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

Комплексная оценка уязвимости компьютерных систем

(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	ПКв-2	способен разрабатывать проектные решения по защите информации в автоматизированных системах, модели угроз безопасности информации и модели нарушителя в автоматизированных системах, проекты нормативных документов, регламентирующих работу по защите информации	ИД1 $_{ПКв-2}$ обладает способностью создания проектных решений по защите информации в автоматизированных системах
			ИД2 $_{ПКв-2}$ обладает способностью моделирования различных угроз безопасности информации в автоматизированных системах
			ИД-3$_{ПКв-2}$ обладает способностью разработки проектов нормативных документов, регламентирующих работу по защите информации

Код и наименование индикатора достижения компетенции	Результаты обучения (показатели оценивания)
ИД1 $_{ПКв-2}$ обладает способностью создания проектных решений по защите информации в автоматизированных системах	Знает: базовые понятия современных методов оценки безопасности компьютерных систем; проблемы обеспечения безопасности информации, решаемые с применением современных методов и средств защиты информации защиты информации в компьютерных системах;
	Умеет: выявлять угрозы и определять их актуальность для современных компьютерных систем; описывать (моделировать) объекты защиты и угрозы безопасности компьютерных систем;
	Владеет: практическими навыками применения методов обеспечения безопасности компьютерных систем; навыками применения современных методов оценки безопасности компьютерных систем
ИД2 $_{ПКв-2}$ обладает способностью моделирования различных угроз безопасности информации в автоматизированных системах	Знает: принципы и способы использования существующих средств защиты информации в компьютерных системах; принципы применения современных методов оценки безопасности компьютерных систем
	Умеет: применять наиболее эффективные методы обеспечения безопасности компьютерных систем; применять современные методы оценки безопасности компьютерных систем

	Владеет: навыками применения современных методов оценки безопасности компьютерных систем и моделирования различных угроз безопасности информации в автоматизированных системах
ИД-З$_{ПКв-2}$ обладает способностью разработки проектов нормативных документов, регламентирующих работу по защите информации	Знает: понятия методов оценки безопасности, нормативно-правовые акты в области защиты информации
	Умеет: Разрабатывать проекты нормативных документов, регламентирующих работу по защите информации
	Владеет: навыками оценки защищенности автоматизированных систем критически важных объектов с помощью типовых программных средств; навыками оценки защищенности объектов информатизации с помощью типовых программных средств

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 акаде-мических часов**	**Распределение трудоемкости по семестрам,** Акад. ч
		Семестр А
Общая трудоемкость дисциплины	**144**	**144**
Контактная работа в т. ч. аудиторные занятия:	**75,4**	**75,4**
Лекции	36	36
в том числе в форме практической подготовки	–	–
Практические занятия	36	36
в том числе в форме практической подготовки	36	36
Консультации текущие	2,4	2,4
Вид аттестации (зачет)	1	1
Самостоятельная работа:	**68,6**	**68,6**
Подготовка курсовой работы	**28**	**28**
Проработка материалов по конспекту лекций	5	5
Проработка материалов по учебнику для подготовки к практическим занятиям	12,6	12,6
Подготовка к коллоквиуму	5	5
Оформление отчетов по практическим работам	18	18

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	Общие вопросы оценки безопасности компьютерных	Введение. Предметная область оценки безопасности компьютерных систем. Исторические сведения и этапы развития оценки безопасности компьютерных систем. Математические основы оценки безопасности компьютерных систем.	47

	систем		
2	Методы и средства оценки безопасности компьютерных систем	Анализ рисков в области защиты информации. Международная практика защиты информации. Национальные особенности защиты информации. Постановка задачи анализа рисков. Методы, использующие оценку рисков на качественном уровне. Методы, использующие оценку рисков на количественном уровне. Методы, использующие смешанную оценку рисков. Управление рисками и международные стандарты. Технологии анализа рисков. Инструментальные средства анализа рисков. Аудит безопасности и анализ рисков. Анализ защищенности компьютерной системы. Учет возможностей обнаружения атак и управления рисками в компьютерных системах для оценки безопасности компьютерных систем.	47
3	Организация оценки безопасности компьютерных систем	Организация службы информационной безопасности. Формирование экспертных систем оценки безопасности компьютерных систем. Жизненный цикл компьютерных систем. Модель угроз и принципы обеспечения безопасности компьютерных систем. Политика безопасности. Оценка рисков и ущербов комплексной безопасности компьютерных систем.	46,6
	Консультации текущие		2,4
	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	Общие вопросы оценки безопасности компьютерных систем	12*	12*	23
2	Методы и средства оценки безопасности компьютерных систем	12*	12*	23
3	Организация комплексной оценки безопасности компьютерных систем	12*	12*	22,6
	Консультации текущие	2,4		
	Зачет	1		

*****в форме практической подготовки

5.2.1 Лекции

№ п/п	Наименование раздела дисциплины	Тематика лекционных занятий	Трудоемкость, ак. ч
1	Общие вопросы оценки безопасности компьютерных систем	Введение. Предметная область оценки безопасности компьютерных систем. Исторические сведения и этапы развития оценки безопасности компьютерных систем.	12*
2	Методы и средства оценки безопасности компьютерных систем	Анализ рисков в области защиты информации. Международная практика защиты информации. Национальные особенности защиты информации. Управление рисками и международные стандарты. Технологии анализа рисков.	12*
3	Организация оценки безопасности компьютерныхсистем	Организация службы информационной безопасности. Жизненный цикл компьютерных систем. Политика безопасности. Оценка рисков и ущербов безопасности компьютерных систем	12*

5.2.2 Практические занятия (семинары)

№ п/п	Наименование раздела дисциплины	Тематика практических занятий (семинаров)	Трудоемкость, ак. ч
1	Общие вопросы оценки безопасности	Математические основы оценки безопасности компьютерных систем. Специализированное ПО.	12

	компьютерных систем		
2	Методы и средства оценки безопасности компьютерных систем	Постановка задачи анализа рисков. Методы, использующие оценку рисков на качественном уровне. Методы, использующие оценку рисков на количественном уровне. Методы, использующие смешанную оценку рисков. Инструментальные средства анализа рисков. Аудит безопасности и анализ рисков. Анализ защищенности компьютерной системы.	12
3	Организация оценки безопасности компьютерныхсистем	Модель угроз и принципы обеспечения безопасности компьютерных систем. Политика безопасности на практике. Практическая оценка рисков и ущербов безопасности компьютерных систем	12

5.2.3 Лабораторный практикум

Не предусмотрен.

5.2.4 Самостоятельная работа обучающихся

№ п/п	Наименование раздела дисциплины	Вид СРО	Трудоемкость, ак. ч
1	Общие вопросы оценки безопасности компьютерных систем Методы и средства оценки безопасности компьютерных систем Общие вопросы оценки безопасности компьютерных систем	Подготовка к коллоквиуму Подготовка курсовой работы	23
2	Методы и средства оценки безопасности компьютерных систем Общие вопросы оценки безопасности компьютерных систем Методы и средства оценки безопасности компьютерных систем	Подготовка доклада с визуальным представлением презентации Подготовка курсовой работы	23
3	Организация оценки безопасности компьютерныхсистем	Домашнее задание Подготовка курсовой работы	22,6
	Итого		68,6

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

КОМПЛЕКСНАЯ ОЦЕНКА УЯЗВИМОСТИ КОМПЬЮТЕРНЫХ СИСТЕМ

1 Перечень компетенций с указанием этапов их формирования

№ п/п	Код компетенции	Формулировка компетенции	Код и наименование индикатора достижения компетенции
1	ПКв-2	способен разрабатывать проектные решения по защите информации в автоматизированных системах, модели угроз безопасности информации и модели нарушителя в автоматизированных системах, проекты нормативных документов, регламентирующих работу по защите информации	ИД1 $_{ПКв-2}$ обладает способностью создания проектных решений по защите информации в автоматизированных системах
			ИД2 $_{ПКв-2}$ обладает способностью моделирования различных угроз безопасности информации в автоматизированных системах
			ИД-3$_{ПКв-2}$ обладает способностью разработки проектов нормативных документов, регламентирующих работу по защите информации

Код и наименование индикатора достижения компетенции	Результаты обучения (показатели оценивания)
ИД1 $_{ПКв-2}$ обладает способностью создания проектных решений по защите информации в автоматизированных системах	Знает: базовые понятия современных методов оценки безопасности компьютерных систем; проблемы обеспечения безопасности информации, решаемые с применением современных методов и средств защиты информации защиты информации в компьютерных системах;
	Умеет: выявлять угрозы и определять их актуальность для современных компьютерных систем; описывать (моделировать) объекты защиты и угрозы безопасности компьютерных систем;
	Владеет: практическими навыками применения методов обеспечения безопасности компьютерных систем; навыками применения современных методов оценки безопасности компьютерных систем
ИД2 $_{ПКв-2}$ обладает способностью моделирования различных угроз безопасности информации в автоматизированных системах	Знает: принципы и способы использования существующих средств защиты информации в компьютерных системах; принципы применения современных методов оценки безопасности компьютерных систем
	Умеет: применять наиболее эффективные методы обеспечения безопасности компьютерных систем; применять современные методы оценки безопасности компьютерных систем
	Владеет: навыками применения современных методов оценки безопасности компьютерных систем и моделирования различных угроз безопасности информации в автоматизированных системах
ИД-3$_{ПКв-2}$ обладает способностью разработки проектов нормативных документов, регламентирующих работу по защите информации	Знает: понятия методов оценки безопасности, нормативно-правовые акты в области защиты информации
	Умеет: Разрабатывать проекты нормативных документов, регламентирующих работу по защите информации
	Владеет: навыками оценки защищенности автоматизированных систем критически важных объектов с помощью типовых программных средств; навыками оценки защищенности объектов информатизации с помощью типовых программных средств

2 Паспорт оценочных материалов по дисциплине

№ п/п	Разделы дисциплины	Индекс контролируемой компетенци	Оценочные материалы		Технология/процедура оценивания (способ контроля)
			наименование	№№ заданий	

		и (или ее части)			
1	Общие вопросы оценки безопасности компьютерных систем	ПКв-2	Тестовые задания	1-15	Бланочное или компьютерное тестирование
			Проработка материалов для подготовки к практическим занятиям	16-25	
2 4	Методы и средства оценки безопасности компьютерных систем		Кейс-задание	26-29	Защита практической работы
			Подготовка доклада с визуальным представлением презентаци	30-40	Проверка преподавателем
			Подготовка курсовой работы	41-48	Защита курсовой работы
3	Организация оценки безопасности компьютерных систем		Вопросы к зачету	49-70	Проверка преподавателем

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 30 контрольных заданий, из них:

- 10 контрольных заданий на проверку знаний;
- 10 контрольных заданий на проверку умений;
- 10 контрольных заданий на проверку навыков.

3.1 Тесты (тестовые задания к зачету)

3.1.1 ***Шифр и наименование компетенции*** **ПКв-2** **–** способен разрабатывать проектные решения по защите информации в автоматизированных системах, модели угроз безопасности информации и модели нарушителя в автоматизированных системах, проекты нормативных документов, регламентирующих работу по защите информации

№ задания	Тестовое задание с вариантами ответов и правильными ответами
1	Ядро безопасности должно гарантировать: **1. Собственную неизменность.** 2. Конфиденциальность. 3. Анонимность. 4. Динамичность
2	Матрицы полномочий предназначены для: 1. Копирования данных. 2. Вычисления определителя. **3. Разграничения доступа к информации.**

	4. Стабильности работы операционной системы
3	Для оценки защищенности компьютерной системы достаточно рассмотреть ее: **1. Достоверную вычислительную базу.** 2. Уровень доступа. 3. Программное обеспечение. 4. Анонимность
4	Способ допуска к компьютерным ресурсам, основанный на использовании уникальной метки, – это: 1. Разовый доступ 2. Разграничение доступа по времени. 3. Гостевой доступ. **4. Разграничение доступа по мандатам.**
5	Реализацию угрозы информационной безопасности называют: **1. Атакой.** 2. Контратакой. 3. Блокадой. 4. Отступлением
6	Анализом возможных угроз ИБ и выбором соответствующих мер противодействия занимается: **1. Политика безопасности.** 2. Социальная политика. 3. Внутренняя политика. 4. Политика невмешательства.
7	События, следствием которых могут быть нежелательные воздействия на информацию, – это: 1. Антропогенные факторы 2. Стабилизирующие факторы. 3. **Дестабилизирующие факторы**. 4. Природные факторы.
8	Возможность возникновения события, которое оказывает нежелательные воздействия на информацию: **1. Угроза.** 2. Ошибка. 3. Отказ. 4. Сбой
9	Злоумышленное действие – это действие: **1. Специально направленное на нарушение информации.** 2. Произошедшее случайным образом. 3. Произошедшее под действием непреодолимых факторов.
10	Стандарт X.509 описывает: 1. Основы ИБ в привязке к эталонной семиуровневой модели. **2. Процедуру аутентификации с использованием службы каталогов.** 3. Модели управления доступом. 4. Анализ последствий нарушения ИБ и выявление злоумышленников
11	Концептуальной основой администрирования средств безопасности в стандарте X.800 является: **1. Информационная база управления безопасностью.** 2. База данных уязвимостей. 3. Контроль согласованности конфигураций различных компонентов.
12	Из перечисленных сервисов стандарт X.800 предусматривает: **1. Целостность данных.** **2. Аутентификацию.** 3. Контроль защищенности. 4. Обнаружение отказов и оперативное восстановление.
13	Протокол TCP/IP обеспечивает: 1. Идентификацию. 2. Шифрование. 3. Аутентификацию. **4. Создание виртуальных каналов.**
14	Комплект протоколов, предложенный IETF, обеспечивает аутентификацию, проверку целостности и шифрование IP пакетов: **1. IPSec.**

	2. OSPF. 3. ARP. 4. ICMP.
15	Метод, обычно использующийся профессиональными взломщиками при информационной атаке: 1. Атака на наиболее защищенную цель. 2. Атака на промежуточную цель. **3. Атака на наименее защищенную цель.** 4. Атака осуществляется без целенаправленного выбора цели.

3.2 Проработка материала для подготовки к практическим занятиям

3.2.1 ***Шифр и наименование компетенции*** **ПКв-2 –** способен разрабатывать проектные решения по защите информации в автоматизированных системах, модели угроз безопасности информации и модели нарушителя в автоматизированных системах, проекты нормативных документов, регламентирующих работу по защите информации

Номер задания	Текст задания
16.	Администрирование АИС: функции администратора, функции Службы безопасности
17.	Механизмы безопасности для обеспечения «неотказуемости» системы
18.	Администрирование средств безопасности
19.	Сети с выделенными каналами и их преимущества
20.	Аутентификация субъектов в распределенных системах, проблемы и решения. Схема Kerberos.
21.	Нормативно-правовое регулирование защиты информации: направления защиты
22.	Организационно-распорядительная защита информации: цели защиты, принципы построения защиты
23.	Виды криптосистем
24.	Описание стандарта X.509
25.	Методика выявления каналов несанкционированного доступа к информации

3.3 Кейс-задания

3.3.1 ***Шифр и наименование компетенции*** **ПКв-2 –** способен разрабатывать проектные решения по защите информации в автоматизированных системах, модели угроз безопасности информации и модели нарушителя в автоматизированных системах, проекты нормативных документов, регламентирующих работу по защите информации

Номер задания	Примерные варианты заданий
26	Разработать содержание и последовательность работ выполняемых при построении комплексной системы защиты информации; Перечислить основные этапы построения КСЗИ. Указать ГОСТы с учётом которых должны быть разработаны требования к системе защиты информации. Перечислить основные понятия которые будут определены при проектировании КСЗИ. **Ответ:** **1. Подготовка организационно-распорядительной документации.** **2. Обследование информационной инфраструктуры Заказчика.** **3. Разработка «Плана защиты информации».** **4. Разработка «Технического задания на создание КСЗИ».** **5. Разработка «Технического проекта на создание КСЗИ».** **6. Приведение информационной инфраструктуры Заказчика в соответствие с «Техническим проектом на создание КСЗИ».** **7. Разработка «Эксплуатационной документации на КСЗИ».** **8. Внедрение КСЗИ.**

	9. Испытание КСЗИ. **10. Проведение государственной экспертизы КСЗИ и получение «Аттестата соответствия».** **11. Поддержка и обслуживание КСЗИ** **ГОСТ Р 51583 «Защита информации. Порядок создания автоматизированных систем в защищенном исполнении. Общие положения»** **ГОСТ Р 51624 «Защита информации. Автоматизированные системы в защищенном исполнении. Общие требования** **Субъекты доступа** **Методы управления доступом** **Меры защиты информации** **Виды и типы средств защиты информации** **Структура КСЗИ информационной системы** **Меры защиты информации при информационном взаимодействии с иными информационными системами и информационно-телекоммуникационными сетями**
27	Изучить принцип обследования защищенности объекта информатизации (ОИ) посредством существующих стандартов и методик; Написать отчёт исследования предприятия, закреплённого преподавателем, содержащий общие сведения о предприятии, о его деятельности и организационной структуре Ответ: **Для решения данной задачи проводится комплексное обследование защищенности ОИ, результаты которого основываются на выявленных угрозах безопасности информации и оценке рисков нанесения возможного ущерба, а также позволяют оценить необходимость и достаточность принятых на объекте мер обеспечения безопасности информации. Предполагается, что по результатам комплексного обследования ОИ определяются адекватные потребностям ИС (по степени защищенности ее ресурсов) требования к средствам ее защиты, что позволяет добиться максимальной отдачи от инвестиций в создание и обслуживание системы обеспечения информационной безопасности (СОИБ) ИС.** **Задача проводимого обзора существующих стандартов и методик реализации обследования защищенности ОИ состоит в определении оценки объективности и полноценности данных стандартов и методик.** **Если посмотреть на общую существующую классификацию видов обследования ИБ (обследования защищенности), то можно выделить три вида обследования защищенности:** **инструментальное (дискретное и непрерывное);** **обследование защищенности ОИ на соответствие существующим стандартам и методикам;** **обследование защищенности как части специализированных исследований ОИ** **Перечень рассмотренных стандартов и методик, описывающих процессы обследования защищенности ОИ, представлены в стандартах** **ISO/IEC 15408, ISO/IEC 17799, ISO/IEC 27001:2005 и ISO/IEC 17799:2005 а** **также руководящих документах ФСТЭК. Предполагается, что в результате комплексного обследования защищенности ОИ происходит выделение актуальных угроз безопасности информации и определение перечня контрмер – эффективных методов противодействия значимым угрозам. Однако проведенная оценка показывает, что четкое следование существующим стандартам и методам и, как следствие, объективность и полнота выдаваемых экспертных оценок в ходе проведения обследования защищенности во многом зависит от квалификации**

	эксперта, проводящего обследование защищенности. **Таким образом, ставится актуальная в настоящее время задача по разработке механизма (и методики) обследования защищенности ОИ, способного выдавать обоснованные количественные оценки эффективности принятых мер противодействия, обоснованного количественного расчета деструктивных воздействий, проведения оценки угроз ОИ. Результатом применения разрабатываемого механизма должно стать снижение субъективности конечных оценок состояния защищенности ОИ и возможность обоснованной оценки эффективности принятых мер парирования угроз на ОИ.**
28	Разработать перечень нормативных документов на основе которых осуществляется построение системы защиты информации и перечень действий, осуществляющихся в каждом из этапов **Ответ:** **Этап 1. Формирование требований к системе защиты информации (предпроектный этап).** **1.1 Принятие решения о необходимости защиты обрабатываемой информации.** **1.2 Классификация объекта по требованиям защиты информации (установление уровня защищенности обрабатываемой информации).** **1.3 Определение угроз безопасности информации, реализация которых может привести к нарушению безопасности обрабатываемой информации.** **1.4 Определение требований к системе защиты информации.** **Этап 2. Разработка системы защиты информации (этап проектирования).** **2.1 Проектирование системы защиты информации.** **2.2 Разработка эксплуатационной документации на систему защиты информации.** **Этап 3. Внедрение системы защиты информации (этап установки, настройки, испытаний).** **3.1 Установка и настройка средств защиты информации.** **3.2 Внедрение организационных мер защиты информации, в том числе, разработка документов, определяющих правила и процедуры, реализуемые оператором для обеспечения защиты информации в ходе эксплуатации объекта.** **3.3 Выявление и анализ уязвимостей программных и технических средств, принятие мер по их устранению;** **3.4 Испытания и опытная эксплуатации системы защиты информации.** **Этап 4. Подтверждение соответствия системы защиты информации (этап оценки).** **4.1 Подача и рассмотрение заявки на аттестацию.** **4.2 Предварительное ознакомление с аттестуемым объектом (при необходимости).** **4.3 Разработка программы и методики аттестационных испытаний.** **4.4 Проведение аттестационных испытаний объекта.** **4.5 Оформление, регистрация и выдача аттестата соответствия.**
29	Разработать нормативные документы ФСТЭК по построению модели угроз. Построить модель угроз информационной системы персональных данных функционирующей в Вашей организации. Ответ: **В соответствии с «Методикой определения актуальных угроз безопасности**

	персональных данных при их обработке в информационных системах персональных данных» разработанной ФСТЭК, определение уровня исходной защищённости производится на основании анализа технических и эксплуатационных характеристик ИСПДн. **Исходный уровень защищенности определяется следующим образом:** **ИСПДн имеет высокий уровень исходной защищенности, если не менее 70% характеристик ИСПДн соответствуют уровню «высокий» (суммируются положительные решения по первому столбцу, соответствующему высокому уровню защищенности), а остальные – среднему уровню защищенности (положительные решения по второму столбцу).** **ИСПДн имеет средний уровень исходной защищенности, если не выполняются условия по пункту 1 и не менее 70% характеристик ИСПДн соответствуют уровню не ниже «средний» (берется отношение суммы положительные решений по второму столбцу, соответствующему среднему уровню защищенности, к общему количеству решений), а остальные – низкому уровню защищенности.** **ИСПДн имеет низкую степень исходной защищенности, если не выполняются условия по пунктам 1 и 2.** **В соответствии с «Методикой определения актуальных угроз безопасности персональных данных при их обработке в информационных системах персональных данных» разработанной ФСТЭК, под частотой (вероятностью) реализации угрозы понимается определяемый экспертным путем показатель, характеризующий, насколько вероятным является реализация конкретной угрозы безопасности ПДн для данной ИСПДн в складывающихся условиях обстановки**

3.4 Подготовка доклада

Примерные темы для доклада

3.4.1 Шифр и наименование компетенции: **ПКв-2 –** способен разрабатывать проектные решения по защите информации в автоматизированных системах, модели угроз безопасности информации и модели нарушителя в автоматизированных системах, проекты нормативных документов, регламентирующих работу по защите информации

Номер задания	Тема доклада
30.	Стандарты и спецификации в области ИБ
31.	Административный уровень ИБ. Концепция и политика безопасности учреждения/предприятия
32.	Факторы, влияющие на требуемый уровень защиты информации.
33.	Мероприятия, входящие в состав предпроектного обследование компании
34.	Построение модели угроз ИСПДн с учетом выбора своего варианта задания
35.	Принципы организации КСЗИ
36.	Анализ и оценка угроз безопасности информации
37.	Классификация мер обеспечения безопасности компьютерных систем
38.	Кадровое построение КСЗИ
39.	Стандарт оценки уязвимостей CVSS
40.	Методы идентификации риска

3.5. Подготовка курсовой работы

Примерные темы для курсовой работы

3.5.1 Шифр и наименование компетенции: **ПКв-2 –** способен разрабатывать проектные решения по защите информации в автоматизированных системах, модели угроз безопасности информации и модели нарушителя в автоматизированных системах, проекты нормативных документов, регламентирующих работу по защите информации

Номер задания	Текст задания

41.	Последовательность работ при построении комплексной системы защиты информации с учетом выбора своего варианта задания
42.	Изучение методов комплексного исследование объекта информатизации с учетом выбора своего варианта задания
43.	Изучение информации циркулирующей в корпоративной информационной системе с учетом выбора своего варианта задания
44.	Изучение построения системы защиты информации на основе нормативных актов и методических указаний с учетом выбора своего варианта задания
45.	Построение модели угроз ИСПДн с учетом выбора своего варианта задания
46.	Изучение действующей нормативной документации объекта информатизации с учетом выбора своего варианта задания
47.	Составление плана мероприятий по улучшению защищённости объекта информатизации с учетом выбора своего варианта задания
48.	Разработка политики информационной безопасности с учетом выбора своего варианта задания

3.6 Зачет (собеседование)

Вопросы для зачета

3.6.1 Шифр и наименование компетенции: **ПКв-2** **–** способен разрабатывать проектные решения по защите информации в автоматизированных системах, модели угроз безопасности информации и модели нарушителя в автоматизированных системах, проекты нормативных документов, регламентирующих работу по защите информации

Номер вопроса (задачи, задания)	Текст вопроса (задачи, задания)
49.	Определение и место проблем информационной безопасности в общей совокупности информационных проблем современного общества. Анализ развития подходов к защите информации. Современная постановка задачи защиты информации.
50.	Особенности и состав научно-методологического базиса решения задач защиты информации. Общеметодологические принципы формирования теории защиты информации.
51.	Основное содержание теории защиты информации. Модели систем и процессов защиты информации.
52.	Определение и содержание понятия угрозы информации в современных системах ее обработки. Системная классификация угроз. Система показателей уязвимости информации. Методы и модели оценки уязвимости информации.
53.	Постановка задачи определения требований к защите информации. Методы оценки параметров защищаемой информации. Факторы, влияющие на требуемый уровень защиты информации.
54.	Определение и общеметодологические принципы построения систем защиты информации. Основы архитектурного построения систем защиты. Типизация и стандартизация систем защиты.
55.	Основные выводы из истории развития теории и практики защиты информации. Перспективы развития теории и практики защиты. Трансформация проблемы защиты информации в проблему обеспечения информационной безопасности.
56.	Основные подходы к оценке и принципы оценки безопасности ИТ, используемые в TCSEC, ITSEC, РД Гостехкомиссии России. Сходство и различия.
57.	Концепция разработки и оценки СЗИ НСД, действующая в России (на основе РД Гостехкомиссии России). Сходство и различия в подходах к оценке безопасности ИТ, изложенных в РД Гостехкомиссии России и «Общих критериях».
58.	Концепция оценки безопасности ИТ, лежащая в основе «Общих критериев». Сходство и различия в подходах к оценке безопасности ИТ, изложенных в РД Гостехкомиссии России и «Общих критериях».
59.	Понятие и сущность КСЗИ. Назначение КСЗИ. Методика выявления нарушителей (незаконных пользователей) и состава интересующей их информации.
60.	Методология защиты информации как теоретический базис построения КСЗИ. Оценка степени уязвимости информации в результате действий нарушителей различных категорий.
61.	Методика выявления каналов несанкционированного доступа к

	информации. Определение источников дестабилизирующего воздействия на информацию и видов их воздействия.
62.	Принципы организации КСЗИ. Соотношение между каналами несанкционированного доступа и источниками воздействия на информацию.
63.	Основные требования, предъявляемые к КСЗИ. Определение возможных методов несанкционированного доступа к защищаемой информации.
64.	Содержательная характеристика этапов разработки КСЗИ. Анализ потенциальных последствий реализации несанкционированного доступа.
65.	Основные факторы, влияющие на организацию КСЗИ. Организационно-правовая форма и характер основной деятельности предприятия.
66.	Основные факторы, влияющие на организацию КСЗИ. Состав, объем и степень конфиденциальности защищаемой информации. Методика выявления способов воздействия на информацию
67.	Основные факторы, влияющие на организацию КСЗИ. Структура и территориальное расположение предприятия. Определение причин, обстоятельств и условий дестабилизирующего воздействия на информацию.
68.	Основные факторы, влияющие на организацию КСЗИ. Степень автоматизации основных процедур обработки защищаемой информации. Оценка ущерба от потенциального дестабилизирующего воздействия на информацию.
69.	Методика определения состава защищаемой информации. Значение носителей защищаемой информации как объектов защиты. Факторы, определяющие состав носителей информации.
70.	Этапы работы по выявлению состава защищаемой информации. Методика выявления состава носителей защищаемой информации. Хранилища носителей информации как объект защиты.

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* ПКв-2 –** способен разрабатывать проектные решения по защите информации в автоматизированных системах, модели угроз безопасности информации и модели нарушителя в автоматизированных системах, проекты нормативных документов, регламентирующих работу по защите информации					
ЗНАТЬ: базовые понятия современных методов оценки безопасности компьютерных систем; проблемы обеспечения безопасности информации, решаемые с применением современных методов и средств защиты информации в компьютерных системах; принципы и способы использования существующих средств защиты информации в компьютерных системах; принципы применения современных методов оценки безопасности компьютерных систем	Тест (тестовые задания к зачету) Собеседование (зачет)	Уровень знаний	50% и более правильных ответов	Зачтено	Освоена (базовый, повышенный)
			менее 50% правильных ответов	Не зачтено	Не освоена (недостаточный)
УМЕТЬ: выявлять угрозы и определять их актуальность для современных компьютерных систем; описывать (моделировать) объекты защиты и угрозы безопасности компьютерных систем; применять наиболее эффективные методы	Кейс-задание	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)

обеспечения безопасности компьютерных систем; применять современные методы оценки безопасности компьютерных систем					
ВЛАДЕТЬ: практическими навыками применения методов обеспечения безопасности компьютерных систем; навыками применения современных методов оценки безопасности компьютерных систем; навыками применения современных методов оценки безопасности компьютерных систем и моделирования различных угроз безопасности информации в автоматизированных системах	Курсовая работа	Методика и правильность решения задачи	Обучающийся разобрался в предложенной конкретной ситуации, самостоятельно решил поставленную задачу на основе полученных знаний	Зачтено	Освоена (базовый, повышенный)
			Обучающийся не разобрался в сложившейся ситуации, не выявил причины случившегося и не предложил вариантов решения	Не зачтено	Не освоена (недостаточный)