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

Безопасность персональных данных
(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 «Безопасность персональных данных» 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-6;	способен при решении профессиональных задач организовывать защиту информации ограниченного доступа в автоматизированных системах в соответствии с нормативными правовыми актами, нормативными и методическими документами Федеральной службы безопасности Российской Федерации, Федеральной службы по техническому и экспортному контролю;	ИД1опк-6 – обладает навыками разработки автоматизированных систем с учетом политики информационной безопасности с использованием современных программных средств
2	ОПК-5.1	способен разрабатывать и реализовывать политику информационной безопасности открытых информационных систем	ИД1 $_{ОПК-5.1}$. обладает навыками разработки политик информационное безопасности различных открытых информационных систем
3	ОПК-5.3	способен осуществлять контроль обеспечения информационной безопасности и проводить верификацию данных в открытых информационных системах	ИД1$_{ОПК-5.3}$.обладает навыками контроля данных, в том числе персональных и обеспечения их безопасности

Код и наименование индикатора достижения компетенции	Результаты обучения (показатели оценивания)
ИД1$_{опк-6}$– обладает навыками разработки автоматизированных систем с учетом политики информационной безопасности с использованием современных программных средств	Знает: основы теории проектирования информационных систем персональных данных
	Умеет: формировать конструкторскую документацию при проектировании информационных систем персональных данных
	Владеет: навыками разработки технических проектов систем защиты
ИД1 ОПК-5.1. обладает навыками	Знает: требования к содержанию и составу внутренних

разработки политик информационное безопасности различных открытых информационных систем	нормативных документов по защите персональных данных
	Умеет: обосновать контекст безопасности для организации оператора персональных данных
	Владеет: навыками по формированию основных разделов политик информационное безопасности
ИД1ОПК-5.3.обладает навыками контроля данных, в том числе персональных и обеспечения их безопасности	Знает: требования законодательства к планам контролирующих мероприятий информационных систем персональных данных
	Умеет: выполнять периодический контроль требований по защите персональных данных
	Владеет: навыками использования инструментальных средств контроля правил защиты персональных данных в информационных системах

3. Место дисциплины (модуля) в структуре ООП ВО

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

Дисциплина является предшествующей для *следующих видов практик:*

– производственная практика, преддипломная практика;

– производственная практика, эксплуатационная практика.

4. Объем дисциплины (модуля) и виды учебной работы

Общая трудоемкость дисциплины (модуля) составляет _6_ зачетные единицы.

Виды учебной работы	**Всего ак. ч**	**Распределение трудоемкости по семестрам, ак. ч**	
		5 семестр	6 семестр
Общая трудоемкость дисциплины (модуля)	216	72	144
Контактная работа в т. ч. аудиторные занятия:	121	45	72
Лекции	51	15	36
в том числе в форме практической подготовки	–	–	–
Практические/лабораторные занятия	66	30	36
в том числе в форме практической подготовки	–	–	–
Консультации текущие	4.1	0.8	3.4
Вид аттестации – зачет	0,2	0,1	0,1
Самостоятельная работа:	94.6	21.14	68.6
Проработка материалов по лекциям, учебникам, учебным пособиям	40	13.3	26.6
Подготовка к практическим/лабораторным занятиям	20	6.6	13.3
Курсовой проект/работа	27.2	–	27.2
Домашнее задание, реферат	6.4	6.4	–

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

5.1 Содержание разделов дисциплины (модуля)

№ п/п	Наименование раздела дисциплины	Содержание раздела *(указываются темы и дидактические единицы)*	Трудоемкость раздела, ак.ч
1	Правовые и организационные вопросы технической защиты персональных данных	Основные понятия в области технической защиты информации (ТЗИ). Стратегия национальной безопасности Российской Федерации до 2020 года. Доктрина информационной безопасности Российской Федерации. Концептуальные основы ТЗИ. Законодательные и иные правовые акты,	72

		регулирующие вопросы ТЗИ. Система документов по ТЗИ и краткая характеристика ее основных составляющих. Структура и направления деятельности системы ТЗИ в субъектах Российской Федерации. Система органов по ТЗИ в Российской Федерации, их задачи, распределение полномочий по обеспечению ТЗИ. Лицензирование деятельности в области технической защиты информации. Сертификация средств защиты информации, аттестация объектов информатизации по требованиям безопасности информации. Основные документы, определяющие направления и порядок организации деятельности, организационные и технические меры по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных. Права субъектов персональных данных. Способы защиты прав субъектов персональных данных.	
2	Основы организации и ведения работ по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных	Классификация информационных систем персональных данных. Состав мер по обеспечению безопасности персональных данных. Порядок выбора мер по обеспечению безопасности персональных данных, подлежащих реализации в информационной системе. Содержание мер по обеспечению безопасности персональных данных, реализуемых в рамках системы защиты персональных данных. Организация обеспечения безопасности персональных данных в организациях и учреждениях. Перечень основных этапов при организации работ по обеспечению безопасности персональных данных. Содержание, порядок разработки и ввода в действие внутренних нормативных документов и актов ненормативного характера по обработке персональных данных и обеспечению безопасности персональных данных. Обязанности оператора, осуществляющего обработку персональных данных. Комплекс организационных и технических мероприятий (применения технических средств), в рамках подсистемы защиты персональных данных, развертываемой в информационной системе персональных данных в процессе ее создания или модернизации. Основное содержание этапов организации обеспечения безопасности персональных данных. Варианты реализации мероприятий по защите персональных данных и типовые модели защищенных информационных систем персональных данных с использованием существующих сертифицированных средств	144

		защиты информации.	
	Консультации текущие		
	Консультации перед экзаменом		
	Зачет, экзамен		14.6

5.2 Разделы дисциплины и виды занятий

№ п/п	Наименование раздела дисциплины	Лекции, ак. ч	Практические/лабораторные занятия, ак. ч	СРО, ак. ч
1	Правовые и организационные вопросы технической защиты персональных данных	15	30	21.14
2	Основы организации и ведения работ по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных	36	36	68.6
	Консультации текущие			
	Консультации перед экзаменом			
	Зачет, экзамен	14.6		

5.2.1 Лекции

№ п/п	Наименование раздела дисциплины	Тематика лекционных занятий	Трудоемкость, ак. ч
1	Правовые и организационные вопросы технической защиты персональных данных	Основные понятия в области технической защиты информации (ТЗИ). Законодательные и иные правовые акты, регулирующие вопросы ТЗИ. Система документов по ТЗИ и краткая характеристика ее основных составляющих.	6*
2	Правовые и организационные вопросы технической защиты персональных данных	Структура и направления деятельности системы ТЗИ в субъектах Российской Федерации. Система органов по ТЗИ в Российской Федерации. Лицензирование деятельности в области технической защиты информации. Сертификация средств защиты информации, аттестация объектов информатизации по требованиям безопасности информации.	6*
3	Правовые и организационные вопросы технической защиты персональных данных	Основные документы, определяющие направления и порядок организации деятельности, организационные и технические меры по обеспечению безопасности персональных данных.	3*
4	Основы организации и ведения работ по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных	Понятия «безопасности информации», «угрозы безопасности информации», «уязвимости», «источника угрозы». Целостность, конфиденциальность и доступность информации. Классификационная схема угроз безопасности информации.	4*
5	Основы организации и ведения работ по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных.	Методические рекомендации по классификации и категорированию объектов информатизации. Характеристика основных угроз несанкционированного доступа и моделей нарушителя безопасности информации	4*

6	Основы организации и ведения работ по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных	Особенности информационного элемента информационной системы персональных данных. Угрозы утечки информации по техническим каналам	4*
7	Основы организации и ведения работ по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных	Основные типы актуальных угроз безопасности персональных данных при их обработке в информационных системах персональных данных, порядок их определения. Угрозы несанкционированного доступа к информации в информационных системах персональных данных.	4*
8	Основы организации и ведения работ по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных	Основные принципы обеспечения безопасности персональных данных при их обработке.	4*
9	Основы организации и ведения работ по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных	Основные направления деятельности по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных.	4*
10	Основы организации и ведения работ по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных	Классификация информационных систем персональных данных.	4*
11	Основы организации и ведения работ по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных	Состав мер по обеспечению безопасности персональных данных. Порядок выбора мер по обеспечению безопасности персональных данных, подлежащих реализации в информационной системе.	4*
12	Основы организации и ведения работ по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных	Содержание, порядок разработки и ввода в действие внутренних нормативных документов и актов ненормативного характера по обработке персональных данных и обеспечению безопасности персональных данных. Обязанности оператора, осуществляющего обработку персональных данных.	4*

5.2.2 Практические занятия (семинары)

№ п/п	Наименование раздела дисциплины	Тематика практических занятий (семинаров)	Трудоемкость, ак. ч
1	Правовые и организационные вопросы технической защиты персональных данных	Анализ Стратегии национальной безопасности Российской Федерации года и Доктрины информационной безопасности Российской Федерации. Концептуальные основы ТЗИ	6*
		Анализ классификационной схемы угроз безопасности информации и их общая характеристика.	6*
		Анализ особенностей проведения комплексного исследования объектов информатизации на наличие угроз безопасности информации и методов оценки опасности угроз.	6*
		Разработка типовых документов, содержащих Классификационную схему угроз безопасности информации при организации обработки персональных данных.	6*
		Разработка типовых документов, содержащих информацию о Классификации и категорировании объектов информатизации.	6*
		Разработка типовых документов, содержащих общую и частную моделей нарушителя.	6*
2	Основы организации и ведения работ по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных	Анализ общего порядка организации обеспечения безопасности персональных данных в информационных системах персональных данных.	6*
		Анализ категорирования персональных данных обрабатываемых в информационных системах	6*
		Разработка документа, содержащего концепцию защиты персональных данных.	6*
		Разработка документа, содержащего облик системы защиты персональных данных и ее внедрение	6*
		Анализ порядка классификации информационных систем персональных данных	6*
		Анализ содержания мер по обеспечению безопасности персональных данных, реализуемых в рамках системы защиты персональных данных	6*

5.2.3 Лабораторный практикум

Не предусмотрен.

5.2.4 Самостоятельная работа обучающихся

№ п/п	Наименование раздела дисциплины	Вид СРО	Трудоемкость, ак. ч
1	Правовые и организационные вопросы технической защиты персональных данных	Проработка материалов по учебнику для подготовки к практическим занятиям	13.3

		Оформление отчетов по практическим работам	6.2
2	Основы организации и ведения работ по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных	Проработка материалов по учебнику для подготовки к практическим занятиям	26.6
		Оформление отчетов по практическим работам	13.3
		Работа над курсовым проектом	27.2

6 Учебно-методическое и информационное обеспечение дисциплины (модуля)

Для освоения дисциплины обучающийся может использовать:

6.1 Основная литература

1. Петренко, В. И. Защита персональных данных в информационных системах : учебное пособие / В. И. Петренко ; Северо-Кавказский федеральный университет. – Ставрополь : Северо-Кавказский Федеральный университет (СКФУ), 2016. – 201 с. : схем. — URL: https://biblioclub.ru/index.php?page=book&id=459205
2. Аверченков, В. И. Защита персональных данных в организации / В. И. Аверченков, М. Ю. Рытов, Т. Р. Гайнулин. – 3-е изд., стер. – Москва : ФЛИНТА, 2016. – 124 с. — URL: https://biblioclub.ru/index.php?page=book&id=93260
3. Скрипник, Д. А. Обеспечение безопасности персональных данных: курс / Д. А. Скрипник ; Национальный Открытый Университет "ИНТУИТ". – Москва : Интернет-Университет Информационных Технологий (ИНТУИТ), 2011. – 109 с. : ил., схем. — URL: https://biblioclub.ru/index.php?page=book&id=234794

6.2 Дополнительная литература

1. Кияев, В. Безопасность информационных систем: курс : [16+] / В. Кияев, О. Граничин. – Москва : Национальный Открытый Университет «ИНТУИТ», 2016. – 192 с. : ил. — URL: https://biblioclub.ru/index.php?page=book&id=429032
2. Программно-аппаратные средства обеспечения информационной безопасности : учебное пособие / А. В. Душкин, О. М. Барсуков, К. В. Славнов, Е. В. Кравцов ; под ред. А. В. Душкина. – Москва : Горячая линия – Телеком, 2016. – 248 с. : схем., табл., ил. – URL: https://biblioclub.ru/index.php?page=book&id=483768

6.3 Перечень учебно-методического обеспечения для самостоятельной работы обучающихся

1. Данылив, М. М. 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. – 32 с. Режим доступа в электронной среде: http://biblos.vsuet.ru/MegaPro/Web/SearchResult/MarcFormat/100813.

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

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 (модулю), включая перечень программного обеспечения и информационных справочных систем

При изучении дисциплины используется программное обеспечение и информационные справочные системы: информационная среда для дистанционного обучения «Moodle», локальная сеть университета и глобальная сеть Internet.

При освоении дисциплины используется лицензионное и открытое программное обеспечение – *ОС Windows; Microsoft Office.*

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 промежуточной аттестации	Комплект мебели для учебного процесса – 80 шт. Переносной проектор Acer. Аудио-визуальная система лекционных аудиторий (мультимедийный проектор EpsonEB-X18, настенный экран ScreenMedia)	Microsoft Windows 8.1, Microsoft Office 2007 Standart, Microsoft Office 2007 Russian Academic OPEN No Level #44822753 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 (модулю)

Оценочные материалы (ОМ) для дисциплины (модуля) включают в себя:

- 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 (модуля)**.

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

ОЦЕНОЧНЫЕМАТЕРИАЛЫ

ДЛЯ ПРОМЕЖУТОЧНОЙ АТТЕСТАЦИИ

по дисциплине

Безопасность персональных данных

1 Перечень компетенций с указанием этапов их формирования

№ п/п	Код компетенции	Формулировка компетенции	Код и наименование индикатора достижения компетенции
1	ОПК-6	способен при решении профессиональных задач организовывать защиту информации ограниченного доступа в автоматизированных системах в соответствии с нормативными правовыми актами, нормативными и методическими документами Федеральной службы безопасности Российской Федерации, Федеральной службы по техническому и экспортному контролю	ИД1$_{ОПК-6}$ – обладает навыками разработки автоматизированных систем с учетом политики информационной безопасности с использованием современных программных средств
2	ОПК-5.1	способен разрабатывать и реализовывать политику информационной безопасности открытых информационных систем	ИД1$_{ОПК-5.1}$ – обладает навыками разработки политик информационное безопасности различных открытых информационных систем
3	ОПК-5.3	способен осуществлять контроль обеспечения информационной безопасности и проводить верификацию данных в открытых информационных системах	ИД1$_{ОПК-5.3}$ – обладает навыками контроля данных, в том числе персональных и обеспечения их безопасности

Код и наименование индикатора достижения компетенции	Результаты обучения (показатели оценивания)
ИД1$_{ОПК-6}$ – обладает навыками разработки автоматизированных систем с учетом политики информационной безопасности с использованием современных программных средств	Знает: основы теории проектирования информационных систем персональных данных
	Умеет: формировать конструкторскую документацию при проектировании информационных систем персональных данных
	Владеет: навыками разработки технических проектов систем защиты
ИД1$_{ОПК-5.1}$ – обладает навыками разработки политик информационное безопасности различных открытых информационных систем	Знает: требования к содержанию и составу внутренних нормативных документов по защите персональных данных
	Умеет: обосновать контекст безопасности для организации оператора персональных данных
	Владеет: навыками по формированию основных разделов политик информационное безопасности
ИД1$_{ОПК-5.3}$ – обладает навыками контроля данных, в том числе персональных и обеспечения их безопасности	Знает: требования законодательства к планам контролирующих мероприятий информационных систем персональных данных
	Умеет: выполнять периодический контроль требований по защите персональных данных
	Владеет: навыками использования инструментальных средств контроля правил защиты персональных данных в информационных системах

2 Паспорт оценочных материалов по дисциплине

№ п/п	Разделы дисциплины	Код и наименование индикатора достижения компетенции	Оценочные материалы		Технология/процедура оценивания (способ контроля)
			наименование	№№ заданий	
1	Правовые и организационные вопросы технической защиты персональных данных	ИД1$_{ОПК-6}$ – обладает навыками разработки автоматизированных систем с учетом политики информационной безопасности с использованием современных программных средств	Вопросы к зачету	1-15	Проверка преподавателем (уровневая шкала)
			Банк тестовых заданий	46-60	Бланочное тестирование (процентная шкала)
			Задания для практических работ	101-110	Проверка преподавателем (уровневая шкала)
			Домашнее задание	131-140	Проверка преподавателем (уровневая шкала)
2	Классификация открытых информационных систем	ИД1$_{ОПК-5.1}$ – обладает навыками разработки политик информационное безопасности различных открытых информационных систем ИД1$_{ОПК-5.3}$ – обладает навыками контроля данных, в том числе персональных и обеспечения их безопасности	Вопросы к зачету	16-30 31-45	Проверка преподавателем (уровневая шкала)
			Банк тестовых заданий	61-85 86-100	Бланочное тестирование (процентная шкала)
			Задания для практических работ	111-120 121-130	Проверка преподавателем (уровневая шкала)
			Домашнее задание	131-140	Проверка преподавателем (уровневая шкала)

3 Оценочные материалы для промежуточной аттестации

Аттестация обучающегося по дисциплине проводится в форме письменного ответа и предусматривает возможность последующего собеседования (зачета).

Каждый вариант теста включает 2 контрольных вопроса и1 задачу, из них:

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

- 5 контрольныхзаданий на проверку навыков.

Каждый билет включает 3 контрольных вопроса, из них:

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

3.1 Вопросы к экзамену.

ОПК-6 способен при решении профессиональных задач организовывать защиту информации ограниченного доступа в автоматизированных системах в соответствии с нормативными правовыми актами, нормативными и методическими документами Федеральной службы безопасности Российской Федерации, Федеральной службы по техническому и экспортному контролю ($ИД1_{ОПК-6}$ – обладает навыками разработки автоматизированных систем с учетом политики информационной безопасности с использованием современных программных средств)

№ задания	Формулировка вопроса
1	Что такое защита информации?
2	Что является основным содержанием защиты информации?
3	Что такое защищаемая информация?
4	Что такое угроза безопасности информации?
5	Что такое естественная угроза безопасности информации?
6	Что такое искусственная угроза безопасности информации?
7	Какое отличие между непреднамеренными и преднамеренными угрозами безопасности информации?
8	Какие основные виды преднамеренных угроз безопасности информации?
9	Какими основными законами Российской федерации регламентирована защита конфиденциальных данных в организациях различной ведомственной принадлежности?
10	Какие основные категории конфиденциальных данных, обрабатываемых в информационных системах?
11	Какие объекты из состава информационных систем в учреждении требуют реализации организационных и технических мероприятий по защите конфиденциальных данных?
12	Какая информация о человеке должна быть отнесена к категории персональные данные?
13	Какая информация о сотрудниках должна быть отнесена к категории персональные данные?
14	Какая технологическая информация об информационных системах должна быть отнесена к категории персональные данные?
15	Какие данные требуют выполнения ряда мероприятий по защите информации в организации кроме конфиденциальных данных?

ОПК-5.1 Способен разрабатывать и реализовывать политику информационной безопасности открытых информационных систем ($ИД1_{ОПК-5.1}$ – обладает навыками разработки политик информационное безопасности различных открытых информационных систем).

№ задания	Формулировка вопроса
16	Что является информационным основанием функционирования организации различной ведомственной принадлежности?
17	Какой состав программного обеспечения типовой информационной системы?
18	Какой состав аппаратного обеспечения типовой информационной системы?
19	Какими особенностями функционирования обладают информационные системы с точки зрения решения задачи обеспечения защиты конфиденциальных данных?
20	Основные способы защиты информации при обработке персональных данных в информационных системах.
21	Основные средства защиты информации при обработке персональных данных в информационных системах.
22	Состав и основные функции систем защиты информации уровня отдельных ЭВМ.
23	Какие основные принципы построения и эксплуатации систем защиты информации?
24	Назовите основные типы систем защиты информации, используемые для защиты конфиденциальных данных в информационных системах?
25	Какими защитными функциями обеспечения безопасности информации наиболее распространенных операционных систем можно воспользоваться при построении защиты конфиденциальных?

26	Какой главный недостаток защитных функций обеспечения безопасности информации наиболее распространенных операционных систем с точки зрения защиты конфиденциальных данных?
27	Назовите основные защитные функции, реализуемые операционной системой WINDOWSXP.
28	Назовите основные защитные функции, реализуемые операционной системой LINUX.
29	Какой состав системы защиты информации уровня отдельной ЭВМ?
30	Что является информационным основанием функционирования организации различной ведомственной принадлежности?

ОПК-5.3 способен осуществлять контроль обеспечения информационной безопасности и проводить верификацию данных в открытых информационных системах ($ИД1_{ОПК-5.3}$ – обладает навыками контроля данных, в том числе персональных и обеспечения их безопасности,)

№ задания	Формулировка вопроса
31	Какие параметры могут использоваться в качестве критериев анализа межсетевых экранов.
32	Назовите назначение системы обнаружения вторжений.
33	Назовите назначение средств построения виртуальных частных сетей.
34	Назовите назначение средств централизованного управления информационной безопасностью.
35	Назовите назначение средств анализа защищенности информационных систем.
36	Какие основные этапы и их содержание выполняемых действий руководителем учреждения при организации защиты персональных данных?
37	Какие основные этапы и их содержание выполняемых действий ответственным за обработку персональных данных сотрудником при организации защиты персональных данных?
38	Какие основные этапы и их содержание выполняемых действий ответственным за защиту персональных данных сотрудником при организации защиты?
39	Какие основные признаки классификации информационных систем при организации защиты персональных данных?
40	Какая последовательность действий при проведении классификации информационных систем?
41	Какие основные классы конфиденциальности информационных систем существуют?
42	Что такое акт классификации информационной системы?
43	Что такое политики безопасности персональных данных?
44	Что такое модель угроз безопасности персональных данных?
45	Что такое сертификат ФСТЭК России на устанавливаемые системы защиты?

3.2Тесты (тестовые задания)

ОПК-6 способен при решении профессиональных задач организовывать защиту информации ограниченного доступа в автоматизированных системах в соответствии с нормативными правовыми актами, нормативными и методическими документами Федеральной службы безопасности Российской Федерации, Федеральной службы по техническому и экспортному контролю ($ИД1_{ОПК-6}$ – обладает навыками разработки автоматизированных систем с учетом политики информационной безопасности с использованием современных программных средств)

№ задания	Тестовое задание с вариантами
46	Данные, полученные при сканировании паспорта оператором персональных данных для подтверждения осуществления определенных действий конкретным лицом, относят 1. к биометрическим персональным данным 2. к специальной категории персональных данных **3. к персональным данным**
47	Оператор до начала обработки персональных данных обязан уведомить территориальный орган Роскомнадзора о своем намерении осуществлять обработку персональных данных. Верно ли данное суждение? **1. Да** 2. Нет
48	Неавтоматизированная обработка персональных данных это: 1. обработка персональных данных с помощью средств вычислительной техники **2. обработка персональных данных, осуществляемая при непосредственном участии человека**

	3. смешенная обработка персональных данных
49	Фотографические изображения обучающихся, сотрудников и посетителей организации относят: **1. К биометрическим персональным данным** 2. К специальной категории персональных данных
50	Сбор, хранение, использование и распространение информации о частной жизни человека без его согласия допускается согласно Конституции РФ? 1. резрешено без ограничений 2. разрешено частично **3. запрещено**
51	Оператором персональных данных может быть физическое лицо? 1. может 2. не может 3. может при обработке деперсонифицированных данных
52	Фотографическое изображение, содержащееся в личном деле работника, относят 1. к биометрическим персональным данным 2. к специальной категории персональных данных **3. к персональным данным**
53	Сведения, характеризующие физиологические и биологические особенности человека, на основе которых можно установить его личность и которые используются оператором для установления личности субъекта персональных данных, относят: **1. К биометрическим персональным данным** 2. К специальной категории персональных данных 3. К общедоступным персональным данным 4. К личным данным
54	Обработка специальных категорий персональных данных допускается в целях? 1. Накопления 2. Реализации 3. Анализа **4. Запрещена**
55	Что такое «распространение персональных данных»? 1. Действия, в результате которых становится возможным без использования дополнительной информации определить принадлежность персональных данных конкретному субъекту персональных данных 2. Любое действие (операция) или совокупность действий (операций), совершаемых с использованием средств автоматизации или без использования таких средств с персональными данными, включая сбор, запись, систематизацию, накопление, хранение, уточнение (обновление, изменение), извлечение, использование, передачу (распространение, предоставление, доступ), обезличивание, блокирование, удаление, уничтожение персональных данных **3. Действия, направленные на раскрытие персональных данных неопределенному кругу лиц**
56	В каких из перечисленных случаев обработка персональных данных без согласия субъекта разрешена? (Выберите все правильные ответы) **1. В связи с исполнением судебных актов** **2. При противодействии терроризму** **3. В случаях, предусмотренных законодательством Российской Федерации о персональных данных**
57	Как называется совокупность условий и факторов, создающих потенциальную или реально существующую опасность нарушения безопасности информации? 1. уязвимость 2. слабое место системы **3. угроза** 4. атака
58	В отношении информации, доступ к которой ограничен федеральными законами, необходимо соблюдать следующее требование: 1. обеспечение доступности 2. обеспечение неотказуемости **3. обеспечение конфиденциальности** 4. обеспечение целостности
59	Как называется гражданин или юридическое лицо, осуществляющие деятельность по эксплуатации информационной системы, в том числе по обработке информации, содержащейся в ее базах данных? **1. оператор информационной системы**

	2. обладатель информации 3. субъект информации 4. обладатель информационной системы
60	Информация, к которой нельзя ограничить доступ: **1. информация о работе государственных органов** **2. информация об окружающей среде** 3. персональные данные субъекта 4. информация о здоровье субъекта

ОПК-5.1 Способен разрабатывать и реализовывать политику информационной безопасности открытых информационных систем (ИД1$_{ОПК-5.1}$ – обладает навыками разработки политик информационное безопасности различных открытых информационных систем).

№ задания	Формулировка вопроса
61	Требования по защите от НСД каких классов ИСПД в многопользовательском режиме при разных правах доступа совпадают? 1. 1 и 2 классов **2. 2 и 3 классов** 3. 1 и 3 классов 4. 3 и 4 классов
62	В каком законодательном документе определено понятие профиля защиты? ФЗ “О персональных данных” **1. ГОСТ “Информационная технология. Методы и средства обеспечения безопасности. Критерии оценки безопасности информационных технологий”** 2. ФЗ “Об информации, информационных технологиях и о защите информации” 3. ФЗ “О безопасности”
63	Наличие межсетевого экрана необходимо при: 1. использовании изолированной локальной сети **2. использовании сетей общего пользования** 3. использовании почтового ящика в сети Интернет 4. использовании автономного автоматизированного рабочего места
64	Если ИСПД подключена к Интернету и в ней используются съемные носители, для защиты от НСД необходимо использование: 1. браузера 2. защищенных каналов связи **3. антивирусной защиты** 4. носителей, открытых на запись
65	В каком документе содержатся состав, содержание и сроки проведения работ по разработке и внедрению СЗПД? **1. в техническом задании СЗПД** 2. матрице доступа 3. в частной модели угроз 4. в проекте СЗПД
66	Какой участник процесса сертификации оформляет экспертное заключение по сертификации средств защиты информации? 1. органы по сертификации средств защиты информации 2. заявитель 3. федеральный орган по сертификации 4. испытательные лаборатории
67	На каком этапе создания системы защиты персональных данных разрабатывается частная модель угроз? 1. ввод в действие 2. эксплуатация 3. стадия проектирования **4. предпроектная стадия**
68	На каком этапе создания СЗПД производится закупка технических средств защиты? 1. эксплуатация 2. ввод в действие 3. (Правильный ответ) стадия проектирования 4. предпроектная стадия

69	Какой срок действия у сертификата средства защиты информации? 1. 10 лет **2. 3 года** 3. 5 лет 4. 2 года
70	Как называется мероприятие по защите информации, предусматривающее применение специальных технических средств, а также реализацию технических решений? 1. создание СЗПД 2. административное мероприятие 3. организационное мероприятие **4. техническое мероприятие**
71	На каком этапе создания СЗПД производится опытная эксплуатация средств защиты? 1. эксплуатация 2. предпроектная стадия 3. стадия проектирования **4. ввод в действие**
72	На каком этапе создания системы защиты персональных данных определяется состав персональных данных и необходимость их обработки? 1. эксплуатация **2. предпроектная стадия** 3. ввод в действие 4. стадия проектирования
80	Какие подсистемы в рамках СЗПД можно не использовать, если ИСПД является изолированной (локальной)? **1. подсистема безопасности межсетевого взаимодействия** 2. подсистема криптографической защиты информации **3. подсистема обнаружения вторжений** 4. подсистема обеспечения целостности 5. подсистема анализа защищенности 6. подсистема управления доступом, регистрации и учета 7. подсистема антивирусной защиты
81	Как называются меры защиты, которые создают маскирующие акустические и вибрационные помехи? 1. криптографические меры защиты **2. активные меры защиты от утечки по техническим каналам** 3. пассивные меры защиты от утечки по техническим каналам 4. активные меры защиты от несанкционированного доступа
82	Какая подсистема в рамках СЗПД предназначена для защиты информационной системы от вредоносных программ? 1. подсистема обнаружения вторжений **2. подсистема антивирусной защиты** 3. подсистема безопасности межсетевого взаимодействия 4. подсистема анализа защищенности
83	Что является основанием для включения оператора в ежегодный план проверок ФСТЭК? 1. предписание Роскомнадзора 2. заявления и обращения граждан **3. истечение 3 лет со дня последней плановой проверки** **4. истечение 3 лет со дня государственной регистрации**
84	Выберите утверждения, характеризующие антивирусы с эвристическим методом обнаружения вирусов: 1. не способны находить неизвестные вирусы **2. способны находить неизвестные вирусы** 3. гарантированно находят известные вирусы **4. имеют большое количество ложных срабатываний**
85	Какой орган является регулятором в части, касающейся контроля и выполнения требований по организации и техническому обеспечению безопасности ПД (не криптографическими методами) при их обработке в ИСПД? **1. ФСТЭК** 2. Роспотребнадзор 3. ФСБ 4. Роскомнадзор

ОПК-5.3 способен осуществлять контроль обеспечения информационной безопасности и проводить верификацию данных в открытых информационных системах ($ИД1_{ОПК-5.3}$ – обладает навыками контроля данных, в том числе персональных и обеспечения их безопасности)

№ задания	Тестовое задание с вариантами
86	Что является первоисточником права в Российской Федерации? 1. Уголовный кодекс РФ **2. Конституция РФ** 3. Международные договора РФ 4. Федеральные законы РФ
87	На кого возлагается ответственность за организацию работ по ТКЗИ в организации? 1. отдел кадров 2. руководителя подразделения по защите информации 3. **руководителя организации** 4. главного конструктора
88	Как называется автоматизированная система, реализующая информационную технологию выполнения установленных функций в соответствии с требованиями стандартов и/или иных нормативных документов по защите информации? 1. государственная автоматизированная система 2. автоматизированная система обработки персональных данных 3. **автоматизированная система в защищенном исполнении** 4. объект информатизации
89	Как называется комплекс административных и ограничительных мер, направленных на защиту информации путем регламентации деятельности персонала и порядка функционирования средств (систем)? 1. правовые меры защиты 2. **организационные меры защиты** 3. криптографические меры защиты 4. программно-технические меры защиты
90	Выделите организационные меры защиты информации от утечки по ТКУИ. **1. определение границ контролируемой зоны** 2. экранирование ОТСС 3. пространственное зашумление 4. **введение временных ограничений в режимах использования технических средств**
91	Что позволяет субъекту(пользователю, процессу, действующему от имени какого-либо пользователя, или программно-аппаратному компоненту) назвать себя? 1. манипулятор **2. идентификатор** 3. аутентификатор 4. агрегатор
92	Выделите формы подтверждения соответствия, выделенные в ФЗ "О техническом регулировании": **1. добровольная сертификация** 2. испытания **3. декларирование соответствия** **4. обязательная сертификация** 5. лицензирование
93	В соответствии с ФЗ №149 "Об информации, информационных технологиях и о защите информации" информация разделяется на следующие категории: 1. общедоступная и конфиденциальная **2. общедоступная и ограниченного доступа** 3. ограниченного доступа и государственная тайна 4. конфиденциальная информация и государственная тайна
94	Какой федеральный орган осуществляет деятельность по аккредитации объектов информатизации? 1. ФСБ **2. ФСТЭК** 3. Роспотребнадзор **4.** Минкомсвязь
95	Как называется информация или носитель информации, или информационный процесс, которые необходимо защищать в соответствии с поставленной целью защиты информации? 1. субъект защиты

	2. автоматизированная система **3.** объект информатизации **4. объект защиты**
96	Какая логическая цепочка является корректной? 1. Источник угрозы - уязвимость -атака- угроза 2. Источник угрозы - угроза - уязвимость -атака **3. Источник угрозы - уязвимость-угроза-атака** 4. Угроза-уязвимость-источник угрозы-атака
97	Как называется воздействие на защищаемую информацию с помощью вредоносных программ? 1. программно-аналитическое воздействие 2. программно-аппаратное воздействие 3. технически-математическое воздействие 4. **программно-математическое воздействие**
98	Какая категория является наиболее рискованной для компании с точки зрения вероятного мошенничества и нарушения безопасности? **1. Сотрудники** 2. Хакеры 3. Атакующие 4. Контрагенты (лица, работающие по договору)
99	Если различным группам пользователей с различным уровнем доступа требуется доступ к одной и той же информации, какое из указанных ниже действий следует предпринять руководству? 1. Снизить уровень безопасности этой информации для обеспечения ее доступности и удобства использования 2. Требовать подписания специального разрешения каждый раз, когда человеку требуется доступ к этой информации **3. Улучшить контроль за безопасностью этой информации** 4. Снизить уровень классификации этой информации
100	Что самое главное должно продумать руководство при классификации данных? 1. Типы сотрудников, контрагентов и клиентов, которые будут иметь доступ к данным **2. Необходимый уровень доступности, целостности и конфиденциальности** 3. Оценить уровень риска и отменить контрмеры 4. Управление доступом, которое должно защищать данные

3.3 Задания для практических работ (типовые задачи)

ОПК-6 способен при решении профессиональных задач организовывать защиту информации ограниченного доступа в автоматизированных системах в соответствии с нормативными правовыми актами, нормативными и методическими документами Федеральной службы безопасности Российской Федерации, Федеральной службы по техническому и экспортному контролю ($ИД1_{ОПК-6}$ – обладает навыками разработки автоматизированных систем с учетом политики информационной безопасности с использованием современных программных средств)

№ задания	Условие задачи (формулировка задания)
101	Определение перечня угроз безопасности персональных данных при их обработке в информационных системах персональных данных
102	Определение уровня исходной защищённости
103	Определение частоты (вероятности) реализации рассматриваемой угрозы
104	Определение коэффициента реализуемости угрозы и возможности реализации
105	Определение актуальных угроз безопасности персональных данных при их обработке в информационных системах персональных данных
106	Определение типа актуальной угрозы
107	Определение состава и содержания организационных мер по обеспечению безопасности персональных данных при их обработке в информационных системах ПДн
108	Определение состава и содержания технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах ПДн
109	Разработка заявки на проведение аттестации ИСД
110	Разработка информационной карточки к заявке на проведение аттестации ИСД

ОПК-5.1 Способен разрабатывать и реализовывать политику информационной безопасности открытых информационных систем ($ИД1_{ОПК-5.1}$ – обладает навыками разработки политик

информационной безопасности различных открытых информационных систем, $ИД2_{ОПК-5.1}$ – обладает навыками внедрения и администрирования политик информационной безопасности различных открытых информационных систем).

№ задания	Условие задачи (формулировка задания)
111	В соответствии с требованиями службы безопасности Ольга еженедельно меняет парольную фразу для доступа к зашифрованному контейнеру на рабочем компьютере. В качестве парольных фраз она использует фразы из своей любимой книги «Маленький принц» на английском языке. Для того чтобы помнить текущий пароль, Ольга оставляет подсказки на своем рабочем месте.
112	BMP (англ. BitMap Picture) – аппаратно-независимое побитовое изображение Windows, используемое для хранения растровых изображений. Дамп памяти изображения размером 5x3 пикселя показан на рисунке Известно, что в картинку было внедрено секретное сообщение так, что изображение не было изменено. Найдите скрытое сообщение
113	Представлен листинг кода на языке C++, выполняющий проверку введенного пароля по определенным параметрам. Определите пароль, при котором программа выведет фразу «Password is correct». Ответ обоснуйте
114	Злоумышленник разработал сетевой вредоносный код, который осуществляет отправку пользовательской информации с зараженного компьютера на центральный сервер. Для того, чтобы его сетевая активность не была обнаружена антивирусными программами, создается скрытый канал передачи информации с использованием поля ID (Идентификатор пакета) в заголовке IP-пакета Файлы какого суммарного объема пользователю зараженного компьютера необходимо отправить в сеть, чтобы вредоносная программа смогла загрузить на центральный сервер 1 Кб пользовательской информации? Ответ обоснуйте.
115	Участники киберсети обмениваются между собой сообщениями с использованием «японского кроссворда». Каждое число в таком кроссворде напротив строки или столбца обозначает один горизонтальный или вертикальный блок, состоящий из указанного числа подряд идущих закрашенных клеток. Между закрашенными блоками должно быть не менее одной пустой клетки. Количество чисел в строке или столбце определяет количество таких блоков в строке или столбце соответственно. Помогите аналитику расшифровать его.
116	У администратора Ивана на рабочем компьютере стоит четырехзначный пароль, состоящий из цифр. После трех неудачных попыток ввода пароля компьютер блокируется. Известно, что сумма первых двух цифр и сумма последних двух цифр пароля равны простым числам. Помощник шпиона пригласил Ивана в кафе на обед. На какое минимальное время необходимо задержать Ивана, чтобы шпион смог гарантированно подобрать пароль от компьютера и скопировать данные, если на ввод пароля требуется 1 секунда, блокировка компьютера осуществляется на 10 секунд, а время копирования нужных данных составляет 2 минуты?
117	Аналитику удалось перехватить зашифрованное изображение, но программа шифрования утеряна. Известно, что шифрование осуществлялось методом «двоичного гаммирования», т.е. путем последовательного выполнения операции «побитового исключающего ИЛИ» между каждым байтом изображения и байтом ключа. Известно также, что ключ формировался в самой программе шифрования. Восстановите текст, записанный на изображении, а также алгоритм шифрования и используемый ключ.
118	Система охраны осуществляет удаленный учёт прохода сотрудников на предприятие с использованием карт сотрудников и контрольной суммы. Для внесения в электронный журнал записи о проходе сотрудника вычисляется контрольная сумма на основе текущей даты, фамилии сотрудника и серийного номера карты
119	Какой серийный номер записать на карту, чтобы успешно пройти на предприятие? В какие дни лучше всего посетить предприятие, чтобы не вызвать подозрений. Ответ обоснуйте/
120	Имеется фрагмент программы на языке C. Был получен фрагмент скомпилированного исполняемого файла в шестнадцатеричном формате, в котором удалось обнаружить следующий программный код. Определите, что нужно подать на вход программы, чтобы в результате выполнения вывелась строка «Пароль верный!». Ответ обоснуйте.

ОПК-5.3 способен осуществлять контроль обеспечения информационной безопасности и проводить верификацию данных в открытых информационных системах ($ИД1_{ОПК-5.3}$ – обладает навыками контроля данных, в том числе персональных и обеспечения их безопасности)

№ задания	Условие задачи (формулировка задания)
121	Олег создал сайт, в котором спрятал IP-адрес своего секретного сервера в формате xxx.xxx.xxx.xxx (xxx –

	число от 0 до 255). На сайте Олег оставил подсказки. Определите IP-адрес секретного сервера Олега.
122	Для входа в систему используется пароль, который состоит из трех двузначных чисел. Двузначные числа образуют между собой примитивную пифагорову тройку (сумма квадратов двух чисел равна квадрату третьего числа, каждое из чисел натуральное, числа взаимно простые). Известно, что первым всегда стоит наименьшее двузначное число. Сколько максимально времени потребуется для подбора пароля, если ввод пароля занимает 1 секунду, а задержка между вводом паролей составляет 1 секунду? Ответ дать в виде числа секунд.
123	Администратору был предоставлен журнал аудита входа в информационную систему. Формат записи журнала: Логин ТипОперации Время ТипОперации принимает одно из значений: Вход или Выход. Время записано в формате ДД.ММ.ГГГГ ЧЧ:ММ:СС. Каждая запись начинается с новой строки. В качестве разделителя между полями записи используется знак табуляции (TAB). Система подразумевает, что при корректной работе у пользователей не может быть более одной открытой сессии. Известно, что была попытка несанкционированного подключения к системе с использованием логина одного из пользователей. Определите время несанкционированного подключения и логин скомпрометированного пользователя.
124	Для передачи сообщения используется цифровая клавиатура и следующий алгоритм шифрования: каждый символ кодируется последовательностью из 3-х цифр. При этом, последовательность не может начинаться с 0 и 9, двигаться между клавишами можно только по правилам шахматного коня. Алфавит какой длины можно использовать при таком алгоритме шифрования?
125	В одном институте спроектировали сеть, схематично изображенной на рисунке. Каждый маленький треугольник на рисунке обозначает компьютер. Треугольники с общей стороной соответствуют компьютерам, которые соединены между собой напрямую. Нарушитель решает заразить один из компьютеров сети вирусом. Вирус распространяется по сети от заражённого компьютера ко всем соседним незаражённым. Однако при передаче на новый компьютер код вируса сжимается в три раза. Когда вирус сжимается до размера 1 Кб, он больше не может передаваться на соседние устройства, но компьютер, на котором он находится, считается заражённым. Какое максимальное количество компьютеров сможет заразить вирус без обнаружения антивирусом, если на первом заражённом компьютере вирус имеет размер 243Кб. В ответе укажите максимальное количество зараженных компьютеров и компьютер, на который нарушитель должен скопировать вирус.
126	Пользователь хранит на сервере секретное слово, доступ к которому можно получить, авторизовавшись через web-сайт. Сервер выдаст секретное слово только в том случае, если ему будет отправлена верная зашифрованная последовательность, сформированная из логина и пароля. Чтобы не забыть логин и пароль, пользователь оставил себе подсказки на сайте. Также известно, что: 1. Логин и пароль имеют одинаковую длину. 2. Логин состоит только из латинских букв, пароль состоит только из цифр. Определите секретное слово.
127	Аналитику удалось обнаружить папку с графическими изображениями и текстовым файлом. Известно, что в изображениях скрыто кодовое слово. Помогите определить кодовое слово, если известно, что для его сокрытия изменили содержимое всех файлов.
128	Система аутентификации шифрует пароли особым образом, показанном в виде функции scrambler на языке C++. Зная алгоритм шифрования, вычислите пароль. Фрагмент кода указан ниже.
129	В разделе импорта заголовка исполняемого файла содержится информация о подключаемых библиотеках (DLL) и импортируемых из них функциях. Для подмены одной из DLL необходимо, чтобы имя библиотеки и набор функций совпадали с именем библиотеки и набором функций, описанными в разделе импорта исполняемого файла. Для упрощения разработки подменяемой библиотеки DLL, из всех библиотек выбирают ту, из которой импортируется наименьшее количество функций. Из предоставленного образа раздела импорта определите имя библиотеки, из которой импортируется наименьшее количество функций. В ответе укажите имя библиотеки DLL, имена импортируемых из нее функций и количество аргументов каждой из таких функций
130	Пользователь хранит на сервере секретное слово, доступ к которому можно получить, авторизовавшись через web-сайт. Сервер выдаст секретное слово только в том случае, если ему будет отправлена верная зашифрованная последовательность, сформированная из логина и пароля. Чтобы не забыть логин и пароль, пользователь оставил себе подсказки на сайте. Определите секретное слово.

3.4 Домашнее задание (типовые задачи)

ОПК-6 способен при решении профессиональных задач организовывать защиту информации ограниченного доступа в автоматизированных системах в соответствии с нормативными правовыми актами, нормативными и методическими документами Федеральной службы безопасности Российской Федерации, Федеральной службы по

техническому и экспортному контролю ($ИД1_{ОПК-6}$ – обладает навыками разработки автоматизированных систем с учетом политики информационной безопасности с использованием современных программных средств).

ОПК-5.1 Способен разрабатывать и реализовывать политику информационной безопасности открытых информационных систем ($ИД1_{ОПК-5.1}$ – обладает навыками разработки политик информационной безопасности различных открытых информационных систем, $ИД2_{ОПК-5.1}$ – обладает навыками внедрения и администрирования политик информационной безопасности различных открытых информационных систем).

ОПК-5.3 способен осуществлять контроль обеспечения информационной безопасности и проводить верификацию данных в открытых информационных системах ($ИД1_{ОПК-5.3}$ – обладает навыками контроля данных, в том числе персональных и обеспечения их безопасности)

№ задания	Формулировка задания
131	Тема реферата. В каком случае предусмотрен самый высокий штраф за неправомерную обработку персональных данных
132	Тема реферата. Какую ответственность можно понести за нарушение законов в области обработки персональных данных
133	Тема реферата. Что является основной деятельностью Группы реагирования на инциденты информационной безопасность.
134	Тема реферата. Какие средства защиты информации реализуют те же функции, что аппаратные и программные средства в отдельности, и имеют промежуточные свойства, такие как защита помещения от прослушивания
135	Тема реферата. Как называется комплекс аппаратных и программных мер, осуществляющих фильтрацию проходящих через него сетевых пакетов
136	Тема реферата. Сколько существует основных методов поиска вирусов при использовании антивирусных программ
137	Тема реферата. Какой модуль системы защиты информации содержит централизованную, управляемую IT инфраструктуру предприятия с изолированным сервером для хранения информации
138	Тема реферата. Что является заключительным шагом при создании системы защиты информации
139	Тема реферата. Всегда ли Политика обеспечения безопасности персональных данных должна разрабатываться как отельный документ
140	Тема реферата. Как называется подсистема, которая предназначена для поддержания в актуальном состоянии организационно-распорядительных документов по обеспечению ИБ

4. Методические материалы,определяющие процедуры оценивания знаний, умений, навыкови (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.

5. 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-6 способен при решении профессиональных задач организовывать защиту информации ограниченного доступа в автоматизированных системах в соответствии с нормативными правовыми актами, нормативными и методическими документами Федеральной службы безопасности Российской Федерации, Федеральной службы по техническому и экспортному контролю					
ИД1$_{ОПК-6}$ – обладает навыками разработки автоматизированных систем с учетом политики информационной безопасности с использованием современных программных средств					
Знает: основы теории проектирования информационных систем персональных данных	Результаты текущего тестирования	Правильность ответов при тестировании	Обучающийся ответил на 85-100 % вопросов	Отлично	Освоена / повышенный
			Обучающийся ответил на 70-84 % вопросов	Хорошо	Освоена / повышенный
			Обучающийсяответил на 50-69 % вопросов	Удовлетворительно	Освоена / базовый
			Обучающийся ответил на 0-49 % вопросов	неудовлетворительно	Не освоена / недостаточный
	Вопросы к зачету	Правильность ответов	Обучающийсядал исчерпывающий ответ на вопрос, не допустил ошибок. Студент владеет знаниями и умениями по дисциплине в полном объеме	Отлично	Освоена / повышенный
			Обучающийсядал подробный и полный ответ, допустил не более 1 ошибки. Студент владеет знаниями и умениями по дисциплине в полном объеме	Хорошо	Освоена / повышенный
			Обучающийсядал поверхностный ответ на вопрос, допустил более 2 ошибок	Удовлетворительно	Освоена / базовый
			Обучающийсяне смог правильно ответить на вопрос, допустил ошибку в анализе задания	неудовлетворительно	Не освоена / недостаточный
Умеет: формировать конструкторскую документацию при проектировании информационных систем персональных данных	Задания для практических работ	Правильность и полнота выполнения задания	Обучающийся правильно выбрал инструменты для решения задачи, систематизировал и наглядно представил полученные данные, сделал развернутые выводы	Отлично	Освоена / повышенный
			Обучающийся правильно выбрал инструменты для решения задачи, систематизировал и наглядно представил полученные данные, сделал краткие выводы	Хорошо	Освоена / повышенный
			Обучающийся правильно выбрал инструменты для решения задачи, но не смог грамотно их применить, выводы отсутствуют	Удовлетворительно	Освоена / базовый
			Обучающийся не смог правильно выбрать инструменты для решения задачи	неудовлетворительно	Не освоена / недостаточный

Владеет: навыками разработки технических проектов систем защиты	Домашнее задание	Правильность и полнота выполнения задания	Обучающийся разносторонне проанализировал ситуацию, выбрал верную методику решения, сделал развернутые выводы, не допустил ошибок в расчетах	Отлично	Освоена / повышенный
			Обучающийся разносторонне проанализировал ситуацию, полностью выполнил задание, сделал вывод, допустил не более 1 ошибки в расчетах	Хорошо	Освоена / повышенный
			Обучающийся поверхностно проанализировал ситуацию, выполнил задание, сделал вывод, допустил не более 2 ошибок в расчетах	Удовлетворительно	Освоена / базовый
			Обучающийся не смог правильно решить задачу, допустил ошибку в анализе ситуации	неудовлетворительно	Не освоена / недостаточный
ОПК-5.1 Способен разрабатывать и реализовывать политику информационной безопасности открытых информационных систем					
ИД1$_{ОПК-5.1}$ – обладает навыками разработки политик информационной безопасности различных открытых информационных систем, ИД2$_{ОПК-5.1}$ – обладает навыками внедрения и администрирования политик информационной безопасности различных открытых информационных систем					
Знает: требования к содержанию и составу внутренних нормативных документов по защите персональных данных Знает: требования законодательства к планам контролирующих мероприятий информационных систем персональных данных	Результаты текущего тестирования	Правильность ответов при тестировании	Обучающийся ответил на 85-100 % вопросов	Отлично	Освоена / повышенный
			Обучающийся ответил на 70-84 % вопросов	Хорошо	Освоена / повышенный
			Обучающийся ответил на 50-69 % вопросов	Удовлетворительно	Освоена / базовый
			Обучающийся ответил на 0-49 % вопросов	неудовлетворительно	Не освоена / недостаточный
	Вопросы к зачету	Правильность ответов	Обучающийся дал исчерпывающий ответ на вопрос, не допустил ошибок. Студент владеет знаниями и умениями по дисциплине в полном объеме	Отлично	Освоена / повышенный
			Обучающийся дал подробный и полный ответ, допустил не более 1 ошибки. Студент владеет знаниями и умениями по дисциплине в полном объеме	Хорошо	Освоена / повышенный
			Обучающийся дал поверхностный ответ на вопрос, допустил более 2 ошибок	Удовлетворительно	Освоена / базовый
			Обучающийся не смог правильно ответить на вопрос, допустил ошибку в анализе задания	неудовлетворительно	Не освоена / недостаточный
Умеет: обосновать контекст безопасности для организации оператора персональных данных Умеет: выполнять периодический контроль требований по защите персональных данных	Задания для практических работ	Правильность и полнота выполнения задания	Обучающийся правильно выбрал инструменты для решения задачи, систематизировал и наглядно представил полученные данные, сделал развернутые выводы	Отлично	Освоена / повышенный
			Обучающийся правильно выбрал инструменты для решения задачи, систематизировал и наглядно представил полученные данные, сделал краткие выводы	Хорошо	Освоена / повышенный
			Обучающийся правильно выбрал инструменты для	Удовлетворите	Освоена /

			решения задачи, но не смог грамотно их применить, выводы отсутствуют	льно	базовый
			Обучающийся не смог правильно выбрать инструменты для решения задачи	неудовлетвори тельно	Не освоена / недостаточный
Владеет: навыками по формированию основных разделов политик информационное безопасности Владеет: навыками использования инструментальных средств контроля правил защиты персональных данных в информационных системах	Домашнее задание	Правильнос ть и полнота выполнения задания	Обучающийся разносторонне проанализировал ситуацию, выбрал верную методику решения, сделал развернутые выводы, не допустил ошибок в расчетах	Отлично	Освоена / повышенный
			Обучающийся разносторонне проанализировал ситуацию, полностью выполнил задание, сделал вывод, допустил не более 1 ошибки в расчетах	Хорошо	Освоена / повышенный
			Обучающийся поверхностно проанализировал ситуацию, выполнил задание, сделал вывод, допустил не более 2 ошибок в расчетах	Удовлетворите льно	Освоена / базовый
			Обучающийся не смог правильно решить задачу, допустил ошибку в анализе ситуации	неудовлетвори тельно	Не освоена / недостаточный
ОПК-5.3 способен осуществлять контроль обеспечения информационной безопасности и проводить верификацию данных в открытых информационных системах					
$ИД1_{ОПК-5.3}$ – обладает навыками контроля данных, в том числе персональных и обеспечения их безопасности					
Знает: требования законодательства к планам контролирующих мероприятий информационных систем персональных данных	Результаты текущего тестирования	Правильнос ть ответов при тестировани и	Обучающийся ответил на 85-100 % вопросов	Отлично	Освоена / повышенный
			Обучающийся ответил на 70-84 % вопросов	Хорошо	Освоена / повышенный
			Обучающийся ответил на 50-69 % вопросов	Удовлетворите льно	Освоена / базовый
			Обучающийся ответил на 0-49 % вопросов	неудовлетвори тельно	Не освоена / недостаточный
	Вопросы к зачету	Правильнос ть ответов	Обучающийся дал исчерпывающий ответ на вопрос, не допустил ошибок. Студент владеет знаниями и умениями по дисциплине в полном объеме	Отлично	Освоена / повышенный
			Обучающийся дал подробный и полный ответ, допустил не более 1 ошибки. Студент владеет знаниями и умениями по дисциплине в полном объеме	Хорошо	Освоена / повышенный
			Обучающийся дал поверхностный ответ на вопрос, допустил более 2 ошибок	Удовлетворите льно	Освоена / базовый
			Обучающийся не смог правильно ответить на вопрос, допустил ошибку в анализе задания	неудовлетвори тельно	Не освоена / недостаточный
Умеет: выполнять периодический контроль требований по защите персональных данных	Задания для практических работ	Правильнос ть и полнота выполнения задания	Обучающийся правильно выбрал инструменты для решения задачи, систематизировал и наглядно представил полученные данные, сделал развернутые выводы	Отлично	Освоена / повышенный
			Обучающийся правильно выбрал инструменты для	Хорошо	Освоена /

			решения задачи, систематизировал и наглядно представил полученные данные, сделал краткие выводы		повышенный
			Обучающийся правильно выбрал инструменты для решения задачи, но не смог грамотно их применить, выводы отсутствуют	Удовлетворительно	Освоена / базовый
			Обучающийся не смог правильно выбрать инструменты для решения задачи	неудовлетворительно	Не освоена / недостаточный
Владеет: навыками использования инструментальных средств контроля правил защиты персональных данных в информационных системах	Задания для практических работ	Правильность и полнота выполнения задания	Обучающийся разносторонне проанализировал ситуацию, выбрал верную методику решения, сделал развернутые выводы, не допустил ошибок в расчетах	Отлично	Освоена / повышенный
			Обучающийся разносторонне проанализировал ситуацию, полностью выполнил задание, сделал вывод, допустил не более 1 ошибки в расчетах	Хорошо	Освоена / повышенный
			Обучающийся поверхностно проанализировал ситуацию, выполнил задание, сделал вывод, допустил не более 2 ошибок в расчетах	Удовлетворительно	Освоена / базовый
			Обучающийся не смог правильно решить задачу, допустил ошибку в анализе ситуации	неудовлетворительно	Не освоена / недостаточный