угрозы информационной безопасности. Подходы к построению систем защиты информации	Изучение и отработка программно-технических мер обеспечения информационной безопасности.	10

5.2.3 Лабораторный практикум Не предусмотрен

5.2.4 Самостоятельная работа обучающихся (СРО)

№ п/п	Наименование раздела дисциплины	Вид СРО	Трудоемкость, ак. ч.
1	Введение в проблему информационной безопасности. Основные понятия защиты информации. Законодательные основы информационной безопасности. Стандарты и спецификации в области информационной безопасности	Проработка материалов по лекциям, учебникам, учебным пособиям	3
		Подготовка к практическим занятиям	3
		Подготовка доклада с визуальным представлением средствами Power Point	10
2	Угрозы информационной безопасности. Подходы к построению систем защиты информации. Введение в проблему информационной безопасности. Основные понятия защиты информации	Проработка материалов по лекциям, учебникам, учебным пособиям	3
		Подготовка к практическим занятиям	3
		Расчетно-практическая работа «Создание алгоритма и программы кодирования и декодирования методом Шеннона-Фэно»	10
3	Законодательные основы информационной безопасности. Стандарты и спецификации в области информационной безопасности	Проработка материалов по лекциям, учебникам, учебным пособиям	3
		Подготовка к практическим занятиям	3
		Тестирование	8,5

6. Учебно-методическое и информационное обеспечение дисциплины

Для освоения дисциплины обучающийся может использовать:

6.1 Основная литература

1. Паршин, К. А. Методы и средства проектирования информационных систем и технологий : учебно-методическое пособие / К. А. Паршин. – Екатеринбург : , 2018. –
129 с. – Текст : электронный // Лань : электронно-библиотечная система. – URL: https://e.lanbook.com/book/121337

2. Нестеров, С. А. Основы информационной безопасности : учебник для вузов / С. А. Нестеров. – Санкт-Петербург : Лань, 2021. – 324 с. – ISBN 978-5-8114-6738-9. – Текст : электронный // Лань : электронно-библиотечная система. – URL: https://e.lanbook.com/book/165837

3. Информационная безопасность : учебное пособие. – Пермь : ПГГПУ, 2018. –
87 с. – ISBN 978-5-85219-007-9. – Текст : электронный // Лань : электронно-библиотечная система. – URL: https://e.lanbook.com/book/129509

6.2 Дополнительная литература

1. Моргунов, А. В. Информационная безопасность : учебно-методическое пособие / А. В. Моргунов. – Новосибирск : НГТУ, 2019. – 83 с. – ISBN 978-5-7782-3918-0. – Текст : электронный // Лань : электронно-библиотечная система. – URL: https://e.lanbook.com/book/152227

2. Прохорова, О. В. Информационная безопасность и защита информации : учебник для спо / О. В. Прохорова. – 2-е изд., стер. – Санкт-Петербург : Лань, 2021. –
124 с. – ISBN 978-5-8114-7338-0. – Текст : электронный // Лань : электронно-библиотечная система. – URL: https://e.lanbook.com/book/158939

3. Гультяева, Т. А. Основы информационной безопасности : учебное

пособие / Т. А. Гультяева. – Новосибирск : НГТУ, 2018. – 79 с. – ISBN 978-5-7782-3640-0. – Текст : электронный // Лань : электронно-библиотечная система. – URL: https://e.lanbook.com/book/118233

6.3 Перечень учебно-методического обеспечения для самостоятельной работы обучающихся

Основы информационной безопасности [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, 2021. – 20 с.

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 «ВГУИТ»	*https://education.vsuet.ru/*

6.5 Перечень информационных технологий, используемых при осуществлении образовательного процесса по дисциплине, включая перечень программного обеспечения, современных профессиональных баз данных 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 программное обеспечение – ОС Microsoft Windows, ОС ALT Linux, Microsoft Office Professional Plus; VMWare Player, Oracle VM VirtualBox.

7 Материально-техническое обеспечение дисциплины

Учебная лаборатория для проведения практических занятий	**Ауд. 420**: Компьютеры Core i5-4460 – 10 шт., Core i5-4570 – 1 шт., проектор Acer projector X1383WH, экран, стенды – 5 шт., 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, системный блок Supermicro Amibios 786 Q 2000, коммутатор TP-Link SG1024DE, маршрутизатор MikroTik RB2011iLS-IN,	Microsoft Windows 7 [Microsoft Open License Microsoft Windows Professional 7 Russian Upgrade Academic OPEN 1 License No Level#47881748 от 24.12.2010г. http://eopen.microsoft.com] бессрочно, Microsoft Office 2007 Standart [Microsoft Open License Microsoft Office 2007 Russian Academic OPEN No Level #44822753 от 17.11.2008 http://eopen.microsoft.com] бессрочно, Adobe Reader XI [(бесплатное ПО) https://acrobat.adobe.com/ru/ru/acrobat/pdf-reader/volume-distribution.html] бессрочно, Microsoft Visual Studio 2010 [Сублицензионный договор № 17623/VRN3От 07 июля 2010 г. на право использование программы для ЭВМ MSDN AA Developer Electronic Fulfillment, FreePascal[(бесплатноеПО) https://ru.wikipedia.org/wiki/Free_Pascal] бессрочно, ФИКС 2.0.2 [Договор № ТРУБ 27/01/17 с ООО «ВСГРУПП» от 15.02.2017 г. Лицензия на право использования + установочный пакет], СТРАЖ NT 3.0 [Договор № ТРУБ 27/01/17 с ООО «ВСГРУПП» от 15.02.2017 г.], Панцирь [Договор № ТРУБ 27/01/17 с ООО «ВСГРУПП» от 15.02.2017 г.], Ревизор 1 XP [Договор № ТРУБ 27/01/17 с ООО «ВСГРУПП» от 15.02.2017 г. Лицензия на право использования + установочный пакет], Ревизор 3.0 [Договор № ТРУБ 27/01/17 с ООО «ВСГРУПП» от 15.02.2017 г. Лицензия на право использования + установочный пакет], СТРАЖ NT 4.0 [ДОГОВОР № 200016222100015 с ООО «Паскаль»], Secret Net[ДОГОВОР № 200016222100015 с ООО «Паскаль»], GIMP [(бесплатное ПО) https://ru.wikipedia.org/wiki/GIMP] бессрочно, Avidemux [(бесплатное ПО) https://ru.wikipedia.org/wiki/Avidemux] бессрочно, Virtual Dub [(бесплатное ПО) https://ru.wikipedia.org/wiki/VirtualDub] бессрочно, Oracle VM Virtual Box [(бесплатное ПО) https://ru.wikipedia.org/wiki/VirtualBox] бессрочно, Netbeans [(бесплатное ПО) https://netbeans.org/] бессрочно, СЗИ Dallas Lock 8.0 К Сертификат ФСТЭК No2720 25.09.2015; СЗИ Dallas Lock 8.0 С Сертификат ФСТЭК No2945 16.08.2013
Учебная лаборатория для проведения практических занятий	**Ауд. 424** Компьютер РЕГАРД – 11 шт., стенды – 3 шт.	ОС Astra Linux Альт Образование 8.2 [Лицензия № ААА.0217.00 с 21.12.2017 г. Лицензионный договор № РБТ-14/1623-01-ВУЗ от 18.12.2017 г.] бессрочно, Libre Office 6.1 [Лицензия № ААА.0217.00 с 21.12.2017 г. Включен в установочный пакет операционной системы Альт Образование 8.2] бессрочно, wxMaxima [Лицензия № ААА.0217.00 с 21.12.2017 г.] бессрочно, Lazarus [(бесплатное ПО) https://ru.wikipedia.org/wiki/Lazarus] бессрочно, Oracle VM Virtual Box [(бесплатное ПО) https://ru.wikipedia.org/wiki/VirtualBox] бессрочно, FreePascal [(бесплатное ПО)https://ru.wikipedia.org/wiki/Free_Pascal] бессрочно.
Учебная лаборатория для проведения практических занятий	**Ауд. 332а** Компьютеры - 12 шт., стенды – 5 шт.	ОС Astra Linux Альт Образование 8.2 [Лицензия № ААА.0217.00 с 21.12.2017 г. Лицензионный договор № РБТ-14/1623-01-ВУЗ от 18.12.2017 г.] бессрочно, Libre Office 6.1 [Лицензия № ААА.0217.00 с 21.12.2017 г. Включен в установочный пакет операционной системы Альт Образования 8.2] бессрочно , wxMaxima [Лицензия № ААА.0217.00 с 21.12.2017 г. Включен в установочный пакет операционной системы Альт Образование 8.2] бессрочно, Lazarus [(бесплатное ПО) https://ru.wikipedia.org/wiki/Lazarus] бессрочно, SMathStudio [(бесплатное ПО) https://ru.wikipedia.org/wiki/SMath_Studio] бессрочно, Avidemux [(бесплатное ПО) https://ru.wikipedia.org/wiki/Avidemux] бессрочно, Oracle VM Virtual Box [https://ru.wikipedia.org/wiki/VirtualBox] бессрочно, AnyLogic 8.3 [(бесплатное ПО) https://www.anylogic.ru/downloads/personal-learning-edition-download/] бессрочно.

Аудитории для проведения занятий лекционного типа,	**Ауд. 401** Аудио-визуальная система лекционных аудитория (мультимедийный проектор Epson EB-X18, настенный экран Screen Media)	
Аудитории для самостоятельной работы, курсового и дипломного проектирования	**Читальные залы** библиотеки: Компьютеры со свободным доступом в сеть Интернет и Электронными библиотечными и информационно справочными системами, Компьютеры Regard - 12 шт. **Ауд. 424** Компьютер РЕГАРД – 11 шт., стенды – 3 шт	АЛЬт 8.1

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».

ОЦЕНОЧНЫЕ МАТЕРИАЛЫ
ДЛЯ ПРОМЕЖУТОЧНОЙ АТТЕСТАЦИИ

по дисциплине

ОСНОВЫ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

1 Перечень компетенций с указанием этапов их формирования

№ п/п	Код компетенции	Формулировка компетенции	Код и наименование индикатора достижения компетенции
1	ОПК-1	Способен оценивать роль информации, информационных технологий и информационной безопасности в современном обществе, их значение для обеспечения объективных потребностей личности, общества и государства;	ИД2опк-1 - обладает способностью применять достижения современных информационных технологий и информационной безопасности для обеспечения объективных потребностей личности, общества и государства

Код и наименование индикатора достижения компетенции	Результаты обучения (показатели оценивания)
ИД2опк-1 - обладает способностью применять достижения современных информационных технологий и информационной безопасности для обеспечения объективных потребностей личности, общества и государства	Знает: цели, задачи, принципы и основные направления обеспечения информационной безопасности государства; основные термины по проблематике информационной безопасности; методологию создания систем защиты информации
	Умеет: выбирать и анализировать показатели качества и критерии оценки систем и отдельных методов и средств защиты информации; пользоваться современной научно-технической информацией по исследуемым проблемам и задачам личности, общества и государства
	Владеет: навыками разработки политики информационной безопасности автоматизированных систем; навыками формальной постановки и решения задачи обеспечения информационной безопасности компьютерных систем

2 Паспорт оценочных материалов по дисциплине

№ п/п	Разделы дисциплины	Индекс контролируемой компетенции	Оценочные средства		Технология/процедура оценивания (способ контроля)
			наименование	№№ заданий	
1.	Введение в проблему информационной безопасности. Основные понятия защиты информации.	ОПК-1	Банк тестовых заданий	1-5	Бланочное тестирование (процентная шкала)
			Реферат	26-30	Проверка преподавателем (уровневая шкала)
			Собеседование	78-83	Проверка преподавателем (уровневая шкала)
2.	Законодательные основы информационной	ОПК-1	Банк тестовых заданий	6-11	Бланочное тестирование (процентная шкала)
			Реферат	31-40	Проверка преподавателем

	безопасности. Стандарты информационной безопасности (ИБ). Сведения, составляющие государственную тайну и понятие конфиденциальной информации				(уровневая шкала)
			Собеседование	83-88	
3.	Угрозы информационной безопасности. Подходы к построению систем защиты информации.	ОПК-1	Банк тестовых заданий	9-18	Бланочное тестирование (процентная шкала)
			Реферат	41-50	Проверка преподавателем (уровневая шкала)
			Собеседование	89-101	Проверка преподавателем (уровневая шкала)
			Кейс-задачи	62-72	
4.	Меры по обеспечению безопасности компьютерных систем	ОПК-1	Банк тестовых заданий	51-61	Бланочное тестирование (процентная шкала)
			Собеседование	102-117	Проверка преподавателем (уровневая шкала)
			Кейс- задачи	73-76	Проверка преподавателем (уровневая шкала)
			Расчетно-графическое работа	77	

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

Аттестация обучающегося по дисциплине проводится в форме промежуточного тестирования, защиты реферата, выполнения расчетно-практического задания и экзамена

Каждый вариант теста включает 10 контрольных заданий.

Каждый билет включает 2 контрольных вопроса, из них:

- 1 контрольный вопрос на проверку знаний;
- 1 контрольный вопрос на проверку умений и навыков.

3.1 Тесты (тестовые задания)

3.1.1 Шифр и наименование компетенции **ОПК-1** Способен оценивать роль информации, информационных технологий и информационной безопасности в современном обществе, их значение для обеспечения объективных потребностей личности, общества и государства;

№ задания	Тестовое задание с вариантами ответов и правильными ответами
1	Обладатель информации при осуществлении своих прав обязан: – соблюдать права и законные интересы иных лиц; – принимать меры по защите информации; – ограничивать доступ к информации, если такая обязанность установлена федеральными законами. – **соблюдение всех перечисленных пунктов**.
2	В соответствии с Федеральным законом от 27 июля 2006 г. N 149-ФЗ» Об информации, информационных технологиях и о защите информации» информация – это: **– сведения (сообщения, данные) независимо от формы их представления;** – зафиксированная на материальном носителе информация с реквизитами, позволяющими ее идентифицировать; – сведения о фактах, событиях и обстоятельствах жизни гражданина, позволяющие идентифицировать его личность.
3	Каковы задачи государственной системы обеспечения информационной безопасности? – выявление и прогнозирование дестабилизирующих факторов и информационных угроз жизненно важным интересам личности, общества и государства; – осуществление комплекса оперативных и долговременных мер по предупреждению и устранению дестабилизирующих факторов и информационных угроз; – создание и поддержание в готовности сил и средств обеспечения информационной безопасности и другие задачи; – **все перечисленные**
4	Дайте определение государственной системы защиты информации. – государственная система защиты информации – совокупность федеральных и иных органов управления и взаимоувязанных правовых, организационных и технических мер, осуществляемых на различных уровнях управления и реализации информационных отношений и направленных на обеспечение безопасности информационных ресурсов; – государственная система защиты информации – совокупность федеральных и иных органов управления, выполняющие функции по защите информации; – **государственная система защиты информации – совокупность правовых, организационных и технических мер по реализации функций обеспечения информационной безопасности**.

5	Перечислите основные группы информационных ресурсов государства. (3 правильных ответа) – **федеральные ресурсы;** – **информационные ресурсы, находящиеся в совместном ведении Российской Федерации и субъектов РФ;** – **информационные ресурсы субъектов РФ.** – защищаемая информация и информация свободного доступа.
6	Какая из перечисленных видов тайн относится к категории конфиденциальной информации? – **государственная тайна, персональные данные, коммерческая тайна, служебная тайна, банковская тайна.** – персональная данные, коммерческая тайна, служебная тайна. – государственная тайна, коммерческая тайна, служебная тайна
7	Каким нормативно-правовым документом регулируются отношения, связанные со сведениями, содержащими государственную тайну? – Федеральный закон от 27 июля 2006 г. N 149-ФЗ»Об информации, информационных технологиях и о защите информации» – **закон РФ «О государственной тайне» от 21 июля 1993 г;** – закон РФ «О безопасности» от 5 марта 1992 г. № 2446-I
8	Что такое гриф секретности? – **реквизиты, свидетельствующие о степени секретности сведений, содержащихся в их носителе, проставляемые на самом носителе и (или) в сопроводительной документации на него;** – процедура оформления права граждан на доступ к сведениям, составляющим государственную тайну, а предприятий, учреждений и организаций – на проведение работ с использованием таких сведений; – совокупность категорий сведений, в соответствии с которыми сведения относятся к государственной тайне и засекречиваются на основаниях и в порядке, установленных федеральным законодательством
9	Какие виды деятельности по технической защите конфиденциальной информации подлежат лицензированию? – услуги по контролю защищенности конфиденциальной информации от утечки по техническим каналам; – услуги по контролю и мониторингу защищенности конфиденциальной информации от НСД – работы и услуги по аттестационным испытаниям и аттестации средств ЗИ – работы и услуги по проектированию в защищенном исполнении средств и систем информатизации – **все причисленные**
10	Какой правовой документ представляет собой совокупность официальных взглядов на цели, задачи, принципы и основные направления обеспечения информационной безопасности Российской Федерации? – **Доктрина информационной безопасности Российской Федерации 09.09.2000 г**.; – Концепция национальной безопасности Российской Федерации от 17.09.2000 г.; – Закон РФ «О безопасности» от 5 марта 1992 г. № 2446-I
11	Что такое информационная безопасность? – **состояние защищенности ее национальных интересов в информационной сфере, определяющихся совокупностью сбалансированных интересов личности, общества и государства.** – реализация конституционных прав человека и гражданина на доступ к информации, на использование информации в интересах осуществления не запрещенной законом деятельности, физического, духовного и интеллектуального развития, а также защита информации, обеспечивающая личную безопасность. – создание условий для гармоничного развития Российской информационной инфраструктуры. – создание условий для безопасного распространения информации
12	Что является объектом преступлений, предусмотренных главой 28 УК РФ. – **общественные отношения в сфере обеспечения информационной безопасности;** – общественные отношения собственности; – в сфере поддержания основ государственного строя и безопасности государства.
13	Что является общественно опасными последствиями при совершении деяния, предусмотренного ст. 272 УК РФ «Неправомерный доступ к компьютерной информации»? – неправомерный доступ к охраняемой законом информации; – **уничтожение, блокирование, модификация, копирование информации, нарушение работы ЭВМ, системы ЭВМ или их сети;**

	– создание программ для ЭВМ или внесение изменений в существующие программы.
14	Что является общественно опасными деяниями при совершении преступления, предусмотренного ст. 273 УК РФ «Создание, использование и распространение вредоносных программ для ЭВМ»? – создание программ для ЭВМ, заведомо приводящих к несанкционированному уничтожению, блокированию, модификации, копированию информации, нарушению работы ЭВМ, системы ЭВМ или их сети; – внесение изменений в существующие программы, заведомо приводящих к несанкционированному уничтожению, блокированию, модификации, копированию информации, нарушению работы ЭВМ, системы ЭВМ или их сети; – использование либо распространение программ для ЭВМ, заведомо приводящих к несанкционированному уничтожению, блокированию, модификации, копированию информации, нарушению работы ЭВМ, системы ЭВМ или их сети; – **все перечисленные действия.**
15	Перечислите основные уголовно-правовые меры, предусматривающие уголовную ответственность за разглашение государственной тайны? – Ст. 272 «Неправомерный доступ к компьютерной информации», ст. 273 «Создание, использование и распространение вредоносных программ для ЭВМ», ст.274 «Нарушение правил эксплуатации ЭВМ, системы ЭВМ или их сети»; – **Ст. 275 «Государственная измена», ст. 276. «Шпионаж», ст. 283. «Разглашение государственной тайны»;** – Ст. 158 «Кража»; ст.159 «Мошенничество»; ст. 160 «Присвоение или растрата».
16	Какая информация в соответствии с Федеральным законом от 29 июля 2004 г. N 98-ФЗ "О коммерческой тайне" отнесена к сведениям, составляющим коммерческую тайну? (несколько вариантов ответов) – сведения, содержащиеся в учредительных документах юридического лица, документах, подтверждающих факт внесения записей о юридических лицах и об индивидуальных предпринимателях в соответствующие государственные реестры; – **информация об условиях сотрудничества (порядок, форма оплаты, предоставляемые скидки, условия доставки и т. д.) с действительными и потенциальными контрагентами;** – **информация о сделках (текущих и планируемых), включая сведения о предварительных переговорах, условиях договоров и любых дополнениях к ним, порядке заключения и исполнения договоров, а также о достигнутых результатах по сделкам.**
17	В соответствии с Федеральным законом от 27 июля 2006 г. № 152-ФЗ «О персональных данных» под персональными данными понимается: **– любая информация, относящаяся к прямо или косвенно определенному или определяемому физическому лицу (субъекту персональных данных)** – зафиксированная на материальном носителе информация о личности с реквизитами, позволяющими ее идентифицировать; – сведения, касающиеся личности, собранные органом власти в процессе реализации установленных для него полномочий, в отношении которых действует требование конфиденциальности.
18	На какой орган исполнительной власти РФ возлагается функция по обеспечению контроля и надзора за соответствием обработки персональных данных требованиям Федерального закона от 27 июля 2006 г. № 152-ФЗ «О персональных данных»? А. ФСТЭК Б. **РОСКОМНАДЗОР** В.ФСБ Г. ФСО Д. МВД
19	Установите соответствия между двумя множествами вариантов ответов

a. Техническая защита конфиденциальной информации	a. выполнение работ и (или) оказание услуг по ее защите от несанкционированного доступа, от утечки по техническим каналам, а также от специальных воздействий на такую информацию в целях ее уничтожения, искажения или блокирования доступа к ней.
b. Сертификация средств защиты информации	b. осуществляется на соответствие требованиям по безопасности информации, установленным нормативными правовыми актами ФСТЭК России
c. Информационная безопасность	c. состояние защищенности общества и государства, отдельного гражданина от информационно-технического воздействия на информационную инфраструктуру

20	Что является объектом системы сертификации:

	– вид деятельности; – помещения; – **средства защиты информации.**
21	К правовым методам обеспечения информационной безопасности Российской Федерации относится: – **законодательное разграничение полномочий в области обеспечения информационной безопасности Российской Федерации между Федеральными органами государственной власти и органами государственной власти субъектов Российской Федерации, определение целей, задач и механизмов участия в этой деятельности общественных объединений, организаций и граждан;** – разработка, использование и совершенствование средств защиты информации и методов контроля эффективности этих средств, развитие защищенных телекоммуникационных систем, повышение надежности специального программного обеспечения; – совершенствование системы финансирования работ, связанных с реализацией правовых и организационно-технических методов защиты информации, создание системы страхования информационных рисков физических и юридических лиц.
22	К организационно-техническим методам обеспечения информационной безопасности Российской Федерации относится: – разработка программ обеспечения информационной безопасности Российской Федерации и определение порядка их финансирования; – **создание систем и средств предотвращения несанкционированного доступа к обрабатываемой информации и специальных воздействий, вызывающих разрушение, уничтожение, искажение информации, а также изменение штатных режимов функционирования систем и средств информатизации и связи;** – создание правовой базы для формирования в Российской Федерации региональных структур обеспечения информационной безопасности
23	К экономическим методам обеспечения информационной безопасности Российской Федерации относится: – внесение изменений и дополнений в законодательство Российской Федерации, регулирующее отношения в области обеспечения информационной безопасности; – **совершенствование системы финансирования работ, связанных с реализацией правовых и организационно-технических методов защиты информации, создание системы страхования информационных рисков физических и юридических лиц;** – выявление технических устройств и программ, представляющих опасность для нормального функционирования информационно-телекоммуникационных систем, предотвращение перехвата информации по техническим каналам, применение криптографических средств защиты информации при ее хранении, обработке и передаче по каналам связи, контроль за выполнением специальных требований по защите информации.
24	Определите верную последовательность этапов организации комплексной защиты информации 1) изучение руководящих документов; 2) издание приказов по оборудованию комплексной защиты информации; 3) категорирование объектов информации; 4) проведение защитных мероприятий.
25	Сколько этапов составляют действия по подготовке и проведению комплексных специальных проверок выделенных помещений? – 6 этапов; – 3 этапа; – **4 этапа.**

3.2 Реферат

3.2.1 ***Шифр и наименование компетенции*** **УК-1** Способен осуществлять поиск, критический анализ и синтез информации, применять системный подход для решения поставленных задач.

Примерная тематика рефератов

Номер темы	Тема
26	История и современные направления защиты информации.
27	Правовая основа защиты информации за рубежом.
28	Правовая основа защиты информации в России.
29	Засекречивание информации. Политический и социальныйаспекты засекречивания информации.
30	Принципы засекречивания информации: законность,обоснованность, своевременность.
31	Организационно-правовые формы засекречивания информации:перечневая форма и система первоначального засекречивания.
32	Рассекречивание информации. Виды сведений, подлежащих и неподлежащих рассекречиванию.
33	Классификация защищаемой информации по принадлежности,содержанию и степени секретности.
34	Носители секретной информации: документы, изделия(предметы), электромагнитные излучения.
35	Понятие государственной тайны. Сведения, которые подлежатзасекречиванию и которые не могут быть засекречены.
36	Определение грифа секретности сведений, составляющихгосударственную тайну.
37	Порядок допуска к государственной тайне. Основания для отказав допуске. Прекращение допуска.
38	Понятие коммерческой тайны и ее виды: технологическая, организационная, коммерческая. Методы промышленногошпионажа.
39	Правовые основы защиты коммерческой тайны за рубежом и вРоссии.
40	Ответственность за нарушение законодательства о коммерческойтайне.
41	Цели незаконного получения сведений, составляющихкоммерческую тайну.
42	Утечка, разглашение, раскрытие и распространение защищаемойинформации. Объективные и субъективные условия утечки информации
43	Легальные, агентурные и технические каналы утечкиинформации.
44	Субъекты незаконного собирания сведений, составляющихкоммерческую тайну.
45	Источники угроз защищаемой информации.
46	Способы незаконного получения сведений, составляющихкоммерческую тайну.
47	Закрытие свободного доступа к сведениям, составляющимкоммерческую тайну.
48	Политический, экономический и моральный ущерб от утечки сведений, составляющих государственную тайну
49	Выявление, предупреждение и пресечение попыток неправомерного завладения сведениями и документами,составляющими коммерческую тайну.
50	Организация защиты от несанкционированного доступа конфиденциальной информации, обрабатываемой средствамивычислительной техники.
51	Организация защиты конфиденциальной информации от утечкипо техническим каналам.
52	Ограничения в предоставлении государственным органам сведений, составляющих коммерческую тайну. Охранакоммерческой тайны.
53	Защита информации, составляющей профессиональную тайну.
54	Защита информации, составляющей банковскую тайну.
55	Защита сведений, составляющих личную тайну.
56	Понятие защиты информации и режима секретности (конфиденциальности). Меры по обеспечению режимаконфиденциальности.
57	Меры по защите секретных и конфиденциальных сведений: правовые, организационные, инженерно-технические и программно-математические.
58	Система защиты информации, ее структурная и функциональнаячасти.
59	Методы защиты информации: скрытие, ранжирование, дезинформация, дробление, морально-нравственные методы,учет, кодирование, шифрование.
60	Средства защиты информации, требования к ним и решаемые сих помощью задачи.
61	Уголовная ответственность за государственную измену,шпионаж, разглашение государственной тайны и утрату секретных документов, объективная и субъективная сторона этихпреступлений.

3.3 Кейс-задания

3.3.1 Шифр и наименование компетенции **УК-1** Способен осуществлять поиск, критический анализ и синтез информации, применять системный подход для решения поставленных задач.

Номер задания	Текст задания
62	**Администрирование Linux** Перейдите в домашний каталог. Создайте каталог «test». Перейдите в каталог «test». Просмотрите содержимое каталога. Создайте каталог «test2». Создайте файл «text» в каталоге «test2». Переименуйте файл «text» в «textSIT». Скопируйте файл «textSIT» в каталог «test2» под именем «copy.txt». Сделайте скриншоты. Результат покажите преподавателю. Удалите созданные вами файлы.
63	**Администрирование Linux** Перейдите в домашний каталог Создайте каталог «test» Создайте файл «text» в каталоге «test2» Создайте жесткую ссылку «link» на файл «copy.txt. Создайте символическую ссылку «simlink» на файл «copy.txt». Просмотрите результаты в текущем каталоге . Удалите созданные вами файлы и ссылки .
62	**Администрирование Linux** Создать два пользователя “students и prepodavatcli” Задать этим пользователям пароли Создать две группы “SAIT и SAPR” Добавить пользователей в обе группы. Проверить наличие этих пользователей в группах, путем вывода всех пользователей состоящих в каждой группе. Показать результат преподавателю Сделать скриншоты команд и каталога Удалить группы.
63	**Администрирование Linux** Создать два пользователя “students и prepodavatcli” Задать этим пользователям пароли Создать каталог “newfolder” Изменить правообладателя каталога “newfolder” на “students”, и убедится в этом. Сделать скриншоты команд и каталога Удалить пользователей.
64	**Администрирование Linux** Создайте каталог «test», Перейдите в каталог «test». Создайте файл «text» в каталоге «test». Выведете информацию о правах доступа к файлу и каталогу. Поясните назначений всех параметров. Изменяете права доступа: запрет всем пользователям всех действий с файлом. Выведете информацию о правах доступа к файлу. Проверьте изменились ли настройки файла в заданном каталоге. Сделайте скриншоты консоли и каталога с файлом. Результат покажите преподавателю. Удалите созданный файл и каталог.
65	**Администрирование Linux** Создайте каталог «test», Перейдите в каталог «test». Создайте файл «text» в каталоге «test». Выведете информацию о правах доступа к файлу и каталогу. Поясните назначений всех пареметров. Изменяете права доступа: правообладателю **разрешить все**; **запрет остальным пользователям удалять файл.**

	Выведете информацию о правах доступа к файлу. Проверьте изменились ли настройки файла в заданном каталоге. Сделайте скриншоты консоли и каталога с файлом. Результат покажите преподавателю. Удалите созданный файл и каталог.
66	**Администрирование Windows** Создайте группу Students Создайте двух новых пользователей St1, St2 Добавьте созданных пользователей в группу Students Проверьте наличие группы Проверьте наличие пользователей Сделайте скриншоты Покажите результат преподавателю Удалите группу и пользователей.
67	**Администрирование Windows** 1. В оснастке «Локальные пользователи и группы» создайте новую группу пользователей. В качестве имени группы пользователей используйте номер Вашей учебной группы. 2. Создайте учётную запись с именем Вашей учётной записи в кафедральной сети и включите её в созданную группу. 3. Примените к созданной учётной записи настройки: Максимальный срок действия пароля 30 Минимальная длина пароля 6 Требовать неповторяемости паролей 2 Отвечать требованиям сложности + Пороговое значение блокировки 3
68	**Администрирование Windows** Создайте новую консоль. Добавьте в корень консоли оснастки «Редактор объекта групповой политики» и «Результирующая политика». Сохраните консоль в режиме авторский. Запретить редактирование реестра. Ограничить размер профиля пользователя значением 5 МБ
69	**Администрирование Windows** Создайте новую консоль. Добавьте в корень консоли оснастки «Редактор объекта групповой политики» и «Результирующая политика». Сохраните консоль в режиме Пользовательский - полный доступ. Запретить использование командной строки. Запретить изменение рисунка рабочего стола.
70	**Администрирование Windows** Создайте новую консоль. Добавьте в корень консоли оснастки «Редактор объекта групповой политики» и «Результирующая политика». Сохраните консоль в режиме Пользовательский - полный доступ. Установить обязательный запрос пароля при выходе из экранной заставки. Удалить «Завершение сеанса» из меню «Пуск».
71	**Работа с программами AZPR.** 1.Создайте каталог Test, в нем создайте 2 текстовых файла t1.txt, t2.txt. Введите в фалы информацию. Заархивируйте каталог Test, при архивировании используйте пароль 6D1A 2. Проведите атаку методом перебора. 3. Область перебора – все печатаемые символы, длина пароля от 1 до 4 символов. Проверить правильность определенного пароля, распаковав каталог и ознакомившись с его содержимым. 4. Повторить эксперимент. Сократить область перебора до фактически используемого Провести повторное вскрытие. Сравнить затраченное время. 5. Сделайте необходимые скриншоты. 6. Результат покажите преподавателю. 7. Удалите созданный каталог.
72	**Работа с программами AZPR.** Создайте каталог Test, в нем создайте 2 текстовых файла t1.txt, t2.txt. Введите в фалы информацию. Заархивируйте каталог Test, выбрав в качестве пароля английское слово длиной до 5 символов (например love, god, table, admin и т.д.). Провести атаку по словарю. Для этого выбрать вид атаки и в закладке Словарь выбрать файл English.dic. Он содержит набор английских слов и наборы символов, наиболее часто использующиеся в качестве паролей. 2. Попытаться определить пароль методом прямого перебора. Сравнить затраченное время.
73	К защищаемым ресурсам типовой информационной системы относятся: – Обрабатываемая в ИС информация, в совокупности представляющая собой ПДн; – Средства вычислительной техники или их компоненты; – Средства защиты информации и система защиты информации ИС в целом;

– Ключевая информация пользователей и администраторов ИС;
– Аутентификационная информация пользователей и администраторов ИС;
– Активное сетевое оборудование ИС;
– Специальное программное обеспечение ИС;
– Общесистемное программное обеспечение ИС;
– Логические схемы функционирования средств и систем защиты информации, в том числе используемые в криптографических средствах криптографические алгоритмы и протоколы;

Топология и сетевая архитектура ИС.

Таблица Перечень защищаемых ресурсов объекта информатизации

Защищаемые ресурсы	Характеристики безопасности
1	2

Вариант 1
Определение объектов защиты бухгалтерии предприятия.
Вариант 2
Определение объектов защиты медицинского учреждения.
Вариант 3
Определение объектов защиты отдела кадров предприятия.

74

Классификация информации по конфиденциальности
– Классифицировать защищаемую информацию по конфиденциальности;
– Определить категории лиц, имеющих доступ к защищаемой информации и ресурсам.
Таблица 1 – Классификация информации по конфиденциальности

Вариант	Должность	Документ	Конфиденциальная информация. Вид тайны.
1.	Бухгалтер		
2.	Начальника отдела кадров		
3.	Проектировщик		
4.	Сметчик		
5.	Системный администратор		

Составить CRUD таблицу для указанной в Вашем варианте должности.

75

Разработка модели угроз.
На основе таблицы – Угрозы безопасности информации и последствия от их реализации
Составить таблицу Возможные угрозы

Вариант	Компоненты системы	Нарушение конфиденциальности информации	Нарушение целостности информации	Нарушение работоспособности системы
1	Персонал			
2	Аппаратные средства			
3	Программные средства			
4	Данные			

76

Построение модели нарушителя
На основе должностных инструкций сотрудников.
Заполните таблицу 1 «Модель нарушителя» Поясните какими возможностями обладает каждый из уровней нарушителей. Сделайте вывод, какой сотрудник может являться самым опасным нарушителем.

¶ ¶ Должность	Квалификация нарушителя			
	Начальные навыки использования ПК. 1 уровень	Может запускать программы. 2 уровень	Создаёт программы. 3 уровень	Знает, как устроена система защиты. Может управлять. 4 уровень
Бухгалтер				
Начальник отдела кадров				
Инженер-проектировщик				
Системный администратор				
Сметчик				

3.3 Расчетно-практическая работа

Шифр и наименование компетенции **УК-1** Способен осуществлять поиск, критический анализ и синтез информации, применять системный подход для решения поставленных задач.

Целю работы является самостоятельное изучение и выполнения задания по теме «Криптографические методы защиты информации» (Раздел 4) в результате выполнения данного самостоятельного задания у обучающего формируются развитие знаний о необходимости внедрения криптографии в производственный процесс.

77. Задание РПР:

Задание включает в себя написание программы асимметричного шифрования – дешифрования методом RSA. Алгоритм для всех вариантов схожий, индивидуальным является шифруемое сообщение и параметры RSA алгоритма шифрования, например, шифруемое слово: **заказ.** Параметры шифрования p, q: 7, 13. Варианты задания приведены в МУ самостоятельной работы обучающихся.

3.3 Экзамен

Вопросы для экзамена

3.3.1 Шифр и наименование компетенции **УК-1** Способен осуществлять поиск, критический анализ и синтез информации, применять системный подход для решения поставленных задач.

Номер вопроса (задачи, задания)	Текст вопроса (задачи, задания)
78	Понятие информационной безопасности.
79	Актуальность проблемы ИБ.
80	Обеспечение информационной безопасности
81	Понятие безопасности компьютерной информации. Объекты и элементы защиты данных в компьютерных системах
82	Основные направления Доктрины информационной безопасности Российской Федерации
83	Перечень сведений, составляющих государственную тайну .
84	Сведения, не подлежащие отнесению к государственной тайне и засекречиванию

85	Степени секретности сведений и грифы секретности носителей этих сведений
86	Допуск к государственной тайне. Уголовно-правовая защита информации, составляющей государственную тайну
87	Понятие персональные данные. Права субъекта персональных данных. Хранение персональных данных. Ответственность за нарушение норм, регулирующих обработку и защиту персональных данных работника
88	Сведения, которые не могут составлять коммерческую тайну. Права обладателя информации, составляющей коммерческую тайну. Охрана коммерческой тайны. Ответственность за нарушение требований Федерального закона «О коммерческой тайне»
89	Основных виды угроз безопасности
90	Преднамеренные и непреднамеренные искусственные угрозы
91	Виды нарушителей. Модель нарушителя.
92	Классификация угроз безопасности
93	Каналы и методы несанкционированного доступа к информации
94	Уязвимости. Методы оценки уязвимости информации
95	Построение систем защиты от угрозы нарушения целостности информации и отказа доступа
96	Назначение, функции и классификация операционных систем.
97	Отличия файловой системы Linux от Windows
98	Основы администрирования Linux
99	Модель Харрисона-Рузо-Ульмана
100	Модель Белла-ЛаПадула
101	Ролевая модель безопасности
102	Субъектно-объектные модели разграничения доступа. Аксиомы политики безопасности
103	Основные понятия объектно-ориентированного подхода. Применение объектно-ориентированного подхода к рассмотрению защищаемых систем.
104	Недостатки традиционного подхода к информационной безопасности с объектной точки зрения.
105	Меры обеспечения информационной безопасности
106	Построение систем защиты от угрозы отказа доступа к информации.
107	Основные направления и цели использования криптографических методов.
108	Основные причины нарушения безопасности информации при ее обработке СКЗИ.
109	Криптосистема шифрования данных RSA.
110	Аутентификация данных и электронная цифровая подпись.
111	Виды ЭЦП.
112	Основные понятия информационной безопасности Интернет сетей
113	Информационная безопасность компьютерных сетей.
114	Сетевые топологии.
115	Адресация узлов сети
116	Использование межсетевых экранов
117	Рекомендации ФСТЭК по установке межсетевых экранов.

[3] *Только для одной компетенции. Форма представления вариантов кейс-заданий выбирается самостоятельно*

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.

Экзамен по дисциплине выставляется в зачетную ведомость по результатам работы в семестре после выполнения всех видов учебной работы, предусмотренных рабочей программой дисциплины и получении по результатам тестирования, практическим работам и РПР по всем разделам дисциплины:

«60-74» -удовлетворительно;

«75-84» -хорошо;

«85-100» -отлично.

Если обучающийся желает повысить оценку по дисциплине, то он вправе сдавать экзамен в сессию.

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

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-1 Способен оценивать роль информации, информационных технологий и информационной безопасности в современном обществе, их значение для обеспечения объективных потребностей личности, общества и государства					
ЗНАТЬ: цели, задачи, принципы и основные направления обеспечения информационной безопасности государства; основные термины по проблематике информационной безопасности; методологию создания систем защиты информации	Тестирование	Правильность ответов при тестировании	Обучающийся ответил на 85-100 % вопросов	85-10 / отлично	освоена/повышенный
			Обучающийся ответил на 70-84 % вопросов	75-84/ хорошо	освоена/повышенный
			Обучающийся ответил на 50-69 % вопросов	60-74/ удовлетворительно	освоена/базовый
			Обучающийся ответил на 0-49 % вопросов	0-59/ неудовлетворительно	не освоена (недостаточный)
	Экзамен ответы на вопросы Собеседование	Правильность логичность ответов собеседования	обучающийся показал глубокие знания программного материала, грамотно и логично его излагает.	отлично	освоена/повышенный
			обучающийся твердо знает программный материал, грамотно его излагает, не допускает существенных неточностей в ответе.	хорошо	освоена/повышенный
			обучающийся имеет знания только основного материала, но не усвоил его деталей, не допускает грубых ошибок в ответе, требует в отдельных случаях наводящих вопросов для принятия правильного решения.	удовлетворительно	освоена/базовый
			обучающийся допускает грубые ошибки в ответе.	неудовлетворительно	не освоена (недостаточный)
УМЕТЬ: выбирать и анализировать показатели качества и критерии оценки систем и отдельных методов и средств защиты информации;	Практическая / Кейс задача	Правильность выполнения практического задания	обучающийся быстро (не более 10 мин) без ошибок и наводящих вопросов выполняет практическое задание не допускает неточностей при выполнении практического задания правильно и уверенно применяет полученные знания, умения	85-10 / отлично	освоена/повышенный

пользоваться современной научно-технической информацией по исследуемым проблемам и задачам личности, общества и государства			и навыки на практике.		
			обучающийся правильно применяет полученные знания при решении практических заданий, владеет приемами работы посредством ИТ. Практическое задание выполняет не более 20 мин, не требуются наводящие вопросы для решения практического задания..	75-84/ хорошо	освоена/повышенный
			обучающийся требует в отдельных случаях наводящих вопросов для принятия правильного решения, допускает отдельные неточности или неуверенно владеет примами работы с ИТ.	60-74/ удовлетворительно/ зачтено)	освоена/базовый
			обучающийся не может применять полученные знания на практике.	0-59/ неудовлетворительно	не освоена (недостаточный)
ВЛАДЕТЬ: навыками разработки политики информационной безопасности автоматизированных систем; навыками формальной постановки и решения задачи обеспечения информационной безопасности компьютерных систем	Тестирование	Правильность ответов при тестировании	Обучающийся ответил на 85-100 % вопросов	85-10 / отлично	освоена/повышенный
			Обучающийся ответил на 70-84 % вопросов	75-84/ хорошо	освоена/повышенный
			Обучающийся ответил на 50-69 % вопросов	60-74/удовлетворительно/	освоена/базовый
			Обучающийся ответил на 0-49 % вопросов	0-59/ неудовлетворительно	не освоена (недостаточный)
	Реферат (Доклад, презентация)	Правильность, лаконичность и полнота выполнения задания. Разработка презентации теме доклада	Реферат основан на источниках (не менее 10), соответствует заявленной теме, оформлен в соответствии со стандартом вуза, количество страниц не менее 25. Презентация из 15-20 слайдов, приведенный материал отвечает современному уровню развития информационных систем и технологий, студент не допускает неточностей в докладе.	85-10 / отлично	освоена/повышенный
			Реферат основан на источниках (от 5-9), соответствует заявленной теме, оформлен в соответствии со стандартом вуза, количество страниц 15-24. Презентация состоит 10- 15 слайдов, приведенный материал отвечает современному уровню развития информационных систем и технологий, студент допускает	75-84/ хорошо	освоена/повышенный

			неточности в докладе, несущественные ошибки в докладе, которые самостоятельно исправляет.		
			Реферат основан на источниках (до 5), соответствует заявленной теме, оформлен в соответствии со стандартом вуза в презентации менее 10 слайдов, приведенный материал не отвечает современного уровню информационных систем и технологий, студент допускает ошибки в докладе, которые исправляет после наводящих вопросов.	60-74/удовлетворительно	освоена/базовый
			Реферат основан на источниках (до 5), не соответствует заявленной теме, не оформлен в соответствии со стандартом вуза, в презентации менее 7 слайдов, приведенный материал не отвечает современного уровню информационных систем и технологий, студент допускает грубые ошибки в докладе или доклад не сформулирован.	0-59/ неудовлетворительно	не освоена (недостаточный)
	Расчетно-практическая работа	Правильность выполнения практического задания	обучающийся выбрал верную методику решения задачи, программный код отвечает требованиям лаконичности, программа имеет графический интерфейс, работа оформлена в соответствии со стандартом вуза, без замечаний, верно ответил на все вопросы.	85-10 / отлично	освоена/повышенный
			обучающийся выбрал верную методику решения задачи, программа имеет графический интерфейс, работа оформлена в соответствии со стандартом вуза, ответил на все вопросы, но имеются незначительные замечания по тексту и оформлению работы, допустил не более 2 незначительных ошибок в ответе, которые самостоятельно исправил.	75-84/ хорошо	освоена/повышенный
			обучающийся выбрал верную методику решения задачи, программа реализована в консольном режиме, имеются замечания по тексту и оформлению работы, допустил не более 3 ошибок в ответе, который исправил с наводящими вопросами, неуверенно владеет примами работы с ИТ.	60-74/ удовлетворительно/ зачтено)	освоена/базовый

			обучающийся не может применять полученные знания на практике.	0-59/ неудовлетворительно	не освоена (недостаточный)