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

Информационная безопасность в условиях цифровой экономики

(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 «Информационная безопасность в условиях цифровой экономики» является формирование компетенций обучающегося в области профессиональной деятельности и сфере профессиональной деятельности:

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

Дисциплина направлена на решение задач профессиональной деятельности проектного типа.

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

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

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

№ п/п	Код компетенции	Наименование компетенции	Код и наименование индикатора достижения компетенции
1	ПКв-3	способен разрабатывать эксплуатационную документацию на системы защиты информации автоматизированных систем, формировать требования по защите информации, анализировать защищённость информационной инфраструктуры автоматизированной системы.	ИД1 $_{ПКв-3}$ обладает способностью разрабатывать научно-техническую документацию, готовить научно-технические отчеты, обзоры, публикации по результатам выполненных работ

Код и наименование индикатора достижения компетенции	Результаты обучения (показатели оценивания)
ИД1 $_{ПКв-3}$ обладает способностью разрабатывать научно-техническую документацию, готовить научно-технические отчеты, обзоры, публикации по результатам выполненных работ	Знает: как разрабатывать научно-техническую документацию, готовить научно-технические отчеты, обзоры, публикации по результатам выполненных работ
	Умеет: разрабатывать научно-техническую документацию, готовить научно-технические отчеты, обзоры, публикации по результатам выполненных работ
	Владеет: навыками разработки научно-технической документацию, готовить научно-технические отчеты, обзоры, публикации по результатам выполненных работ

3. Место дисциплины в структуре ОП ВО

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

Изучение дисциплины основано на знаниях, умениях и навыках, полученных при изучении обучающимися дисциплин:

– Гуманитарные аспекты информационной безопасности;
– Производственная практика, преддипломная практика;
– Производственная практика, эксплуатационная практика.

Дисциплина является предшествующей для следующих дисциплин видов практик:

– Технологии разработки защищенного документооборота;
– Надежность и защищенность программного обеспечения.

4. Объем дисциплины и виды учебных занятий

Общая трудоемкость дисциплины составляет 2 зачетных единиц.

Виды учебной работы	Всего ак.ч	Распределение трудоемкости по семестрам, ак.ч
		А семестр
Общая трудоемкость дисциплины	**72**	**72**
Контактная работа, в т.ч. аудиторные занятия::	**37**	**37**
Лекции	18	18
в том числе в форме практической подготовки	–	–
Практические занятия (ПЗ)	18	18
в том числе в форме практической подготовки	18	18
Консультации текущие	0,9	0,9
Вид аттестации (зачет, экзамен)	0,1	0,1
Самостоятельная работа:	**35**	**35**
Изучение материалов по учебникам (собеседование, тестирование, решение кейс-заданий)	12	12
Изучение материалов, изложенных в лекциях (собеседование, тестирование, решение кейс-заданий)	10	10
Подготовка к защите по практическим занятиям и лабораторным работам (собеседование)	13	13

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

5.1 Содержание разделов дисциплины

№ п/п	Наименование разделов дисциплины	Содержание раздела	Трудоемкость раздела, ак.ч
1	Нормативные документы в области ИБ в условиях цифровой экономики. Сквозные технологии цифровой экономики.	Важность и актуальность дисциплины. Ее взаимосвязь с другими дисциплинами специальностях в условиях цифровой экономики. Содержание дисциплины. Виды контроля знаний. Принципы, подходы и виды управления. Цели и задачи управления ИБ. Понятие системы управления. Понятие ИБ. Место ИБ в рамках общей системы управления предприятием. Законодательные и нормативно-правовые акты Российской Федерации по защите информации. Структура, задачи и основные функции Государственной системы защиты информации.	16
2	Структура и задачи органов обеспечивающих ИБ. Нормативное регулирование вопросов безопасности информационных технологий цифровой экономики.	Органы обеспечения информационной безопасности. Сертификация. Период эксплуатации СУИБ перед сертификацией. Органы по сертификации, работающие в РФ (их различия и требования). Этапы сертификационного аудита. Решение о сертификации	19
3	Организационно-технические и режимные меры и методы. Современное состояние средств защиты технологий цифровой экономики в информационных	Методология проверки и оценки состояния информационной безопасности (защиты информации (данных) и ресурсов ИС). Ввод системы в эксплуатацию. Возможные проблемы и способы их решения. Внешние аудиты ИБ на соответствие требованиям нормативных документов. Этапы проведения аудита ИБ. Результаты аудита ИБ и их интерпретация	19

	системах и технологиях управления бизне-процессами.		
4	ИБ: конфиденциальность, целостность, доступность	Определения и сущность конфиденциальности, целостности, доступности – неотъемлемых составляющих информационной безопасности	17

5.2 Разделы дисциплины и виды занятий

№ п/п	Наименование раздела дисциплины	Лекции, час	Практические занятия, ак. ч	СР, час
1	Нормативные документы в области ИБ в условиях цифровой экономики. Сквозные технологии цифровой экономики.	4	4	8
2	Структура и задачи органов обеспечивающих ИБ. Нормативное регулирование вопросов безопасности информационных технологий цифровой экономики.	4	5	10
3	Организационно-технические и режимные меры и методы. Современное состояние средств защиты технологий цифровой экономики в информационных системах и технологиях управления бизне-процессами.	4	5	10
4	ИБ: конфиденциальность, целостность, доступность	6	4	7
	Зачет, экзамен	0,1		

5.2.1 Лекции

№ п/п	Наименование раздела дисциплины	Тематика лекционных занятий	Трудоемкость, Час
1	Нормативные документы в области ИБ в условиях цифровой экономики. Сквозные технологии цифровой экономики.	Важность и актуальность дисциплины. Ее взаимосвязь с другими дисциплинами специальности в условиях цифровой экономики. Содержание дисциплины. Виды контроля знаний. Принципы, подходы и виды управления. Цели и задачи управления ИБ. Понятие системы управления. Понятие ИБ. Место ИБ в рамках общей системы управления предприятием. Законодательные и нормативно-правовые акты Российской Федерации по защите информации. Структура, задачи и основные функции Государственной системы защиты информации.	4
2	Структура и задачи органов обеспечивающих ИБ. Нормативное регулирование вопросов безопасности информационных технологий цифровой экономики.	Органы обеспечения информационной безопасности. Сертификация. Период эксплуатации СУИБ перед сертификацией. Органы по сертификации, работающие в РФ (их различия и требования). Этапы сертификационного аудита. Решение о сертификации	5
3	Организационно-технические и режимные меры и методы. Современное состояние средств защиты технологий цифровой экономики в информационных системах и технологиях управления бизне-процессами.	Методология проверки и оценки состояния информационной безопасности (защиты информации (данных) и ресурсов ИС). Ввод системы в эксплуатацию. Возможные проблемы и способы их решения. Внешние аудиты ИБ на соответствие требованиям нормативных документов. Этапы проведения аудита ИБ. Результаты аудита ИБ и их интерпретация	5
4	ИБ: конфиденциальность, целостность, доступность	Определения и сущность конфиденциальности, целостности, доступности – неотъемлемых составляющих информационной безопасности	4

	Итого		18

5.2.2 Практические занятия

№ п/п	Наименование раздела дисциплины	Тематика практических занятий	Трудоемкость, час
1	Нормативные документы в области ИБ в условиях цифровой экономики. Сквозные технологии цифровой экономики.	Существующие стандарты и методологии по управлению ИБ: их отличия, сильные и слабые стороны (на примере семейства стандартов ISO/IEC 2700x, СТО БР ИББС-1.0, ГОСТ Р ИСО/МЭК 17799, ГОСТ Р ИСО/МЭК 27001, ISO/IEC 18044, ISO/IEC 25999 и др.). Мировые тенденции развития сквозных цифровых технологий	4
2	Структура и задачи органов обеспечивающих ИБ. Нормативное регулирование вопросов безопасности информационных технологий цифровой экономики.	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». Вопросы информационной безопасности программы «Цифровая экономика РФ»	5
3	Организационно-технические и режимные меры и методы. Современное состояние средств защиты технологий цифровой экономики в информационных системах и технологиях управления бизне-процессами.	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. Анализ состояния средств защиты информационных технологий цифровой экономики.	5
4	ИБ: конфиденциальность, целостность, доступность	Документирование процесса внедрения разработанных процессов. Типовой документ «Положение о применимости». Цель документа. Структура и содержание документа. Процесс разработки документа, решение спорных ситуаций при разработке документа	4
	Итого		18*

5.2.3 Самостоятельная работа обучающихся (СРО)

№	Наименование раздела	Вид СРО	Трудоемкость,

п/п	дисциплины		час
1	Нормативные документы в области ИБ в условиях цифровой экономики. Сквозные технологии цифровой экономики.	Подготовка доклада	8
2	Структура и задачи органов обеспечивающих ИБ. Нормативное регулирование вопросов безопасности информационных технологий цифровой экономики.		10
3	Организационно-технические и режимные меры и методы. Современное состояние средств защиты технологий цифровой экономики в информационных системах и технологиях управления бизне-процессами.	Домашнее задание	10
4	ИБ: конфиденциальность, целостность, доступность		7
	Итого		35

6Учебно-методическое и информационное обеспечение дисциплины

Для освоения дисциплины обучающийся может использовать:

6. 1. Основная литература

1. Возможности Visual Studio 2013 и их использование для облачных вычислений. Сафонов В. О. Национальный Открытый Университет «ИНТУИТ» 2016. – 380 с. http://www.knigafund.ru/books/177984

2 Гухман В.Б. Информационная цивилизация [Электронный ресурс]: учебное пособие. — Москва; Берлин: Директ-Медиа, 2018. — 247 с. — Режим доступа: http://biblioclub.ru/index.php?page=book&id=493598.

3. Малюк, А.А. Защита информации в информационном обществе [Электронный ресурс]: учебное пособие / А.А. Малюк. — Электрон. дан. — Москва: Горячая линия-Телеком, 2017. — 230 с. — Режим доступа: https://e.lanbook.com/book/111078.

4 Загинайлов Ю.Н. Теория информационной безопасности и методология защиты информации [Электронный ресурс]: учебное пособие / Ю.Н. Загинайлов. — Москва; Берлин: Директ-Медиа, 2015. — 253 с. — Режим доступа: http://biblioclub.ru/index.php?page=book&id=276557.

5. Компьютерные сети. Фомин Д. В. Директ-Медиа, 2015. – 66 с. http://www.knigafund.ru/books/185091

6. Развитие платформы облачных вычислений Microsoft Windows Azure. Сафонов В. О. Национальный Открытый Университет «ИНТУИТ», 2016. – 393 с. http://www.knigafund.ru/books/175954

7. Облачные вычисления в образовании. Соснин В. В. Национальный Открытый Университет «ИНТУИТ», 2016. – 110 с. http://www.knigafund.ru/books/176370

8. Введение в облачные вычисления и технологии. Губарев В. В., Савульчик С. А., Чистяков Н. А. НГТУ, 2014. – 48 с. http://www.knigafund.ru/books/186408

6.2. Дополнительная литература

1. Анализ и оценка типовых топологий вычислительных сетей. Соколов Р. С. Лаборатория книги, 2014. – 55 с. http://www.knigafund.ru/books/189024

2. Организация сети передачи голоса по IP протоколу на базе распределенной локальной вычислительной сети АГУ. Лебедев Я. Н. Лаборатория книги, 2015. – 107 с. http://www.knigafund.ru/books/194834

3. Аппаратные и программные решения для беспроводных сенсорных сетей. Калачев А. Национальный Открытый Университет «ИНТУИТ», 2016. – 241 с. http://www.knigafund.ru/books/176978

4. Теория вычислительных процессов. Кузнецов А. С., Царев Р. Ю., Князьков А. Н. Сибирский федеральный университет, 2015. – 184 с. http://www.knigafund.ru/books/184651

5. Администрирование сетей на платформе MS Windows Server. Власов Ю. В., Рицкова Т. И. Интернет-Университет Информационных Технологий, 2016. – 384 с. http://www.knigafund.ru/books/178113

6. Системы защиты информации в ведущих зарубежных странах [Электронный ресурс]: учебное пособие для вузов / В.И. Аверченков, М.Ю. Рытов, Г.В. Кондрашин, М.В. Руданов-ский.— 4-е изд., стер. — Москва: Издательство «Флинта», 2016. — 224 с. — Режим доступа: http://biblioclub.ru/index.php?page=book&id=93351.

7. Царегородцев А.В. Методы и средства защиты информации в государственном управлении [Электронный ресурс]: учебное пособие / А.В. Царегородцев, М.М. Тараскин. — Москва: Проспект, 2017. — 205 с. — Режим доступа : http://biblioclub.ru/index.php?page=book&id=468250.

8. Бекетнова Ю.М. Международные основы и стандарты информационной безопасности финансово-экономических систем [Электронный ресурс]: учебное пособие / Ю.М. Бекетнова, Г.О. Крылов, С.Л. Ларионова; Финансовый университет при Правительстве Российской Федерации. — Москва: Прометей, 2018. — 173 с. — Режим доступа : http://biblioclub.ru/index.php?page=book&id=494850.

6.3 Перечень учебно-методического обеспечения для самостоятельной работы обучающихся

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

Безопасность облачных и распределенных вычислений [Электронный ресурс]: методические указания для самостоятельной работы для студентов, обучающихся по направлению 10.05.03– «Информационная безопасность автоматизированных систем», очной формы обучения / А. В. Скрыпников, Е. В. Чернышова ; ВГУИТ, Кафедра информационной безопасности. - Воронеж : ВГУИТ, 2016. - 29 с. http://biblos.vsuet.ru/ProtectedView/Book/ViewBook/1520

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

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

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

Microsoft Office Professional Plus 2010; Microsoft Windows 7; VMWare Player.

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

Информационная безопасность в условиях цифровой экономики

1 Перечень компетенций с указанием этапов их формирования

№ п/п	Код компетенции	Формулировка компетенции	Код и наименование индикатора достижения компетенции
1	ПКв-3	Способен разрабатывать эксплуатационную документацию на системы защиты информации автоматизированных систем, формировать требования по защите информации, анализировать защищённость информационной инфраструктуры автоматизированной системы.	ИД1 $_{ПКв-3}$ обладает способностью разрабатывать научно-техническую документацию, готовить научно-технические отчеты, обзоры, публикации по результатам выполненных работ

Код и наименование индикатора достижения компетенции	**Результаты обучения (показатели оценивания)**
ИД1$_{ПКв-3}$ обладает способностью разрабатывать научно-техническую документацию, готовить научно-технические отчеты, обзоры, публикации по результатам выполненных работ	Знает как разрабатывать научно-техническую документацию, готовить научно-технические отчеты, обзоры, публикации по результатам выполненных работ
	Умеет разрабатывать научно-техническую документацию, готовить научно-технические отчеты, обзоры, публикации по результатам выполненных работ
	Владеет навыками разработки научно-технической документацию, готовить научно-технические отчеты, обзоры, публикации по результатам выполненных работ

2 Паспорт фонда оценочных средств по дисциплине

№ п/п	Разделы дисциплины	Индекс контролируемой компетенции (или ее части)	Оценочные средства		Технология/процедура оценивания (способ контроля)
			наименование	№№ заданий	
1	Цифровые технологии: информационная безопасность в условиях цифровой экономики	ПКв-3	Тест	1-7	Компьютерное тестирование Процентная шкала. 0-100 %; 0-59,99% - неудовлетворительно; 60-74,99% - удовлетворительно; 75- 84,99% -хорошо; 85-100% - отлично.
			Собеседование (вопросы для зачета)	32-35	Проверка преподавателем Отметка в системе «зачтено – не зачтено»
			Собеседование (вопросы к защите практических работ)	50-52	Компьютерное тестирование Процентная шкала. 0-100 %; 0-59,99% - неудовлетворительно; 60-74,99% - удовлетворительно; 75- 84,99% -хорошо; 85-100% - отлично.
			Домашнее задание, реферат	58-62	Проверка преподавателем Отметка в системе «зачтено – не зачтено»
	Биометрические технологии и тендеции их разви-	ПКв-3	Тест	8-16	Компьютерное тестирование Процентная шкала. 0-100 %; 0-59,99% - неудовлетворительно; 60-74,99% - удовлетворительно;

	тия				75- 84,99% -хорошо; 85-100% - отлично.
			Собеседование (вопросы для зачета)	36-39	Проверка преподавателем Отметка в системе «зачтено – не зачтено»
			Собеседование (вопросы к защите практических работ)	53-54	Компьютерное тестирование Процентная шкала. 0-100 %; 0-59,99% - неудовлетворительно; 60-74,99% - удовлетворительно; 75- 84,99% -хорошо; 85-100% - отлично.
			Домашнее задание, реферат	63-67	Проверка преподавателем Отметка в системе «зачтено – не зачтено»
	Особенности электронной цифровой подписи как элемент ИБ.	ПКв-3	Тест	17-26	Компьютерное тестирование Процентная шкала. 0-100 %; 0-59,99% - неудовлетворительно; 60-74,99% - удовлетворительно; 75- 84,99% -хорошо; 85-100% - отлично.
			Собеседование (вопросы для зачета)	40-44	Проверка преподавателем Отметка в системе «зачтено – не зачтено»
			Собеседование (вопросы к защите практических работ)	55-56	Компьютерное тестирование Процентная шкала. 0-100 %; 0-59,99% - неудовлетворительно; 60-74,99% - удовлетворительно; 75- 84,99% -хорошо; 85-100% - отлично.
			Домашнее задание, реферат	68-71	Проверка преподавателем Отметка в системе «зачтено – не зачтено»
	Направление информационная безопасность в программе цифровая экономика.	ПКв-3	Тест	27-31	Компьютерное тестирование Процентная шкала. 0-100 %; 0-59,99% - неудовлетворительно; 60-74,99% - удовлетворительно; 75- 84,99% -хорошо; 85-100% - отлично.
			Собеседование (вопросы для зачета)	45-49	Проверка преподавателем Отметка в системе «зачтено – не зачтено»
			Собеседование (вопросы к защите практических работ)	57-59	Компьютерное тестирование Процентная шкала. 0-100 %; 0-59,99% - неудовлетворительно; 60-74,99% - удовлетворительно; 75- 84,99% -хорошо; 85-100% - отлично.
			Домашнее задание, реферат	72-75	Проверка преподавателем Отметка в системе «зачтено – не зачтено»

3 Оценочные материалы для промежуточной аттестации.

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

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

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

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

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

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

Каждый вариант теста включает 15 контрольных заданий, из них:

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

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

3.1 Тесты *(тестовые задания)*

3.1.1 Шифр и наименование компетенции

ПКв-3 Способен разрабатывать эксплуатационную документацию на системы защиты информации автоматизированных систем, формировать требования по защите информации, анализировать защищённость информационной инфраструктуры автоматизированной системы.

№ задания	Тестовое задание
1.	Рисками цифровизации экономики являются: 1. Нарушения прав человека в цифровом мире, в том числе в части сохранности личных данных; **2. Сопутствующие риски, появление которых обусловлено изменением на основе цифровизации существующих ранее технологий, а также совершенствованием действовавших ранее и созданием новых бизнес-моделей;** 3. Наращивания возможностей внешнего информационно-технического воздействия; **4. Несовершенства, неподготовленности нормативно-правовой базы, обеспечивающей протекание процессов цифровизации;** 5. Роста масштабов компьютерной преступности; 6. Отставания от ведущих иностранных государств;

	7. Злоупотребления технологиями и новыми возможностями, связанными с цифровизацией, с несанкционированным использованием чужой информации и ресурсов;
2.	Перечислите стратегии развития цифровой реальности Ответ: 1. Создании единого информационного реестра всех ресурсов в цифровой экономике; 2. Создание и внедрение технологии учета всех процессов, которые приводят к тем или иным изменениям этих ресурсов; 3. Обеспечить наполнение и оперативное обновление единого реестра ресурсов актуальными, достоверными и объективными исходными данными.
3.	Угрозами цифровизации экономики являются: **1. Нарушения прав человека в цифровом мире, в том числе в части сохранности личных данных;** 2. Сопутствующие риски, появление которых обусловлено изменением на основе цифровизации существующих ранее технологий, а также совершенствованием действовавших ранее и созданием новых бизнес-моделей; **3. Наращивания возможностей внешнего информационно-технического воздействия;** 4. Несовершенства, неподготовленности нормативно-правовой базы, обеспечивающей протекание процессов цифровизации; **5. Роста масштабов компьютерной преступности;** **6. Отставания от ведущих иностранных государств;** 7. Злоупотребления технологиями и новыми возможностями, связанными с цифровизацией, с несанкционированным использованием чужой информации и ресурсов;
4.	Перечислите два основных вида кибервойн: **Ответ: оперативные и стратегические.**
5.	Как расшифровывается сокращение «сквот», часто встречающееся в материалах и публикациях по программе «Цифровая экономика»: 1) виртуальное сообщество киберсквоттеров, регистрирующих на себя популярные интернет-домены цифровых сервисов; 2) среднеквадратичное отклонение показателей цифровой экономики от показателей традиционной экономики; **3) сквозная технология;** 4) виртуальная реальность;
6.	По данным аналитических компаний SAS и Deloitte, основными трудностями развития искусственного интеллекта являются: 1. **изменение перечня профессий и востребованных человеческих навыков;** **2. нормативно-правовые риски;** 3. нехватку поддержки со стороны руководства; **4. этические вопросы**. 5. неясное экономическое обоснование;
7.	Перечислите основные барьеры внедрения и использования искусственного интеллекта. **Ответ: нехватка поддержки со стороны руководства; неясное экономическое обоснование**.
8.	Перечислите два типа систем биометрических данных: **Ответ: статические биометрические данные; динамические биометрические данные.**
9.	Расположите в порядке распространённости биометрические системы которые активно применяются на мировом рынке технологии, основанные на распознавании и использовании следующих биометрических данных: 1. изображение лица; 2. отпечатки пальцев; 3. голос; 4. изображение радужной оболочки глаза; 5. рисунок вен; 6. геометрия ладони, ДНК и иное; **Ответ: 1- отпечатки пальцев; 2- изображение лица; 3- изображение радужной оболочки глаза; 4- геометрия ладони, ДНК и иное; 5- голос; 6- рисунок вен;**
10.	Из каких этапов идентификация с использованием любых типов биометрических данных состоит: **1. запись;** **2. выделение биометрического образца;** **3. сравнение;** **4. получение результата;** 5. обработка результатов;
11.	Первоочередным фактором развития биометрических технологий в мире являются:

	Ответ: инициативы государств, направленные на обеспечение национальной безопасности
12.	Из всех моделей многофакторной аутентификации наиболее распространенной (и традиционной) является: **Ответ: двухфакторная аутентификация**
13.	Направления использования биометрических технологий
14.	Существуют следующие направления использования биометрических технологий в финансовой сфере: 1. банкоматы и терминалы самообслуживания (далее – АТМ); 2. совершение покупок с помощью биометрических технологий; 3. дистанционное обслуживание; 4. корпоративное использование биометрических технологий; Выберите правильный вариант ответа: 1) 1,2; 2) 2,3; 3) 3,4; **4) 1,2,3,4;**
15.	Дактилоскопическая информация, полученная в результате проведения государственной дактилоскопической регистрации, используется для: 1. розыска пропавших без вести граждан Российской Федерации, иностранных граждан и лиц без гражданства; 2. установления по неопознанным трупам личности человека; 3. установления личности граждан Российской Федерации, иностранных граждан и лиц без гражданства, не способных по состоянию здоровья или возрасту сообщить данные о своей личности;4. подтверждения личности граждан Российской Федерации, иностранных граждан и лиц без гражданства (миграционный учет); Выберите правильный вариант ответа: 1) 1,2; 2) 2,3; 3) 3,4; **4) 1,2,3,4;**
16.	Механизм удаленной идентификации предусматривает 2 этапа: **Ответ: Регистрация физического лица в ЕСИА и Единой биометрической системе; Удаленная идентификация.**
17.	Электронная цифровая подпись — 1) **реквизит электронного документа, предназначенный для защиты данного электронного документа от подделки, полученный в результате криптографического преобразования информации с использованием закрытого ключа электронной цифровой подписи и позволяющий идентифицировать владельца сертификата ключа подписи, а также установить отсутствие искажения информации в электронном документе;** 2) аппаратные и (или) программные средства, обеспечивающие реализацию хотя бы одной из следующих функций — создание электронной цифровой подписи в электронном документе с использованием закрытого ключа электронной цифровой подписи, подтверждение с использованием открытого ключа электронной цифровой подписи подлинности электронной цифровой подписи в электронном документе, создание закрытых и открытых ключей электронных цифровых подписей; 3) документ на бумажном носителе, выданный в соответствии с правилами системы сертификации для подтверждения соответствия средств электронной цифровой подписи установленным требованиям; 4) документ на бумажном носителе или электронный документ с электронной цифровой подписью уполномоченного лица удостоверяющего центра, которые включают в себя открытый ключ электронной цифровой подписи и которые выдаются удостоверяющим центром участнику информационной системы для подтверждения подлинности электронной цифровой подписи и идентификации владельца сертификата ключа подписи;
18.	Средства электронной цифровой подписи — 1) реквизит электронного документа, предназначенный для защиты данного электронного документа от подделки, полученный в результате криптографического преобразования информации с использованием закрытого ключа электронной цифровой подписи и позволяющий идентифицировать владельца сертификата ключа подписи, а также установить отсутствие искажения информации в электронном документе; **2) аппаратные и (или) программные средства, обеспечивающие реализацию хотя бы одной из следующих функций — создание электронной цифровой подписи в электронном документе с использованием закрытого ключа электронной цифровой подписи, подтверждение с использованием открытого ключа электронной цифровой подписи подлинности электронной цифровой подписи в электронном документе, создание закрытых и открытых ключей электронных цифровых подписей;**

	3) документ на бумажном носителе, выданный в соответствии с правилами системы сертификации для подтверждения соответствия средств электронной цифровой подписи установленным требованиям; 4) документ на бумажном носителе или электронный документ с электронной цифровой подписью уполномоченного лица удостоверяющего центра, которые включают в себя открытый ключ электронной цифровой подписи и которые выдаются удостоверяющим центром участнику информационной системы для подтверждения подлинности электронной цифровой подписи и идентификации владельца сертификата ключа подписи;
19.	Сертификат средств электронной цифровой подписи — 1) реквизит электронного документа, предназначенный для защиты данного электронного документа от подделки, полученный в результате криптографического преобразования информации с использованием закрытого ключа электронной цифровой подписи и позволяющий идентифицировать владельца сертификата ключа подписи, а также установить отсутствие искажения информации в электронном документе; 2) аппаратные и (или) программные средства, обеспечивающие реализацию хотя бы одной из следующих функций — создание электронной цифровой подписи в электронном документе с использованием закрытого ключа электронной цифровой подписи, подтверждение с использованием открытого ключа электронной цифровой подписи подлинности электронной цифровой подписи в электронном документе, создание закрытых и открытых ключей электронных цифровых подписей; **3) документ на бумажном носителе, выданный в соответствии с правилами системы сертификации для подтверждения соответствия средств электронной цифровой подписи установленным требованиям;** 4) документ на бумажном носителе или электронный документ с электронной цифровой подписью уполномоченного лица удостоверяющего центра, которые включают в себя открытый ключ электронной цифровой подписи и которые выдаются удостоверяющим центром участнику информационной системы для подтверждения подлинности электронной цифровой подписи и идентификации владельца сертификата ключа подписи;
20.	Сертификат ключа подписи — 1) реквизит электронного документа, предназначенный для защиты данного электронного документа от подделки, полученный в результате криптографического преобразования информации с использованием закрытого ключа электронной цифровой подписи и позволяющий идентифицировать владельца сертификата ключа подписи, а также установить отсутствие искажения информации в электронном документе; 2) аппаратные и (или) программные средства, обеспечивающие реализацию хотя бы одной из следующих функций — создание электронной цифровой подписи в электронном документе с использованием закрытого ключа электронной цифровой подписи, подтверждение с использованием открытого ключа электронной цифровой подписи подлинности электронной цифровой подписи в электронном документе, создание закрытых и открытых ключей электронных цифровых подписей; 3) документ на бумажном носителе, выданный в соответствии с правилами системы сертификации для подтверждения соответствия средств электронной цифровой подписи установленным требованиям; **4) документ на бумажном носителе или электронный документ с электронной цифровой подписью уполномоченного лица удостоверяющего центра, которые включают в себя открытый ключ электронной цифровой подписи и которые выдаются удостоверяющим центром участнику информационной системы для подтверждения подлинности электронной цифровой подписи и идентификации владельца сертификата ключа подписи;**
21.	Закрытый ключ электронной цифровой подписи — 1) реквизит электронного документа, предназначенный для защиты данного электронного документа от подделки, полученный в результате криптографического преобразования информации с использованием закрытого ключа электронной цифровой подписи и позволяющий идентифицировать владельца сертификата ключа подписи, а также установить отсутствие искажения информации в электронном документе; **2) уникальная последовательность символов, известная владельцу сертификата ключа подписи и предназначенная для создания в электронных документах электронной цифровой подписи с использованием средств электронной цифровой подписи;** 3) документ на бумажном носителе, выданный в соответствии с правилами системы сертификации для подтверждения соответствия средств электронной цифровой подписи установленным требованиям; 4) документ на бумажном носителе или электронный документ с электронной цифровой подписью уполномоченного лица удостоверяющего центра, которые включают в себя открытый ключ

	электронной цифровой подписи и которые выдаются удостоверяющим центром участнику информационной системы для подтверждения подлинности электронной цифровой подписи и идентификации владельца сертификата ключа подписи;
22.	Владелец сертификата ключа подписи — 1) реквизит электронного документа, предназначенный для защиты данного электронного документа от подделки, полученный в результате криптографического преобразования информации с использованием закрытого ключа электронной цифровой подписи и позволяющий идентифицировать владельца сертификата ключа подписи, а также установить отсутствие искажения информации в электронном документе; **2) физическое лицо, на имя которого удостоверяющим центром выдан сертификат ключа подписи и которое владеет соответствующим закрытым ключом электронной цифровой подписи, позволяющим с помощью средств электронной цифровой подписи создавать свою электронную цифровую подпись в электронных документах (подписывать электронные документы);** 3) физическое лицо, использующее полученные в удостоверяющем центре сведения о сертификате ключа подписи для проверки принадлежности электронной цифровой подписи владельцу сертификата ключа подписи; 4) документ на бумажном носителе или электронный документ с электронной цифровой подписью уполномоченного лица удостоверяющего центра, которые включают в себя открытый ключ электронной цифровой подписи и которые выдаются удостоверяющим центром участнику информационной системы для подтверждения подлинности электронной цифровой подписи и идентификации владельца сертификата ключа подписи;
23.	Пользователь сертификата ключа подписи — 1) реквизит электронного документа, предназначенный для защиты данного электронного документа от подделки, полученный в результате криптографического преобразования информации с использованием закрытого ключа электронной цифровой подписи и позволяющий идентифицировать владельца сертификата ключа подписи, а также установить отсутствие искажения информации в электронном документе; 2) физическое лицо, на имя которого удостоверяющим центром выдан сертификат ключа подписи и которое владеет соответствующим закрытым ключом электронной цифровой подписи, позволяющим с помощью средств электронной цифровой подписи создавать свою электронную цифровую подпись в электронных документах (подписывать электронные документы); **3) физическое лицо, использующее полученные в удостоверяющем центре сведения о сертификате ключа подписи для проверки принадлежности электронной цифровой подписи владельцу сертификата ключа подписи;** 4) документ на бумажном носителе или электронный документ с электронной цифровой подписью уполномоченного лица удостоверяющего центра, которые включают в себя открытый ключ электронной цифровой подписи и которые выдаются удостоверяющим центром участнику информационной системы для подтверждения подлинности электронной цифровой подписи и идентификации владельца сертификата ключа подписи;;
24.	Симметричный ключ — 1) реквизит электронного документа, предназначенный для защиты данного электронного документа от подделки, полученный в результате криптографического преобразования информации с использованием закрытого ключа электронной цифровой подписи и позволяющий идентифицировать владельца сертификата ключа подписи, а также установить отсутствие искажения информации в электронном документе; **2) кодирование и раскодирование документа производится одинаково. Этим ключом владеет определенная группа людей, доверяющих друг другу и несущих единую, равную ответственность за сохранность ключа;** 3) документ на бумажном носителе, выданный в соответствии с правилами системы сертификации для подтверждения соответствия средств электронной цифровой подписи установленным требованиям; 4) данные шифруются одним ключом, а расшифровываются другим. Клиент обладает ключом для расшифровки;
25.	Несимметричный ключ — 1) реквизит электронного документа, предназначенный для защиты данного электронного документа от подделки, полученный в результате криптографического преобразования информации с использованием закрытого ключа электронной цифровой подписи и позволяющий идентифицировать владельца сертификата ключа подписи, а также установить отсутствие искажения информации в электронном документе; 2) кодирование и раскодирование документа производится одинаково. Этим ключом владеет определенная группа людей, доверяющих друг другу и несущих единую, равную ответствен-

	ность за сохранность ключа; 3) документ на бумажном носителе, выданный в соответствии с правилами системы сертификации для подтверждения соответствия средств электронной цифровой подписи установленным требованиям; 4) **данные шифруются одним ключом, а расшифровываются другим. Клиент обладает ключом для расшифровки;**
26.	В числе способов обеспечения сохранности секретных ключей можно назвать следующие: **1) хранение на носителях, которые трудно копируются, например специальные чип - карты, доступ к которым имеет лишь владелец ключа, знающий PIN-код;** **2) использование методов, позволяющих с очень высокой степенью достоверности обеспечить привязку электронно-цифровой подписи к подписанту (примером может служить технология цифровой обработки папиллярного узора отпечатка пальца, радужной оболочки глаза, автографа и других биометрических параметров);** **3) шифрование секретных ключей на других ключах, которые могут быть тоже зашифрованы;** 4) подтверждение подлинности электронно-цифровой подписи в электронном документе;
27.	Перечислите угрозы информационной безопасности в условиях цифровой экономики **1. Киберпреступления (например, проникновение злоумышленников в информационные системы банков);** **2. Текущий уровень технологической зависимости РФ от других государств, так как по-прежнему широко используются зарубежные средства защиты информации;** **3. Множество коммерческих структур (отечественных и зарубежных) на внутреннем рынке России, которые являются источниками и потребителями информации. Угроза состоит в том, что деятельность этих структур в сфере создания и защиты систем сбора, обработки, хранения и передачи информации слабо контролируется и высока вероятность несанкционированного доступа к конфиденциальной экономической информации;** **4. Хищение информации, содержащей коммерческую тайну (что может нанести экономический ущерб предприятиям, вне зависимости от их формы собственности), а также противоправное копирование информации и ее искажение (вследствие случайных или преднамеренных нарушений технологии работы с информацией);** 5. Недостаточное регулирование правовых отношений в сфере полномочий на использование СМИ среди различных политических сил (речь идет об использовании СМИ для пропаганды идей); 6. Распространение дезинформации о политике РФ, событиях внутри страны и деятельности федеральных органов госвласти;
28.	Какие используются меры по обеспечению защиты информационной безопасности России: **1. Разработка и внедрение национальных защищенных систем электронных денег, электронных платежей, электронной торговли;** **2. Разработка сертифицированных национальных средств защиты информации, внедрение этих средств в системы сбора, хранения, обработки и передачи экономической информации;** **3. Улучшение методов отбора и подготовки персонала для работы с системами сбора, хранения, обработки и передачи экономической информации.** **4. Госконтроль за созданием, развитием и защитой систем сбора, хранения, обработки и передачи экономической информации (речь идет о финансовой, статистической, биржевой, таможенной, налоговой информации);** **5. Перестройка системы госотчетности с целью обеспечения достоверности, полноты и защищенности информации;** **6. Совершенствование нормативной правовой базы, которая регулирует информационные отношения в сегменте экономики;** 7. Создание системы, которая будет противодействовать монополизации сегментов информационной инфраструктуры отечественными и зарубежными субъектами (речь идет в том числе о СМИ и рынке инфоуслуг); 8. Контрпропагандистская деятельность против дезинформации о внутренней политике РФ, целью которой является предотвращение негативных последствий дезинформации;
29.	К наиболее серьезным угрозам информационной безопасности внутренней политики относят: **1. Нарушение конституционных прав и свобод граждан РФ (например, нарушение неприкосновенности частной жизни, нарушение тайны переписки);** **2. Распространение дезинформации о политике РФ, событиях внутри страны и деятельности федеральных органов госвласти;** **3. Распространение дезинформации о событиях, которые происходят за рубежом;**

	4. Деятельность общественных объединений, пропагандирующих разжигание вражды (на расовой, социальной, национальной, религиозной и других почвах), а также продвигающих идеи нарушения целостности РФ, насильственного изменения основ конституционного строя; **5. Недостаточное регулирование правовых отношений в сфере полномочий на использование СМИ среди различных политических сил (речь идет об использовании СМИ для пропаганды идей).** 6. Киберпреступления (например, проникновение злоумышленников в информационные системы банков); 7. Хищение информации, содержащей коммерческую тайну (что может нанести экономический ущерб предприятиям, вне зависимости от их формы собственности), а также противоправное копирование информации и ее искажение (вследствие случайных или преднамеренных нарушений технологии работы с информацией);
30.	Какие используются мероприятия для обеспечения инфобезопасности РФ в сфере внутренней политики? **1. Создание системы, которая будет противодействовать монополизации сегментов информационной инфраструктуры отечественными и зарубежными субъектами (речь идет в том числе о СМИ и рынке инфоуслуг);** **2. Контрпропагандистская деятельность против дезинформации о внутренней политике РФ, целью которой является предотвращение негативных последствий дезинформации;** 3. Распространение дезинформации о политике РФ, событиях внутри страны и деятельности федеральных органов госвласти; 4. Распространение дезинформации о событиях, которые происходят за рубежом;
31.	Какие меры использует государство для обеспечения технологической независимости и безопасности функционирования инфраструктуры обработки данных? **1. Поддержка производителей отечественных средств защиты информации, например, таких как универсальный шлюз безопасности Traffic Inspector Next Generation.** **2. Законодательное ограничение приобретения иностранного программного обеспечения государственными учреждениями и использование преимущественно российского программного обеспечения;** 3. Распространение дезинформации о политике РФ, событиях внутри страны и деятельности федеральных органов госвласти; 4. Распространение дезинформации о событиях, которые происходят за рубежом;

Критерии и шкалы оценки:

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

«неудовлетворительно, удовлетворительно, хорошо, отлично»

0-59,99% - неудовлетворительно;

60-74,99% - удовлетворительно;

75- 84,99% -хорошо;

85-100% - отлично.

3.2 Собеседование (вопросы к устному ответу для зачета)

3.2.1 Шифр и наименование компетенции

ПКв-3- Способен разрабатывать эксплуатационную документацию на системы защиты информации автоматизированных систем, формировать требования по защите информации, анализировать защищённость информационной инфраструктуры автоматизированной системы.

32	Цифровая грамотность
33	Цифровые технлогии в образовании: ожидания и реальность
34	Преодоление цифрового неравенства
35	Цифровые технологии и новые культурные информационные технологии
36	Внешние и внутренние факторы информатизации образования
37	Изменение представлений о месте цифровых технологий в образовании
38	Биометрические технологии и тенденции их развития
39	Применение биометрических технологий в экономике
40	Международный опыт внедрения биометрических технологий в различных секторах
41	Использование биометрических технологий в России

42	Организационное обеспечена цифровой подписи
43	Особенности электронной цифровой подписи
44	Область применения цифровой подписи
45	Электронная подпись как элемент информационной безопасности
46	Основные положение федерального проекта ИБ
47	Цели и показатели федерального проекта ИБ
48	Задачи и результаты федерального проекта ИБ
49	Финансовое обеспечение реализации федерального проекта ИБ

Критерии и шкалы оценки:

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

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

3.3 Собеседование (вопросы к защите практических работ)

3.3.1 Шифр и наименование компетенции

ПКв-3- Способен разрабатывать эксплуатационную документацию на системы защиты информации автоматизированных систем, формировать требования по защите информации, анализировать защищённость информационной инфраструктуры автоматизированной системы.

№ задания	Формулировка вопроса
50.	Какие факторы сдерживают развитие технологий big data?
51.	Назовите отрасли промышленности – лидеры в области использования технологий промышленного интернета.
52.	Организационная основа системы обеспечения информационной безопасности РФ.
53.	Каким образом технологии виртуальной и дополненной реальности могут быть использованы в информационных системах цифровой экономики?
54.	Какие стандарты обеспечения информационной безопасности имеют отношение к цифровой экономике?
55.	Сравните полученные результаты с мировыми тенденциями.
56.	Структура организационной деятельности в сфере ИБ на предприятии.
57.	Определение целей управления ИБ.

Процентная шкала 0-100 %;

85-100% - отлично (практическое задание выполнено в установленный срок с использованием рекомендаций преподавателя; показан высокий уровень знания изученного материала по заданной теме, проявлен творческий подход, умение глубоко анализировать проблему и делать обобщающие практико-ориентированные выводы; работа выполнена без ошибок и недочетов или допущено не более одного недочета);

75- 84,99% - хорошо (практическое задание выполнено в установленный срок с использованием рекомендаций преподавателя; показан хороший уровень владения изученным материалом по заданной теме, работа выполнена полностью, но допущено в ней: а) не более одной негрубой ошибки и одного недочета; б) или не более двух недочетов);

60-74,99% - удовлетворительно (практическое задание выполнено в установленный срок с частичным использованием рекомендаций преподавателя; продемонстрированы минимальные знания по основным темам изученного материала; выполнено не менее половины работы или допущены в ней а) не более двух грубых ошибок, б) не более одной грубой ошибки и одного недочета, в) не более двух-трех негрубых ошибок, г) одна негрубая ошибка и три недочета, д) при отсутствии ошибок, 4-5 недочетов);

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

3.4. Домашнее задание, реферат

ПКв-3- способен разрабатывать эксплуатационную документацию на системы защиты информации автоматизированных систем, формировать требования по защите информации, анализировать защищённость информационной инфраструктуры автоматизированной системы.

№ задания	Формулировка задания
58.	Введение в дисциплину ЦТ в экономике и образовании
59.	Цели, задачи, содержание дисциплины.
60.	Цифровая грамотность
61.	Цифровые технологии в образовании: ожидания и реальность
62.	Преодоление цифрового неравенства
63.	Индустриальная революция, цифровая трансформация и образование
64.	Развитие цифровой инфраструктуры образования
65.	Биометрические технологии как механизм обеспечения ИБ в цифровой экономике
66.	Порядок размещения и обновления биометрических персональных данных в единой биометрической системе
67.	Требования к ИТ и техническим средствам предназначенным для обработки биометрических персональных данных в целях проведения идентификации
68.	Перспективы биометрической идентификации в контексте цифровой экономики РФ
69.	Направление информационная безопасность в программе цифровая экономика
70.	Основные положение федерального проекта ИБ
71.	Цели и показатели федерального проекта ИБ
72.	Задачи и результаты федерального проекта ИБ
73.	Финансовое обеспечение реализации федерального проекта ИБ
74.	Участники федерального проекта ИБ
75.	Модель функционирования результатов и достижения показателей федерального проекта ИБ

Критерии и шкалы оценки:

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

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

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

Процедуры оценивания в ходе изучения дисциплины знаний, умений и навыков, характеризующих этапы формирования компетенций, регламентируются положениями:

- П ВГУИТ 2.4.03 Положение о курсовых экзаменах и зачетах;
- П ВГУИТ 4.1.02 Положение о рейтинговой оценке текущей успеваемости.

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

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

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

Результаты обучения по этапам формирования компетенций	Предмет оценки (продукт или процесс)	Показатель оценивания	Критерии оценивания сформированности компетенций	Шкала оценивания	
				Академическая оценка или баллы	Уровень освоения компетенции
ПКв-3- способен разрабатывать эксплуатационную документацию на системы защиты информации автоматизированных систем, формировать требования по защите информации, анализировать защищённость информационной инфраструктуры автоматизированной системы.					
ЗНАЕТ	Знает методы разработки научно-технической документации и разработку научно-технических отчетов и публикаций	Изложение основных методик разработки научно-технической документации и разработку научно-технических отчетов и публикаций	Изложены основные методики разработки научно-технической документации и разработка научно-технических отчетов и публикаций	Зачтено/ 60-100; Удовлетворительно /60-74,9	Освоена (базовый)
				Хорошо/75-84,9; Отлично/85-100.	Освоена (повышенный)
			Не изложены основные методики разработки научно-технической документации и не разработаны научно-технические отчеты и публикации	Не зачтено / 0-59,99	Не освоена (недостаточный)
УМЕТЬ	Защита практических работ (собеседование), решение тестовых заданий	Применять методики разработки научно-технической документации, готовить научно-технические отчеты, обзоры, публикации по результатам выполненных работ	Самостоятельно разрабатывать научно-техническую документацию, готовить научно-технические отчеты, а также обзоры, публикации по результатам выполненных работ	Зачтено/ 60-100; Удовлетворительно /60-74,99;	Освоена (базовый)
				Хорошо/75-84,99; Отлично/85-100.	Освоена (повышенный)
			Не правильно разрабатывать научно-техническую документацию, готовить научно-технические отчеты, а также обзоры, публикации по результатам выполненных работ	Не зачтено/ 0-59,99	Не освоена (недостаточный)
ВЛАДЕТЬ	Домашнее задание	Демонстрировать навыки разработки научно-технической документацию, готовить научно-технические отчеты, обзоры, публикации по ре-	Приведена демонстрация навыков разработки научно-технической документацию, готовить научно-технические отчеты, обзоры, публикации по результатам выполненных работ	Зачтено/ 60-100	Освоена (повышенный)

		зультатам выполненных работ	Не приедена демонстрация навыков разработки научно-технической документацию, готовить научно-технические отчеты, обзоры, публикации по результатам выполненных работ	Не зачтено/ 0-59,99	Не освоена (недостаточный)