МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ РОССИЙСКОЙ ФЕДЕРАЦИИ

ФЕДЕРАЛЬНОЕ ГОСУДАРСТВЕННОЕ БЮДЖЕТНОЕ ОБРАЗОВАТЕЛЬНОЕ УЧРЕЖДЕНИЕ ВЫСШЕГО ОБРАЗОВАНИЯ

«ВОРОНЕЖСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ ИНЖЕНЕРНЫХ ТЕХНОЛОГИЙ»

ДОКУМЕНТ ПОДПИСАН ЭЛЕКТРОННОЙ ПОДПИСЬЮ

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

УТВЕРЖДАЮ

Проректор по учебной работе

_____ ___Василенко В.Н.___
(подпись) (Ф.И.О.)

«25» мая 2023 г.

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ

Управление информационной безопасностью
(наименование в соответствии с РУП)

Направление подготовки (специальность)

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

Направленность (профиль)

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)

Воронеж

1. Цели и задачи дисциплины

1. Целью освоения дисциплины является формирование компетенций обучающегося в области профессиональной деятельности и сфере профессиональной деятельности:

– Связь, информационные и коммуникационные технологии.

Дисциплина направлена на решение задач профессиональной деятельности следующих типов:

– контрольно-аналитического типа.

Программа составлена в соответствии с требованиями Федерального государственного образовательного стандарта высшего образования по специальности высшего образования 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	ИД1 $_{ОПК-6}$ – обладает навыками разработки автоматизированных систем с учетом политики информационной безопасности с использованием современных программных средств
			ИД2$_{опк-6}$ – обладает способностью формирования комплекса мер, правил, процедур и методов для защиты 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

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: об основных уязвимостях и угрозах безопасности информации, моделях угроз и нарушителя в автоматизированных системах, принципах формирования политики информационной безопасности в автоматизированных системах; рисках информационной безопасности в автоматизированных системах; методах и мерах по управлению информационной безопасностью в автоматизированных системах и оценке эффективности принятых мер.
	Умеет: выявлять уязвимости информационно-технологических ресурсов автоматизированных систем; проводить мониторинг угроз безопасности автоматизированных систем; разрабатывать модели угроз и нарушителей информационной безопасности автоматизированных систем; разрабатывать корпоративную и частные политики информационной безопасности автоматизированных систем; оценивать информационные риски в автоматизированных системах; составлять аналитические обзоры по вопросам обеспечения информационной безопасности автоматизированных систем; разрабатывать предложения по совершенствованию системы управления

	информационной безопасностью автоматизированных систем; определять информационную инфраструктуру и информационные ресурсы организации, подлежащие защите; определять комплекс мер (правила, процедуры, практические приемы, руководящие принципы, методы, средства) для обеспечения информационной безопасности автоматизированных систем; контролировать эффективность принятых мер по реализации частных политик информационной безопасности автоматизированных систем.
	Владеет: навыками управления информационной безопасностью автоматизированных систем; разработки политик информационной безопасности, анализа информационной инфраструктуры автоматизированной системы и степени ее текущей безопасности, участия в экспертизе состояния защищенности информации на объекте защиты; методами мониторинга и аудита, выявления угроз информационной безопасности автоматизированных систем; методами оценки информационных рисков; навыками выбора и обоснования критериев эффективности функционирования защищенных автоматизированных информационных систем.
ИД2$_{опк-6}$ – обладает способностью формирования комплекса мер, правил, процедур и методов для защиты 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	Знает: технологический процесс защиты информации ограниченного доступа в соответствии с нормативными правовыми актами и нормативными методическими документами Федеральной службы безопасности Российской Федерации, Федеральной службы по техническому и экспортному контролю.
	Умеет организовывать технологический процесс защиты информации ограниченного доступа в соответствии с нормативными правовыми актами и нормативными методическими документами Федеральной службы безопасности Российской Федерации, Федеральной службы по техническому и экспортному контролю
	Владеет способностью организовывать технологический процесс защиты информации ограниченного доступа в соответствии с нормативными правовыми актами и нормативными методическими документами Федеральной службы безопасности Российской Федерации, Федеральной службы по техническому и экспортному контролю

3. Место дисциплины в структуре ООП ВО/СПО

Дисциплина относится к обязательной части 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 и виды учебной работы

Общая трудоемкость дисциплины составляет _4_ зачетные единицы.

Виды учебной работы	**Всего академических часов**	**Распределение трудоемкости по семестрам**
		4 семестр
		Акад. ч
Общая трудоемкость дисциплины	**144**	**144**
Контактная работа в т. ч. аудиторные занятия:	**73,9**	**73,9**
Лекции	36	36
в том числе в форме практической подготовки	–	–
Практические занятия	36	36

в том числе в форме практической подготовки	-	-
Консультации текущие	0,9	0,9
Вид аттестации (зачет)	1	1
Самостоятельная работа:	**70,1**	**70,1**
Проработка материалов по конспекту лекций	5	5
Проработка материалов по учебнику для подготовки к практическим занятиям	24,1	24,1
Подготовка к коллоквиуму	5	5
Оформление отчетов по практическим работам	36	36

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, ак.ч
1	Основы управления информационной безопасностью.	Основы построения систем обеспечения информационной безопасности на предприятии Деятельность по обеспечению информационной безопасности. Предметная направленность деятельности по обеспечению информационной безопасности. Цель деятельности по обеспечению информационной безопасности. Принципы и форма деятельности по обеспечению информационной безопасности. Методы деятельности по обеспечению информационной безопасности. Средства обеспечения информационной безопасности. Субъекты обеспечения информационной безопасности.	37
2	Управление рисками, инцидентами и аудит информационной безопасности.	Система управления информационной безопасностью бизнеса Модели непрерывного совершенствования и корпоративное управление. Модели непрерывного совершенствования и международные стандарты. Шаги реализации стандартной системы управления информационной безопасностью организации. Модели COSO, COBIT, ITIL. Контроль и аудит. Анализ и оценка управленческих и экономических показателей системы управления информационной безопасностью бизнеса Способы оценки информационной безопасности. Основные элементы процесса оценки информационной безопасности. Способы измерения атрибутов объекта оценки информационной безопасности. Применение типовых моделей оценки на основе оценки процессов и уровней зрелости процессов для оценки информационной безопасности. Модель оценки информационной безопасности на основе оценки процессов. Риск-ориентированная оценка информационной безопасности	34
3	Рискология информационной безопасности	Цель процесса анализа рисков ИБ. Этапы и участники процесса анализа рисков ИБ. Разработка Методики анализа рисков ИБ. Инвентаризация активов. Понятие актива. Типы активов. Источники информации об активах организации. Выбор угроз ИБ и уязвимостей для выделенных на этапе инвентаризации активов. Оценка рисков ИБ. Планирование мер по обработке выявленных рисков ИБ. Утверждение результатов анализа рисков ИБ у высшего руководства. Использование результатов анализа рисков ИБ	33
4	Обеспечение	Российское законодательство, затрагивающее аспекты и	38,1

	соответствия требованиям законодательства РФ	механизмы обеспечения безопасности в рамках СУИБ (авторское право, защита персональных данных и т.д.). Разработка процессов или дополнение существующих процессов управления ИБ с целью удовлетворения этим требованиям (необходимые документы, процессы, в которых данные требования могут быть выполнены)	
	Консультации текущие		0,9
	Зачет		1

5.2 Разделы дисциплины и виды занятий

№ п/п	Наименование раздела дисциплины	Лекции, ак. ч	Практические занятия, ак. ч	СРО, ак. ч
1	Основы управления информационной безопасностью	10*	10*	17
2	Управление рисками, инцидентами и аудит информационной безопасности	8*	8*	18
3	Рискология информационной безопасности	8*	8*	17
4	Обеспечение соответствия требованиям законодательства РФ	10*	10*	18,1
	Консультации текущие	0,9		
	Зачет	1		

5.2.1 Лекции

№ п/п	Наименование раздела дисциплины	Тематика лекционных занятий	Трудоемкость, ак. ч
1	Основы управления информационной безопасностью.	Основы построения систем обеспечения информационной безопасности на предприятии Деятельность по обеспечению информационной безопасности. Предметная направленность деятельности по обеспечению информационной безопасности. Цель деятельности по обеспечению информационной безопасности. Принципы и форма деятельности по обеспечению информационной безопасности. Методы деятельности по обеспечению информационной безопасности. Средства обеспечения информационной безопасности. Субъекты обеспечения информационной безопасности.	10
2	Управление рисками, инцидентами и аудит информационной безопасности.	Система управления информационной безопасностью бизнеса Модели непрерывного совершенствования и корпоративное управление. Модели непрерывного совершенствования и международные стандарты. Шаги реализации стандартной системы управления информационной безопасностью организации. Модели COSO, COBIT, ITIL. Контроль и аудит. Анализ и оценка управленческих и экономических показателей системы управления информационной безопасностью бизнеса Способы оценки информационной безопасности. Основные элементы процесса оценки информационной безопасности. Способы измерения атрибутов объекта оценки информационной безопасности. Применение типовых моделей оценки на основе оценки процессов и уровней зрелости процессов для оценки информационной безопасности. Модель оценки информационной безопасности на основе оценки процессов. Риск-ориентированная оценка информационной безопасности	8
3	Рискология	Цель процесса анализа рисков ИБ. Этапы и участники	8

	информационной безопасности	процесса анализа рисков ИБ. Разработка Методики анализа рисков ИБ. Инвентаризация активов. Понятие актива. Типы активов. Источники информации об активах организации. Выбор угроз ИБ и уязвимостей для выделенных на этапе инвентаризации активов. Оценка рисков ИБ. Планирование мер по обработке выявленных рисков ИБ. Утверждение результатов анализа рисков ИБ у высшего руководства. Использование результатов анализа рисков ИБ	
4	Обеспечение соответствия требованиям законодательства РФ	Российское законодательство, затрагивающее аспекты и механизмы обеспечения безопасности в рамках СУИБ (авторское право, защита персональных данных и т.д.). Разработка процессов или дополнение существующих процессов управления ИБ с целью удовлетворения этим требованиям (необходимые документы, процессы, в которых данные требования могут быть выполнены)	10

5.2.2 Практические занятия (семинары)

№ п/п	Наименование раздела дисциплины	Тематика практических занятий	Трудоемкость, ак. ч
1	Основы управления информационной безопасностью.	Разработка и управление политикой ИБ информационной системы	10
2	Управление рисками, инцидентами и аудит информационной безопасности.	Анализ модели угроз ИБ и уязвимостей. Анализ модели информационных потоков	8
3	Рискология информационной безопасности	Обязательная документация системы управления информационной безопасностью (СУИБ). Процессы улучшения СУИБ («Внутренний аудит», «Корректирующие действия», «Предупреждающие действия»). Процесс «Мониторинг эффективности» (включая разработку метрик эффективности). Понятие «Зрелость процесса». Процесс «Анализ со стороны высшего руководства». Процесс «Обучение и обеспечение осведомленности»	8
4	Обеспечение соответствия требованиям законодательства РФ	Сертификация по ISO/IEC 27001 или ГОСТ Р ИСО/МЭК 27001. Период эксплуатации СУИБ перед сертификацией. Органы по сертификации, работающие в РФ (их различия и требования). Этапы сертификационного аудита. Решение о сертификации	10

5.2.3 Лабораторный практикум

Не предусмотрен.

5.2.4 Самостоятельная работа обучающихся

№ п/п	Наименование раздела дисциплины	Вид СРО	Трудоемкость, ак. ч
1	Основы управления информационной безопасностью.	Подготовка к коллоквиуму	25
2	Обеспечение соответствия требованиям законодательства РФ		
3	Управление рисками, инцидентами и аудит информационной	Подготовка доклада с визуальным представлением презентации	17

	безопасности		
4	Рискология информационной безопасности	Домашнее задание	18,1
	Итого		70,1

6 Учебно-методическое и информационное обеспечение дисциплины

Для освоения дисциплины обучающийся может использовать:

6.1 Основная литература

1. Крутиков, В.Н. Анализ данных : учебное пособие / В.Н. Крутиков, В.В. Мешечкин ; Министерство образования и науки Российской Федерации, Федеральное государственное бюджетное образовательное учреждение высшего профессионального образования «Кемеровский государственный университет». - Кемерово : Кемеровский государственный университет, 2014. - 138 с. : ил. - Библиогр. в кн. - ISBN 978-5-8353-1770-7 ; То же [Электронный ресурс]. - URL: http://biblioclub.ru/index.php?page=book&id=278426
2. Жуковский, О.И. Информационные технологии и анализ данных : учебное пособие / О.И. Жуковский ; Министерство образования и науки Российской Федерации, Томский Государственный Университет Систем Управления и Радиоэлектроники (ТУСУР). - Томск : Эль Контент, 2014. - 130 с. : схем., ил. - Библиогр.: с. 126. - ISBN 978-5-4332-0158-3 ; То же [Электронный ресурс]. - URL: http://biblioclub.ru/index.php?page=book&id=480500
3. Базы данных в высокопроизводительных информационных системах : учебное пособие / авт.- сост. Е.И. Николаев ; Министерство образования и науки РФ, Федеральное государственное автономное образовательное учреждение высшего образования «Северо-Кавказский федеральный университет». - Ставрополь : СКФУ, 2016. - 163 с. : ил. - Библиогр.: с. 161. ; То же [Электронный ресурс]. - URL: http://biblioclub.ru/index.php?page=book&id=466799

6.2 Дополнительная литература

1. Туманов, В.Е. Проектирование хранилищ данных для систем бизнес-аналитики : учебное пособие / В.Е. Туманов. - Москва : Интернет-Университет Информационных Технологий, 2010. - 616 с. : ил., табл., схем. - (Основы информационных технологий). - ISBN 978-5-9963-0353-3 ; То же [Электронный ресурс]. - URL: http://biblioclub.ru/index.php?page=book&id=233492
2. Добронец, Б.С. Численный вероятностный анализ неопределенных данных : монография / Б.С. Добронец, О.А. Попова ; Министерство образования и науки Российской Федерации, Сибирский Федеральный университет. - Красноярск : Сибирский федеральный университет, 2014. - 168 с. : граф., ил. - Библиогр. в кн. - ISBN 978-5-7638-3093-4 ; То же [Электронный ресурс]. - URL: http://biblioclub.ru/index.php?page=book&

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

Наименование ресурса сети «Интернет»	Электронный адрес ресурса
«Российское образование» - федеральный портал	*http://www.edu.ru/index.php*
Научная электронная библиотека	*http://www.elibrary.ru/defaulttx.asp?*
Федеральная университетская компьютерная сеть России	*http://www.runnet.ru/*
Информационная система «Единое окно доступа к образовательным ресурсам»	*http://www.window.edu.ru/*
Электронная библиотека ВГУИТ	*http://biblos.vsuet.ru/megapro/web*
Сайт Министерства науки и высшего образования РФ	*http://minobrnauki.gow.ru*
Портал открытого on-line образования	*http://npoed.ru*
Информационно-коммуникационные технологии в образовании. Система федеральных образовательных порталов	*http://www.ict.edu.ru/*
Электронная образовательная среда ФГБОУ ВО «ВГУИТ	*http://education.vsuet.ru*

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

При изучении дисциплины используется программное обеспечение 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 Unix; Libre 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

Оценочные материалы (ОМ) для дисциплины 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** .

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

ОЦЕНОЧНЫЕ МАТЕРИАЛЫ
ДЛЯ ПРОМЕЖУТОЧНОЙ АТТЕСТАЦИИ

по дисциплине

УПРАВЛЕНИЕ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТЬЮ

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
			ИД2$_{опк-6}$ – обладает способностью формирования комплекса мер, правил, процедур и методов для защиты 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

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: об основных уязвимостях и угрозах безопасности информации, моделях угроз и нарушителя в автоматизированных системах, принципах формирования политики информационной безопасности в автоматизированных системах; рисках информационной безопасности в автоматизированных системах; методах и мерах по управлению информационной безопасностью в автоматизированных системах и оценке эффективности принятых мер.
	Умеет: выявлять уязвимости информационно-технологических ресурсов автоматизированных систем; проводить мониторинг угроз безопасности автоматизированных систем; разрабатывать модели угроз и нарушителей информационной безопасности автоматизированных систем; разрабатывать корпоративную и частные политики информационной безопасности автоматизированных систем; оценивать информационные риски в автоматизированных системах; составлять аналитические обзоры по вопросам обеспечения информационной безопасности автоматизированных систем; разрабатывать предложения по совершенствованию системы управления информационной безопасностью автоматизированных систем; определять информационную инфраструктуру и информационные ресурсы организации, подлежащие защите; определять комплекс мер (правила, процедуры, практические приемы, руководящие принципы, методы, средства) для обеспечения информационной безопасности автоматизированных систем; контролировать эффективность принятых мер по реализации частных политик информационной безопасности автоматизированных систем.
	Владеет: навыками управления информационной безопасностью автоматизированных систем; разработки политик информационной безопасности, анализа информационной инфраструктуры автоматизированной системы и степени ее текущей безопасности, участия в экспертизе состояния защищенности информации на объекте защиты; методами мониторинга и аудита, выявления угроз информационной безопасности автоматизированных систем; методами оценки информационных рисков; навыками выбора и обоснования

	критериев эффективности функционирования защищенных автоматизированных информационных систем.
ИД2$_{опк-6}$ – обладает способностью формирования комплекса мер, правил, процедур и методов для защиты 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	Знает: технологический процесс защиты информации ограниченного доступа в соответствии с нормативными правовыми актами и нормативными методическими документами Федеральной службы безопасности Российской Федерации, Федеральной службы по техническому и экспортному контролю.
	Умеет организовывать технологический процесс защиты информации ограниченного доступа в соответствии с нормативными правовыми актами и нормативными методическими документами Федеральной службы безопасности Российской Федерации, Федеральной службы по техническому и экспортному контролю
	Владеет способностью организовывать технологический процесс защиты информации ограниченного доступа в соответствии с нормативными правовыми актами и нормативными методическими документами Федеральной службы безопасности Российской Федерации, Федеральной службы по техническому и экспортному контролю

2 Паспорт оценочных материалов по дисциплине

№ п/п	Разделы дисциплины	Индекс контролируемой компетенции (или ее части)	Оценочные материалы		Технология/процедура оценивания (способ контроля)
			наименование	№№ заданий	
1	Основы управления информационной безопасностью	ОПК-6	Банк тестовых заданий	1-25	Бланочное или компьютерное тестирование
2	Управление рисками, инцидентами и аудит информационной безопасности.		Кейс-задача	26-29	Защита практической работы
3	Рискология информационной безопасности		Вопросы к зачету	30-45	Проверка преподавателем
4	Обеспечение соответствия требованиям законодательства РФ				

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 тестирования и предусматривает возможность последующего собеседования (зачета).

Каждый вариант теста включает 25 контрольных заданий, из них:

- 8 контрольных заданий на проверку знаний;
- 8 контрольных заданий на проверку умений;
- 9 контрольных заданий на проверку навыков.

3.1 Тесты (тестовые задания к зачету)

3.1.1 ***Шифр и наименование 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

№ задания	Тестовое задание с вариантами ответов и правильными ответами
1.	Соблюдение каких правил входит в защиту правомочий обладателя информации? (1) Соблюдение конфиденциальности информации — свойства информационной технологии (ИТ) обеспечивать раскрытие информации только в соответствии с правилами разграничения доступа (право распоряжения); (2) Соблюдение целостности информации — свойства ИТ обеспечивать предоставление права модификации (уничтожения) информации только в соответствии с правилами разграничения доступа, а также обеспечивать неизменность информации в условиях случайных ошибок или стихийных бедствий (право владения); (3) Соблюдение доступности информации — свойства ИТ обеспечивать свободный доступ к информации по мере возникновения необходимости (право пользования); **(4) Соблюдение всех перечисленных правил.**
2.	Какая из перечисленных видов тайн относится к категории конфиденциальной информации? **(1) государственная тайна, персональные данные, коммерческая тайна, служебная тайна.** (2) персональная данные, коммерческая тайна, служебная тайна. (3) государственная тайна, коммерческая тайна, служебная тайна
3.	В соответствии с Федеральным законом от 27 июля 2006 г. N 149-ФЗ"Об информации, информационных технологиях и о защите информации" информация – это: **(1) сведения (сообщения, данные) независимо от формы их представления;** (2) зафиксированная на материальном носителе информация с реквизитами, позволяющими ее идентифицировать; (3) сведения о фактах, событиях и обстоятельствах жизни гражданина, позволяющие идентифицировать его личность.
4.	Каковы задачи государственной системы обеспечения информационной безопасности? (1) выявление и прогнозирование дестабилизирующих факторов и информационных угроз жизненно важным интересам личности, общества и государства; (2) осуществление комплекса оперативных и долговременных мер по предупреждению и устранению дестабилизирующих факторов и информационных угроз; (3) создание и поддержание в готовности сил и средств обеспечения информационной безопасности и другие задачи; **(4) все перечисленные выше.**

5.	Дайте определение государственной системы защиты информации. **(1) 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;** (2) Государственная система защиты информации - совокупность федеральных и иных органов управления, выполняющие функции по защите информации; (3) Государственная система защиты информации – совокупность правовых, организационных и технических мер по реализации функций обеспечения информационной безопасности
6.	Перечислите основные группы информационных ресурсов государства. **(1) открытая, запатентованная и закрытая информация;** (2) информация особой важности, совершенно секретная, секретная информация, для служебного пользования, открытая информация; (3) защищаемая информация и информация свободного доступа.
7.	Каким нормативно-правовым документом регулируются отношения, связанные со сведениями, содержащими государственную тайну? (1) Федеральный закон от 27 июля 2006 г. N 149-ФЗ"Об информации, информационных технологиях и о защите информации" **(2) Закон РФ «О государственной тайне» от 21 июля 1993 г. (в ред. Федерального закона от 06.10.97 N 131-ФЗ);** (3) Закон РФ «О безопасности» от 5 марта 1992 г. № 2446-I
8.	Что такое гриф секретности? **(1) реквизиты, свидетельствующие о степени секретности сведений, содержащихся в их носителе, проставляемые на самом носителе и (или) в сопроводительной документации на него;** (2) процедура оформления права граждан на доступ к сведениям, составляющим государственную тайну, а предприятий, учреждений и организаций - на проведение работ с использованием таких сведений; (3) совокупность категорий сведений, в соответствии с которыми сведения относятся к государственной тайне и засекречиваются на основаниях и в порядке, установленных федеральным законодательством
9.	Какова структура системы лицензирования? (1) государственный орган по лицензированию и Центральная лицензионная комиссия при нем, региональные (отраслевые) лицензионные центры и экспертные комиссии при них; **(2) государственный орган по лицензированию и Центральная лицензионная комиссия при нем, региональные (отраслевые) лицензионные центры и экспертные комиссии при них, предприятия, претендующие на получение лицензий в выбранном виде деятельности, и предприятия-потребители услуг в области защиты информации;** (3) лицензионные центры и экспертные комиссии при них, предприятия, претендующие на получение лицензий в выбранном виде деятельности.
10.	Что является объектом системы сертификации: (1) вид деятельности; (2) помещения; **(3) средства защиты информации.**
11.	Какой правовой документ представляет собой совокупность официальных взглядов на цели, задачи, принципы и основные направления обеспечения информационной безопасности Российской Федерации? **(1) Доктрина информационной безопасности Российской Федерации 09.09.2000 г.;** (2) Концепция национальной безопасности Российской Федерации от 17.09.2000 г.; (3) Закон РФ «О безопасности» от 5 марта 1992 г. № 2446-I

12.	Что такое информационная безопасность? **(1) состояние защищенности ее национальных интересов в информационной сфере, определяющихся совокупностью сбалансированных интересов личности, общества и государства**. (2) 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. (3) создание условий для гармоничного развития российской информационной инфраструктуры
13.	К правовым методам обеспечения информационной безопасности Российской Федерации относится: **(1) законодательное разграничение полномочий в области обеспечения информационной безопасности Российской Федерации между федеральными органами государственной вла-сти и органами государственной власти субъектов Российской Федерации, определение це-лей, задач и механизмов участия в этой деятельности общественных объединений, организаций и граждан;** (2) разработка, использование и совершенствование средств защиты информации и методов контроля эффективности этих средств, развитие защищенных телекоммуникационных систем, повышение надежности специального программного обеспечения; (3) совершенствование системы финансирования работ, связанных с реализацией правовых и организационно-технических методов защиты информации, создание системы страхования информационных рисков физических и юридических лиц.
14.	К организационно-техническим методам обеспечения информационной безопасности Российской Федерации относится: (1) разработка программ обеспечения информационной безопасности Российской Федерации и определение порядка их финансирования; **(2) 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;** (3) создание правовой базы для формирования в Российской Федерации региональных структур обеспечения информационной безопасности.
15.	К экономическим методам обеспечения информационной безопасности Российской Федерации относится: (1) внесение изменений и дополнений в законодательство Российской Федерации, регулирующее отношения в области обеспечения информационной безопасности; **(2) совершенствование системы финансирования работ, связанных с реализацией правовых и организационно-технических методов защиты информации, создание системы страхования информационных рисков физических и юридических лиц;** (3) 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.
16.	Что из перечисленного ниже является первым этапом организации комплексной защиты информации? (1) категорирование объектов информации; **(2) изучение руководящих документов;** (3) издание приказов по оборудованию комплексной защиты информации; (4) проведение защитных мероприятий.
17.	Сколько этапов составляют действия по подготовке и проведению комплексных специальных проверок выделенных помещений? (1) 6 этапов; **(2) 3 этапа;** (3) 4 этапа.

18.	Какие из перечисленных мероприятий относятся к подготовительному этапу специальных проверок выделенных помещений? **(1) визуальный осмотр ограждающих конструкций, мебели и других предметов интерьера помещений;** (2) составление акта проведения спецпроверки; (3) разработка легенды прикрытия проведения спецпроверки.
19.	Что является объектом преступлений, предусмотренных главой 28 УК РФ. **(1) общественные отношения в сфере обеспечения информационной безопасности;** (2) общественные отношения собственности; (3) в сфере поддержания основ государственного строя и безопасности государства
20.	Что является общественно опасными последствиями при совершении деяния, предусмотренного ст. 272 УК РФ «Неправомерный доступ к компьютерной информации»? (1) неправомерный доступ к охраняемой законом информации; **(2) уничтожение, блокирование, модификация, копирование информации, нарушение работы ЭВМ, системы ЭВМ или их сети;** (3) создание программ для ЭВМ или внесение изменений в существующие программы.
21.	Что является общественно опасными деяниями при совершении преступления, предусмотренного ст. 273 УК РФ «Создание, использование и распространение вредоносных программ для ЭВМ»? (1) создание программ для ЭВМ, заведомо приводящих к несанкционированному уничтожению, блокированию, модификации, копированию информации, нарушению работы ЭВМ, системы ЭВМ или их сети; (2) внесение изменений в существующие программы, заведомо приводящих к несанкционированному уничтожению, блокированию, модификации, копированию информации, нарушению работы ЭВМ, системы ЭВМ или их сети; (3) использование либо распространение программ для ЭВМ, заведомо приводящих к несанкционированному уничтожению, блокированию, модификации, копированию информации, нарушению работы ЭВМ, системы ЭВМ или их сети; **(4) все перечисленные выше действия.**
22.	Каким нормативным правовым документов регулируются вопросы защиты интеллектуальной собственности в сфере информационной безопасности? (1) Федеральный закон от 27 июля 2006 г. N 149-ФЗ"Об информации, информационных технологиях и о защите информации" **(2) Гражданский кодекс Российской Федерации (часть четвертая) 18.12.2006 №230-ФЗ;** (3) Закон Российской Федерации от 23 сентября 1992 г. N 3523-1 "О правовой охране программ для электронных вычислительных машин и баз данных"
23.	Какая информация в соответствии с Федеральным законом от 29 июля 2004 г. N 98-ФЗ "О коммерческой тайне" не может быть отнесена к сведениям, составляющим коммерческую тайну? **(1) сведения, содержащиеся в учредительных документах юридического лица, документах, подтверждающих факт внесения записей о юридических лицах и об индивидуальных предпринимателях в соответствующие государственные реестры;** (2) Информация об условиях сотрудничества (порядок, форма оплаты, предоставляемые скидки, условия доставки и т. д.) с действительными и потенциальными контрагентами; (3) 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.
24.	В соответствии с Федеральным законом от 27 июля 2006 г. № 152-ФЗ «О персональных данных» под персональными данными понимается: **(1) любая информация, относящаяся к определенному или определяемому на основании та-кой информации физическому лицу (субъекту персональных данных), в том числе его фами-лия, имя, отчество, год, месяц, дата и место рождения, адрес, семейное, социальное, иму-щественное положение, образование, профессия, доходы, другая информация** (2) зафиксированная на материальном носителе информация о личности с реквизитами, поз-воляющими ее идентифицировать; (3) сведения, касающиеся личности, собранные органом власти в процессе реализации установленных для него полномочий, в отношении которых действует требование конфиденциальности.

25.	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»? (1) ФСТЭК **(2) РОСКОМНАДЗОР** (3) ФСБ (4) ФСО (5) МВД

3.2 Кейс-задания

3.2.1 ***Шифр и наименование 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

№ задания	Текст задания
26	Управление непрерывностью деятельности: основные понятия, цели и задачи процесса, роль процесса в рамках СУИБ.
27	Российское законодательство, затрагивающее аспекты и механизмы обеспечения безопасности в рамках СУИБ, обеспечение соответствия требованиям законодательства
28	Процессы улучшения системы управления ИБ: основные процессы, из взаимосвязь и роль в рамках СУИБ.

29	Организация защиты государственной тайны.

3.3 Зачет (собеседование)

3.3.1 ***Шифр и наименование 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

№ задания	Тестовое задание с вариантами ответов и правильными ответами
30	Процессный подход к построению СУИБ и циклическая модель PDCA.
31	Цели и задачи, решаемые СУИБ.
32	Стандартизация в области построения СУИБ: сходства и различия стандартов.
33	Стратегии выбора области деятельности СУИБ.
34	Стратегии построения СУИБ (построение системы в целом, построение отдельных процессов управления ИБ с последующим объединением в систему).
35	Основные этапы разработки СУИБ и роль руководства организации на каждом из этапов.
36	Политика ИБ и политика СУИБ: сходства и различия.
37	Распределение ролей и ответственности в рамках СУИБ: базовая ролевая структура, дополнительные роли в рамках процессов управления ИБ.
38	Анализ рисков ИБ: основные понятия, цели и задачи процесса, роль процесса в рамках СУИБ.
39	Анализ рисков ИБ: основные подходы, основные этапы процесса.
40	Управление инцидентами ИБ: основные понятия, цели и задачи процесса, роль процесса в рамках СУИБ.
41	Расследование инцидентов ИБ: виды расследования инцидентов, критерии выбора необходимого вида расследования, основные этапы расследования (для различных видов расследования).
42	Угрозы информации в ЭВМ.
43	Анализ со стороны руководства: основные понятия, цели и задачи процесса, роль процесса в рамках СУИБ.
44	Методы и средства ограничения доступа.
45	Процессный подход к построению СУИБ и циклическая модель PDCA.

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, а также методическими указаниями.

Итоговая оценка по дисциплине определяется на основании определения средневзвешенному 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/практике

Результаты обучения по этапам формирования компетенций	Предмет оценки (продукт или процесс)	Показатель оценивания	Критерии оценивания сформированности компетенций	Шкала оценивания	
				Академическая оценка или баллы	Уровень освоения компетенции
Шифр и наименование 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					
ЗНАТЬ: об основных уязвимостях и угрозах безопасности информации, моделях угроз и нарушителя в автоматизированных системах, принципах формирования политики информационной безопасности в автоматизированных системах; рисках информационной безопасности в автоматизированных системах; методах и мерах по управлению информационной безопасностью в автоматизированных системах и оценке эффективности принятых мер	Собеседование (зачет)	Уровень знаний	50% и более правильных ответов	Зачтено	Освоена (базовый, повышенный)
			менее 50% правильных ответов	Не зачтено	Не освоена (недостаточный)
УМЕТЬ: выявлять уязвимости информационно-технологических ресурсов автоматизированных систем; проводить мониторинг угроз безопасности автоматизированных систем; разрабатывать	Тест (тестовые задания к зачету)	Умение применять полученные знания	85% и более правильных ответов	Отлично	Освоена (повышенный)
			75-84% правильных ответов	Хорошо	Освоена (повышенный)
			65-74% правильных ответов	Удовлетворительно	Освоена (базовый)
			Менее 64% правильных ответов	Неудовлетворительно	Не освоена (недостаточный)

модели угроз и нарушителей информационной безопасности автоматизированных систем; разрабатывать корпоративную и частные политики информационной безопасности автоматизированных систем; оценивать информационные риски в автоматизированных системах; составлять аналитические обзоры по вопросам обеспечения информационной безопасности автоматизированных систем; разрабатывать предложения по совершенствованию системы управления информационной безопасностью автоматизированных систем; определять информационную инфраструктуру и информационные ресурсы организации, подлежащие защите; определять комплекс мер (правила, процедуры, практические приемы, руководящие принципы, методы, средства) для обеспечения информационной безопасности автоматизированных					

систем; контролировать эффективность принятых мер по реализации частных политик информационной безопасности автоматизированных систем					
ВЛАДЕТЬ: навыками управления информационной безопасностью автоматизированных систем; разработки политик информационной безопасности, анализа информационной инфраструктуры автоматизированной системы и степени ее текущей безопасности, участия в экспертизе состояния защищенности информации на объекте защиты; методами мониторинга и аудита, выявления угроз информационной безопасности автоматизированных систем; методами оценки информационных рисков; навыками выбора и обоснования критериев эффективности функционирования защищенных автоматизированных информационных систем	Кейс-задание	Методика и правильность решения задачи	Обучающийся выполнил кейс задание	Зачтено	Освоена (базовый, повышенный)
			Обучающийся не выполнил кейс задание	Не зачтено	Не освоена (недостаточный)