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

Система обнаружения компьютерных атак
(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-1	способен проводить тестирование систем защиты информации автоматизированных систем; составлять методики тестирования систем, подбирать инструментальные средства тестирования систем защиты информации автоматизированных систем	ИД2 $_{ПКв-1}$ – способен создавать методики тестирования защищенных автоматизированных систем
			ИД3 $_{ПКв-1}$ – способен выбирать инструментальные средства тестирования защищенных автоматизированных систем

Код и наименование индикатора достижения компетенции	Результаты обучения (показатели оценивания)
ИД2 $_{ПКв-1}$ – способен создавать методики тестирования защищенных автоматизированных систем	Знает: методики создания данных автоматизированных систем
	Умеет: определять уязвимые места информационных автоматизированных систем
	Владеет: навыками выявления нарушения защищенности автоматизированных систем
ИД3 $_{ПКв-1}$ – способен выбирать инструментальные средства тестирования защищенных автоматизированных систем	Знает: инструментальные средства тестирования защищенных автоматизированных систем
	Умеет: разрабатывать регламент тестирования защищенных автоматизированных систем
	Владеет: навыками администрирования и управления инструментальными средствами в области информационной безопасности

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 _3_ зачетные единицы.

Виды учебной работы	**Всего академических часов**	**Распределение трудоемкости по семестрам,** Акад. ч
		2 семестр
Общая трудоемкость дисциплины	**108**	**108**
Контактная работа в т. ч. аудиторные занятия:	**55**	**55**
Лекции	18	18
в том числе в форме практической подготовки	–	–
Практические занятия	36	36
в том числе в форме практической подготовки	36	36
Консультации текущие	0,9	0,9
Вид аттестации (зачет)	0,1	0,1
Самостоятельная работа:	**53**	**53**
Проработка материалов по конспекту лекций	3,6	3,6
Проработка материалов по учебнику для подготовки к практическим занятиям	11,6	11,6
Подготовка к коллоквиуму	1,8	1,8
Оформление отчетов по практическим работам	36	36

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

5.1 Содержание разделов дисциплины

№ п/п	Наименование раздела дисциплины	Содержание раздела *(указываются темы и дидактические единицы)*	Трудоемкость раздела, ак.ч
1	Теоретические основы	Модель OSI. Оборудование локальных сетей.	34
2	Классификация атак по уровням иерархической модели OSI	Атаки на физическом уровне. Атаки на канальном уровне; Атаки на сетевом уровне; Атаки на транспортном уровне; Безопасность прикладного уровня.	35
3	Уязвимости	Основные типы уязвимостей.	37
	Консультации текущие		0,9
	Зачет		0,1

5.2 Разделы дисциплины и виды занятий

№ п/п	Наименование раздела дисциплины	Лекции, ак. ч	Практические занятия, ак. ч	СРО, ак. ч
1	Теоретические основы вычислительных сетей	6*****	12*****	16
2	Классификация атак по уровням иерархической модели OSI	6*****	12*****	17
3	Уязвимости	6*****	12*****	19
	Консультации текущие	0,9		
	Зачет	0,1		

5.2.1 Лекции

№	Наименование раздела	Тематика лекционных занятий	Трудоемкос

п/п	дисциплины		ть, ак. ч
1	Теоретические основы вычислительных сетей	Основные понятия информационных сетей; класс информаци-онных сетей как открытые ин-формационные системы; модели и структуры информационных сетей; информационные ре-сурсы сетей. Модель OSI: Прикладной (7) уровень (Application Layer); представительский (6) уровень (Presentation Layer); Сеансовый (5) уровень (Session Layer); Транспортный (4) уровень (Transport Layer); Сетевой (3) уровень (Network Layer); Канальный (2) уровень (Data Link Layer); Физический (1) уровень (Physical Layer)	6*
2	Классификация атак по уровням иерархической модели OSI	Атаки на физическом уровне. Концентраторы. Атаки на канальном уровне; Атаки на коммутаторы; Переполнение CAM-таблицы. VLAN Hoping Атака на STP; MAC Spoofing;Атака на PVLAN (Private VLAN) Атака на DHCP; ARP-spoofing; Атаки на сетевом уровне; Атаки на маршрутизаторы; Среды со статической маршрутизацией; Безопасность статической маршрутизации; Среды с динамической маршрутизацией; Scapy - универсальное средство дли реализации сетевых атак; Среды с протоколом RIP; Безопасность протокола RIP; Ложные маршруты RIP; Понижение версии протокола RIP; Взлом хэша MD5; Обеспечение безопасности протокола RIP; Среды с протоколом OSPF; Безопасность протокола OSPF; Среды с протоколом BGP; Атака BGP Router Masquerading; Атаки на MD5 для BGP; «Слепые» DoS-атаки на BGP- маршрутизаторы; Безопасность протокола BGP; Атаки на BGP; Атаки на транспортном уровне. Транспортный протокол TCP; Известные проблемы; Атаки на TCP; IP- spoofing; TCP hacking; Десинхронизация нулевыми данными; Сканирование сети; SYN-флуд; Атака Teardrop; Безопасность TCP; Атаки на уровне приложений; Безопасность прикладного уровня;Протокол SNMP; Протокол Syslog; Протокол DNS; Безопасность DNS; Веб- приложения; Атаки на веб через управление сессиями; Защита DNS; SQL-инъекции	6*
3	Уязвимости	Основные типы уязвимостей; Уязвимости проектирования; Уязвимости реализации; Уязвимости эксплуатации; Примеры уязвимостей; Права доступа к файлам; Оперативная память; Объявление памяти; Завершение нулевым байтом; Сегментация памяти программы; Переполнение буфера; Переполнения в стеке; Эксплоит без кода эксплоита; Переполнения в куче и bss; Перезапись указателей функций; Форматные строки; Сканирование приложений на наличие уязвимостей; Эксплуатация найденных уязвимостей; Защита от уязвимостей.	6*

5.2.2 Практические занятия (семинары)

№ п/п	Наименование раздела дисциплины	Тематика практических занятий (семинаров)	Трудоемкость, ак. ч
1	Теоретические основы вычислительных сетей	Работа с операционными системами Linux Server и Windows Server.	2*
		Работа с операционными системами Linux Server и Windows Server.	2*

		Основные команды, приемы администрирования.	2*
		Основы администрирования промышленных СУБД. Прз – 1.	2*
		Основы администрирования промышленных СУБД. Прз – 2.	2*
		Основы администрирования промышленных СУБД. Прз – 3.	2*
2	Классификация атак по уровням иерархической модели OSI	Работа с дистрибутивом диагностики и защиты сетей Kali Linux. Прз – 1.	2*
		Работа с дистрибутивом диагностики и защиты сетей Kali Linux. Прз – 2.	2*
		Работа с дистрибутивом диагностики и защиты сетей Kali Linux. Прз – 3.	2*
		Работа с дистрибутивом диагностики и защиты сетей Kali Linux. Прз – 4.	2*
		Работа с дистрибутивом диагностики и защиты сетей Kali Linux. Прз – 5.	2*
		Работа с дистрибутивом диагностики и защиты сетей Kali Linux. Прз – 6.	2*
3	Уязвимости	Антивирусная диагностика и защита. Прз – 1.	2*
		Антивирусная диагностика и защита. Прз – 2.	2*
		Антивирусная диагностика и защита. Прз – 3.	2*
		Антивирусная диагностика и защита. Прз – 4.	2*
		Антивирусная диагностика и защита. Прз – 5.	2*
		Антивирусная диагностика и защита. Прз – 6.	2*

5.2.3 Лабораторный практикум

Не предусмотрен.

5.2.4 Самостоятельная работа обучающихся

№ п/п	Наименование раздела дисциплины	Вид СРО	Трудоемкость, ак. ч
1	Теоретические основы вычислительных сетей	Проработка лекций, учебников (собеседование, коллоквиум)	4
		Подготовка отчетов по практической работе	12
2	Классификация атак по уровням иерархической модели OSI	Проработка лекций, учебников (собеседование, коллоквиум)	5
		Подготовка отчетов по практической работе	12
3	Уязвимости	Проработка лекций, учебников (собеседование)	7
		Подготовка отчетов по практической работе	12

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	*http://www.window.edu.ru/*

образовательным ресурсам»	
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

СИСТЕМА ОБНАРУЖЕНИЯ КОМПЬЮТЕРНЫХ АТАК

1 Перечень компетенций с указанием этапов их формирования

№ п/п	Код компетенции	Формулировка компетенции	Код и наименование индикатора достижения компетенции
1	ПКв-1	способен проводить тестирование систем защиты информации автоматизированных систем; составлять методики тестирования систем, подбирать инструментальные средства тестирования систем защиты информации автоматизированных систем	ИД2 $_{ПКв-1}$ – способен создавать методики тестирования защищенных автоматизированных систем
			ИД3 $_{ПКв-1}$ – способен выбирать инструментальные средства тестирования защищенных автоматизированных систем

Код и наименование индикатора достижения компетенции	Результаты обучения (показатели оценивания)
ИД2 $_{ПКв-1}$ – способен создавать методики тестирования защищенных автоматизированных систем	Знает: методики создания данных автоматизированных систем
	Умеет: определять уязвимые места информационных автоматизированных систем
	Владеет: навыками выявления нарушения защищенности автоматизированных систем
ИД3 $_{ПКв-1}$ – способен выбирать инструментальные средства тестирования защищенных автоматизированных систем	Знает: инструментальные средства тестирования защищенных автоматизированных систем
	Умеет: разрабатывать регламент тестирования защищенных автоматизированных систем
	Владеет: навыками администрирования и управления инструментальными средствами в области информационной безопасности

2 Паспорт оценочных материалов по дисциплине

№ п/п	Разделы дисциплины	Индекс контролируемой компетенции (или ее части)	Оценочные материалы		Технология/процедура оценивания (способ контроля)
			наименование	№№ заданий	
1	Теоретические основы вычислительных сетей	ПКв-1	Тестовые задания	1-25	Бланочное или компьютерное тестирование
2	Классификация атак по уровням иерархической модели OSI		Подготовка к коллоквиуму	26-35	Проверка преподавателем
			Проработка материала лекций	36-45	Проверка преподавателем
3	Уязвимости		Кейс-задание	46-49	Защита практической работы

			Вопросы к зачету	50-70	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 25 контрольных заданий, из них:

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

3.1 Тесты (тестовые задания к зачету)

3.1.1 ***Шифр и наименование компетенции*** **ПКв-1** **–** способен проводить тестирование систем защиты информации автоматизированных систем; составлять методики тестирования систем, подбирать инструментальные средства тестирования систем защиты информации автоматизированных систем

№ задания	Тестовое задание с вариантами ответов и правильными ответами
1.	Системный администратор это **1. пользователь, осуществляющий контроль над системой и отвечающий за её работу** 2. управленческий персонал 3. пользователь, работающий с графическим интерфейсом операционной системы
2.	Заданием параметров запуска приложений занимаются 1. Службы управления по контролю характеристик **2. Службы управления конфигурацией** 3. Службы управления производительностью 4. Службы управления безопасностью
3.	Системный администратор должен: 1. иметь исчерпывающие знания в области операционных систем **2. иметь представление о программировании** **3. иметь широкий кругозор, позволяющий работать с различными архитектурами машин и различными версиями систем** 4. работать с пользовательскими программами
4.	К компонентам ИС относятся **1. Технические средства** 2. Операционные расходы на содержание ИС **3. Информационный фонд** 4. Обслуживающий персонал
5.	К задачам обеспечивающих подсистем не относят 1. Администрирование ОС и СУБД 2. Администрирование данных **3. Администрирование кабельных систем** 4. Администрирование методов обработки информации

6.	Службы эксплуатации и сопровождения отвечают за 1. Учет использования ресурсов в системе 2. Анализ работы ИС 3. Определение режимов копирования **4. Стратегии восстановления**
7.	Объектами администрирования являются: 1. группа пользователей **2. базы данных** **3. операционные системы** 4. ЛВС 5. почтовые и Internet серверы
8.	По уровню автоматизации управления различают информационные системы: 1. **АСУ объектом** 2. стратегические, операторские системы 3. централизованные и децентрализованные системы
9.	По режиму работы комплекса технических средств различают информационные системы: 1. пакетные, реальные, диалоговые 2. **дискретные, непрерывные** 3. управленческие, производственные
10.	По принципу интеграции функциональных задач различают информационные системы: 1. **система, подсистема, отдельные задачи** 2. бухгалтерские, банковские, страховые, налоговые системы 3. централизованные и децентрализованные системы
11.	К задачам администрирования подсистем относятся 1. **Администрирование СУБД** 2. **Администрирование сетевой системы** 3. Web администрирование 4. Администрирование удаленных ПК
12.	В модели OSI обмен управляющей информацией происходит между 1. Субъектами управляющих воздействий 2. **Субъектами приложений управления** 3. Субъектами уровня представления 4. Субъектами вспомогательных служб
13.	Субъекты SMAE расположены на 1. Представительном уровне 2. Транспортном уровне 3. **Прикладном уровне** 4. Канальном уровне 5. Физическом уровне
14.	Обеспечивает подключение удаленных клиентов к внутренней сети с помощью маршрутизации 1. WINS-сервер 2. DHCP-сервер 3. DNS-сервер 4. **VPN-сервер**
15.	Типы профилей пользователя 1. **Локальный** 2. Серверный 3. **Перемещаемый** 4. Сетевой
16.	С помощью каких оснасток можно управлять настройками удаленного компьютера 1. **Административных** 2. С динамическим фокусом 3. Консольные 4. С расширенными правами
17.	Для запрещения изменения настроек пользовательского профиля применяют: 1. Обязательный профиль 2. **Групповые политики** 3. Локальные политики 4. AD 5. Доменные настройки

18.	Политика аудита учетных записей содержит параметры: 1. **Аудит событий входа в систему** 2. Аудит аутентификации 3. Аудит событий управления записью 4. **Аудит управления учетными записями** 5. **Аудит входа в систему**
19.	В модели OSI описывают возможности управляющей системы 1. Знания определений 2. Знания репертуара 3. Знания об экземплярах 4. **Знания управления**
20.	Количество функциональных групп в модели управления FRAPS 1. 3 2. 4 3. **5** 4. 6 5. 7
21.	В модели управления FRAPS непрерывный источник информации для мониторинга работы сети 1. Управление учетом 2. Управление безопасностью 3. **Управление производительностью** 4. Управление конфигурированием
22.	Управление в модели ITIL осуществляется на базе 1. Управления процессами IT сервисов 2. **Управления подсистем** 3. Управления задачами 4. Управления службами контроля
23.	Объектами управления TMN являются 1. Базы данных 2. Информационные системы 3. Операционные системы 4. **Телекоммуникационные ресурсы**
24.	Ракурс развертывания в модели eTOM обеспечивает 1. **Необходимые аппаратные и программные средства** 2. Моделирование системного решения 3. Взаимосвязь между бизнес процессами 4. Поток работ и требования
25.	Совокупность библиотек, которые позволяют вызывать С-процедуры для общения между узлами сети 1. NFS 2. IPX **3. RPC** 4. ICMP

3.2 Подготовка к коллоквиуму

3.2.1 ***Шифр и наименование компетенции*** **ПКв-1** **–** способен проводить тестирование систем защиты информации автоматизированных систем; составлять методики тестирования систем, подбирать инструментальные средства тестирования систем защиты информации автоматизированных систем

№ задания	Текст вопроса (задачи, задания)
26.	Информационные сети. Основные понятия и классы
27.	Семиуровневая модель OSI
28.	Концентраторы
29.	Атаки на канальном уровне

30.	Атаки на маршрутизаторы
31.	Протокол RIP. Безопасность, среды, ложные маршруты.
32.	Протокол BGP. Обеспечение безопасности, атаки.
33.	Атаки на транспортном уровне
34.	Протокол DNS
35.	Атаки на веб через управление сессиями

3.3 Проработка материалов лекций

3.3.1 ***Шифр и наименование компетенции*** **ПКв-1** **–** способен проводить тестирование систем защиты информации автоматизированных систем; составлять методики тестирования систем, подбирать инструментальные средства тестирования систем защиты информации автоматизированных систем

№ задания	Текст вопроса (задачи, задания)
36.	Основные понятия информационных сетей
37.	Модели и структуры информационных систем
38.	Модель OSI и ее уровни
39.	Атаки на физическом уровне
40.	Атаки на сетевом уровне
41.	Безопасность протокола RIP
42.	Среды с динамической маршрутизацией
43.	Транспортный протокол TCP
44.	Среды с протоколом OSPF
45.	Атаки на уровне приложений

3.4 Кейс-задания к практическим работам

3.4.1 ***Шифр и наименование компетенции*** **ПКв-1** **–** способен проводить тестирование систем защиты информации автоматизированных систем; составлять методики тестирования систем, подбирать инструментальные средства тестирования систем защиты информации автоматизированных систем

№ задания	Текст задания

46.	Проанализируйте основные угрозы информации в компьютерных системах. **Ответ:** **Множество угроз может быть разделено на 2 класса – случайные и преднамеренные.** **Случайные угрозы можно классифицировать следующим образом:** **Стихийные бедствия и аварии (чреваты наиболее разрушительными последствиями для КС, т.к. последние подвергаются физическому разрушению, информация утрачивается или доступ к ней становится невозможен)** **Сбои и отказы технических средств (В результате сбоев и отказов нарушается работоспособность технических средств, уничтожаются и искажаются данные и программы, нарушается алгоритм работы устройств)** **Ошибки при разработке КС (приводят к последствиям, аналогичным последствиям сбоев и отказов технических средств. Кроме того, такие ошибки могут быть использованы злоумышленниками для воздействия на ресурсы КС)** **Алгоритмические и программные ошибки;** **Ошибки пользователей и обслуживающего персонала. (Некомпетентное, небрежное или невнимательное выполнение функциональных обязанностей сотрудниками приводят к уничтожению, нарушению целостности и конфиденциальности информации, а также компрометации механизмов защиты)** **Преднамеренные угрозы классифицируются как:** **традиционный или универсальный шпионаж и диверсии (подслушивание, наблюдение, хищение документов, данных, подкуп и шантаж, поджоги и взрывы)** **несанкционированный доступ к информации (НСД) (получение защищаемой информации заинтересованными субъектами с нарушением установленных нормативными и правовыми документами (актами) или обладателями информации прав или правил разграничения доступа к защищаемой информации)** **утечка по техническим каналам (процесс обработки и передачи информации техническими средствами КС сопровождается электромагнитными излучениями в окружающее пространство и наведением электрических сигналов в линиях связи, сигнализации, заземлении и других проводниках)** **модификация структур КС (Несанкционированное изменение структуры КС на этапах разработки и модернизации получило название «закладка»)** **вредоносные программы**
47.	Выделите основные особенности защиты информации на узлах компьютерной сети **Ответ:** **Основной особенностью любой сетевой системы является то, что ее компоненты распределены в пространстве и связь между ними физически осуществляется при помощи сетевых соединений (коаксиальный кабель, витая пара, оптоволокно и т. п.) и программно при помощи механизма сообщений. При этом все управляющие сообщения и данные, пересылаемые между объектами распределенной вычислительной системы, передаются по сетевым соединениям в виде пакетов обмена. Сетевые системы характерны тем, что наряду с локальными угрозами, осуществляемыми в пределах одной компьютерной системы, к ним применим специфический вид угроз, обусловленный распределенностью ресурсов и информации в пространстве. Это так называемые сетевые или удаленные угрозы. Они характерны, во-первых, тем, что злоумышленник может находиться за тысячи километров от атакуемого объекта, и, во-вторых, тем, что нападению может подвергаться не конкретный компьютер, а информация, передающаяся по сетевым соединениям.** **Цели сетевой безопасности могут меняться в зависимости от ситуации, но основные цели обычно связаны с обеспечением составляющих "информационной безопасности":** • **целостности данных;** • **конфиденциальности данных;** • **доступности данных**
48.	**Рассмотрите назначение, виды и особенности сигнатурного анализа и обнаружения аномалий** **Ответ:**

	Сигнатурный анализ основан на предположении, что сценарий атаки известен и попытка ее реализации может быть обнаружена в журналах регистрации событий или путем анализа сетевого трафика. В идеале администратор информационной системы должен устранить все известные ему уязвимости. истемы обнаружения атак, использующие методы сигнатурного анализа, предназначены для решения обозначенной проблемы, так как в большинстве случаев позволяют не только обнаружить, но и предотвратить реализацию атаки на начальной стадии ее выполнения. Процесс обнаружения атак в данных системах сводится к поиску заранее известной последовательности событий или строки символов в упорядоченном во времени потоке информации. Механизм поиска определяется способом описания атаки. Применение методов сигнатурного анализа требует от разработчика СОА выбора или создания специального языка, позволяющего описывать регистрируемые системой события, а также устанавливать соответствия между ними. Универсальность и полнота этого языка являются определяющими факторами эффективной работы системы обнаружения, так как в конечном счете на этом языке будут сформулированы правила, по которым выявляется атака
49.	Рассмотрите уязвимости протокола TCP/IP протокола. **Ответ:** **Протокол IP не ориентирован на установку соединений. Не гарантируется, что пакеты придут в пункт назначения и сохранится порядок, в котором они были отправлены. Злонамеренный пользователь может подменить действительный адрес в поле адреса отправителя любым другим адресом. В TCP, как и IP-адрес, порт отправителя не проверя-ется и поэтому может быть подменен нарушителем. По заголовку TCP можно определить тип отправленного пакета. Тип пакета зависит от набора установленных флагов, которых всего шесть: Urgent, Ack, Push, Reset, Syn и Fin. Флаги Urgent и Push используются довольно редко. Большинство флагов и их комбинаций используются при установлении и разрыве соединений. Протокол UDP не ориентирован на установку соединений. Заголовок UDP-пакета очень простой и не содержит флагов или порядковых номеров. Поскольку компьютер-отправитель не выполняет проверку заголовка UDP, то в качестве номера порта отправителя взломщик может указать любой удобный ему номер. Так как для UDP не требуется установления соединения, то гораздо проще подменить как IP-адрес, так и порт отправителя пакетов. Для создания интерактивных сеансов связи с помощью ICMP-пакетов зло-умышленник может воспользоваться программой, наподобие ISHELL. Блокирование ICMP-пакетов сделает невозможным такой «скрытый» сеанс связи.**

3.5 Зачет (собеседование)

Вопросы для зачета

3.5.1 Шифр и наименование компетенции: **ПКв-1** – способен проводить тестирование систем защиты информации автоматизированных систем; составлять методики тестирования систем, подбирать инструментальные средства тестирования систем защиты информации автоматизированных систем

№ зада-ния	Текст вопроса (задачи, задания)
50.	Перечислите основные угрозы информации в компьютерных системах.
51.	Перечислите особенности защиты информации на узлах компьютерной сети.
52.	Перечислите системы обнаружения атак.
53.	Уязвимости TCP/IP протокола?
54.	Что такое МЭ?
55.	Каковы основные аспекты создания системы обнаружения атак.
56.	Сетевые сенсоры.
57.	Виртуальная частная сеть.
58.	Аутентификация и авторизация. Уязвимости аутентификации и авторизации.
59.	Классификация уязвимостей.

60.	Уязвимости платформы Windows.
61.	Классификация атак.
62.	Модель атаки. Этапы реализации атак.
63.	Что такое система обнаружения атак.
64.	Схема работы системы обнаружения.
65.	Признаки атак. Источники информации об атаках.
66.	Технологии и подходы к обнаружению атак.
67.	Анализ сетевого трафика.
68.	Анализ сервисов и портов.
69.	Системы анализа защищенности.
70.	Журнал регистрации, его назначение

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-1** **–** способен проводить тестирование систем защиты информации автоматизированных систем; составлять методики тестирования систем, подбирать инструментальные средства тестирования систем защиты информации автоматизированных систем					
ЗНАТЬ: методики создания данных автоматизированных систем, инструментальные средства тестирования защищенных автоматизированных систем	Собеседование (зачет)	Уровень знаний	50% и более правильных ответов	Зачтено	Освоена (базовый, повышенный)
			менее 50% правильных ответов	Не зачтено	Не освоена (недостаточный)
УМЕТЬ: определять уязвимые места информационных автоматизированных систем, разрабатывать регламент тестирования защищенных автоматизированных систем	Тест (тестовые задания к зачету)	Умение применять полученные знания	85% и более правильных ответов	Отлично	Освоена (повышенный)
			75-84% правильных ответов	Хорошо	Освоена (повышенный)
			65-74% правильных ответов	Удовлетворительно	Освоена (базовый)
			Менее 64% правильных ответов	Неудовлетворительно	Не освоена (недостаточный)
ВЛАДЕТЬ: навыками выявления нарушения защищенности автоматизированных систем, навыками администрирования и управления инструментальными средствами в области информационной безопасности	Кейс-задание	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)