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

Программно-аппаратные средства обеспечения информационной безопасности

(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 «Программно-аппаратные средства обеспечения информационной безопасности» является формирование компетенций обучающегося в области профессиональной деятельности и сфере профессиональной деятельности:

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

Дисциплина направлена на решение задач профессиональной деятельности научно-исследовательского, проектного, контрольно-аналитического, эксплуатационного типов.

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

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

№ п/п	Код компетенции	Формулировка компетенции	Код и наименование индикатора достижения компетенции
1	ОПК-15	Способностью осуществлять администрирование и контроль функционирования средств и систем защиты информации автоматизированных систем, инструментальный мониторинг защищенности автоматизированных систем	$ИД1_{ОПК-15}$ – обладает способностью применять специализированные технические средства защиты информации, администрирование программного обеспечения в автоматизированных системах
			$ИД2_{ОПК-15}$ – обладает способностью осуществлять инструментальный мониторинг защищённости автоматизированных систем при помощи методов и технологий защиты информации

Код и наименование индикатора достижения компетенции	Результаты обучения (показатели оценивания)
$ИД1_{ОПК-15}$ – обладает способностью применять специализированные технические средства защиты информации, администрирование программного обеспечения в автоматизированных системах	Знает: основные средства и способы обеспечения информационной безопасности
	Умеет: проектировать и администрировать компьютерные сети
	Владеет: навыками использования программно-апппаратных средств обеспечения безопасности компьютерных сетей
$ИД2_{ОПК-15}$ – обладает способностью осуществлять инструментальный мониторинг защищённости автоматизированных систем при помощи методов и технологий защиты информации	Знает: принципы построения систем защиты информации при помощи методов и технологий защиты информации
	Умеет: осуществлять инструментальный мониторинг безопасности компьютерной сети
	Владеет: навыками эксплуатации программно-аппаратных средств обеспечения автоматизированных систем

3. Место дисциплины в структуре ОП ВО

Дисциплина «Программно-аппаратные средства обеспечения информационной безопасности» относится к базовой части ОП ВО.

Изучение дисциплины основано на знаниях, умениях и навыках, полученных при изучении дисциплин «Корпоративные информационные системы» и прохождении учебной (ознакомительной) практики.

Дисциплина является предшествующей для прохождения производственной (преддипломной) практики, подготовке к процедуре защиты и защиты выпускной квалификационной работы.

4. Объем дисциплины и виды учебных занятий

Общая трудоемкость дисциплины составляет 8 зачетных единиц.

Виды учебной работы	**Всего ак. ч**	**Распределение трудоемкости по семестрам, ак. ч**	
		7 семестр	8 семестр
Общая трудоемкость дисциплины	**288**	**108**	**180**
Контактная работа, в т.ч. аудиторные занятия	**168,95**	**75,85**	**93,1**
Лекции	33	15	18
в том числе в форме практической подготовки	–	–	–
Лабораторные работы (ЛР)	66	30	36
в том числе в форме практической подготовки	–	–	–
Практические занятия (ПЗ)	66	30	36
в том числе в форме практической подготовки	–	–	–
Консультации текущие	1,65	0,75	0,9
Консультации перед экзаменом	2	–	2
Виды аттестации – зачет, экзамен	0,3	0,1	0,2
Самостоятельная работа	**85,25**	**32,15**	**53,1**
Проработка материалов по лекциям, учебникам, учебным пособиям	19,25	7,15	12,1
Подготовка к практическим и лабораторным занятиям	18	7	11
Подготовка доклада с презентацией	10	–	10
Домашнее задание	30	10	20
Подготовка к коллоквиуму	8	8	–
Контроль (подготовка к экзамену)	**33,8**	**–**	**33,8**

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, акад. ч
1	Общие сведения о программных и программно-аппаратных методах и средствах обеспечения информационной безопасности	Цели и задачи курса. Содержание дисциплины. Рекомендуемая литература. Основные понятия и определения. Роль и место знаний по дисциплине «Программно-аппаратные средства обеспечения информационной безопасности» при освоении смежных дисциплин по выбранной специальности; в сфере профессиональной деятельности. Роль и место программно-аппаратных средств защиты информации в обеспечении информационной безопасности. Предмет и задачи программно-аппаратной защиты информации. Современный уровень и перспективы развития программно-аппаратных средств обеспечения информационной безопасности.	25,15
2	Разграничение доступа	Избирательное разграничения доступа. Понятие матрицы доступа. Два подхода к кодированию матрицы доступа: векторы и списки. Изолированная программная среда. Полномочное разграничение доступа. Средства динамического изменения полномочий пользователя: необходимость, различные подходы к реализации.	39
3	Аутентификация	Правила безопасного хранения эталонной копии аутентификационной информации. Правила	41

		безопасной передачи по каналам связи аутентификационной информации. Понятие о специализированных сетевых протоколах безопасной аутентификации (Kerberos и т.п.). Проблемы парольной аутентификации. Методы подбора пароля. Средства защиты от подбора и компрометации паролей. Особенности аутентификации с использованием внешних носителей информации. Проблемы генерации и распределения ключей. Особенности биометрической аутентификации. Особенности аутентификации в системах управления базами данных. Реализация подсистем аутентификации в распространенных операционных системах.	
4	Подсистема регистрации и учета	Необходимость регистрации и учета событий в защищенной автоматизированной системе. Основные требования к политике аудита. Требования к организации подсистемы аудита, к политике аудита. Настройка политики аудита в распространенных операционных системах.	50
5	Защита программ и данных от несанкционированного копирования	Задача защиты от несанкционированного копирования. Методы привязки к программно-аппаратной среде. Применение специальных аппаратных устройств (электронных ключей и т.п.) для защиты от несанкционированного копирования информации. Основные методы взлома систем защиты программ и данных от несанкционированного копирования: программная эмуляция эталонной программно-аппаратной среды, непосредственный взлом системы защиты («выкусывание» защитного кода).	49
6	Защита от вредоносных воздействий компьютерных вирусов и программных закладок	Основные типы компьютерных вирусов: файловые, сетевые, почтовые, макровирусы. Основные модели программных закладок: наблюдатель, перехват, искажение. Типичные признаки присутствия в системе компьютерных вирусов и программных закладок. Основные средства и методы противодействия компьютерным вирусам и программным закладкам: сигнатурное и эвристическое сканирование, контроль целостности, антивирусный мониторинг. Факторы, ограничивающие эффективность антивирусных средств.	46,1

5.2 Разделы дисциплины и виды занятий

№ п/п	Наименование раздела дисциплины	Лекции, ак.ч	ЛР, ак.ч	ПЗ, ак.ч	СР, ак.ч
1	Общие сведения о программных и программно-аппаратных методах и средствах обеспечения информационной безопасности	2	6	6	11,15
2	Разграничение доступа	5	12	12	10
3	Аутентификация	6	12	12	11
4	Подсистема регистрации и учета	8	12	12	18
5	Защита программ и данных от несанкционированного копирования	7	12	12	18
6	Защита от вредоносных воздействий компьютерных вирусов и программных закладок	5	12	12	17,1
	Консультации текущие	1,65			
	Консультации перед экзаменом	2			
	Зачет, экзамен	0,3			

5.2.1 Лекции

№ п/п	Наименование раздела дисциплины	Тематика лекционных занятий	Трудоемкость, ак. ч
1	Общие сведения о программных и программно-аппаратных методах и средствах обеспечения информационной безопасности	Цели и задачи курса. Содержание дисциплины. Рекомендуемая литература. Основные понятия и определения. Роль и место знаний по дисциплине «Программно-аппаратные средства обеспечения информационной безопасности» при освоении смежных дисциплин по выбранной специальности; в сфере профессиональной деятельности. Роль и место программно-аппаратных средств защиты информации в обеспечении информационной безопасности. Предмет и задачи программно-аппаратной защиты информации. Современный уровень и перспективы развития программно-аппаратных средств обеспечения информационной безопасности.	2
2	Разграничение доступа	Избирательное разграничения доступа. Понятие матрицы доступа. Два подхода к кодированию матрицы доступа: векторы и списки. Изолированная программная среда. Полномочное разграничение доступа. Средства динамического изменения полномочий пользователя: необходимость, различные подходы к реализации.	5
3	Аутентификация	Правила безопасного хранения эталонной копии аутентификационной информации. Правила безопасной передачи по каналам связи аутентификационной информации. Понятие о специализированных сетевых протоколах безопасной аутентификации (Kerberos и т.п.). Проблемы парольной аутентификации. Методы подбора пароля. Средства защиты от подбора и компрометации паролей. Особенности аутентификации с использованием внешних носителей информации. Проблемы генерации и распределения ключей. Особенности биометрической аутентификации. Особенности аутентификации в системах управления базами данных. Реализация подсистем аутентификации в распространенных операционных системах.	6
4	Подсистема регистрации и учета	Необходимость регистрации и учета событий в защищенной автоматизированной системе. Основные требования к политике аудита. Требования к организации подсистемы аудита, к политике аудита. Настройка политики аудита в распространенных операционных системах.	8
5	Защита программ и данных от несанкционированного копирования	Задача защиты от несанкционированного копирования. Методы привязки к программно-аппаратной среде. Применение специальных аппаратных устройств (электронных ключей и т.п.) для защиты от несанкционированного копирования информации. Основные методы взлома систем защиты программ и данных от несанкционированного копирования: программная эмуляция эталонной программно-аппаратной среды, непосредственный взлом системы защиты («выкусывание» защитного кода).	7
6	Защита от вредоносных воздействий компьютерных вирусов и программных закладок	Основные типы компьютерных вирусов: файловые, сетевые, почтовые, макровирусы. Основные модели программных закладок: наблюдатель, перехват, искажение. Типичные признаки присутствия в системе компьютерных вирусов и программных закладок. Основные средства и методы противодействия компьютерным вирусам и программным закладкам: сигнатурное и эвристическое сканирование, контроль целостности, антивирусный мониторинг. Факторы, ограничивающие эффективность антивирусных средств.	5

5.2.2 Практические занятия

№	Наименование раздела дисциплины	Тематика практических занятий	Трудоемкость, ак. ч
1	Общие сведения о программных и программно-аппаратных методах и средствах обеспечения информационной безопасности	Администрирование, политики и компоненты системы безопасности в операционных системах семейства Windows.	6
2	Разграничение доступа	Разграничение доступа в операционных системах семейства Windows.	12
3	Аутентификация	Инструментальные средства настройки политики безопасности в ОС семейства Windows.	12
4	Подсистема регистрации и учета	Система защиты информации от несанкционированного доступа «Страж NT»	12
5	Защита программ и данных от несанкционированного копирования	Архитектура и функционирование шифрующей файловой системы EFS в ОС семейства Windows.	12
6	Защита от вредоносных воздействий компьютерных вирусов и программных закладок	Настройка системы аудита в ОС Windows.	12

5.2.3 Лабораторный практикум

№ п/п	Наименование раздела дисциплины	Тематика лабораторных занятий	Трудоемкость, ак. ч
1	Общие сведения о программных и программно-аппаратных методах и средствах обеспечения информационной безопасности	Администрирование, политики и компоненты системы безопасности в операционных системах семейства Windows	6
2	Разграничение доступа	Разграничение доступа в операционных системах семейства Windows	12
3	Аутентификация	Инструментальные средства настройки политики безопасности в ОС семейства Windows	12
4	Подсистема регистрации и учета	Контроль полномочий доступа к информационным ресурсам (Ревизор)	12
5	Защита программ и данных от несанкционированного копирования	Работа с программами защиты от несанкционированного копирования	12
6	Защита от вредоносных воздействий компьютерных вирусов и программных закладок	Работа с распространенными антивирусными средствами	12

5.2.4 Самостоятельная работа обучающихся (СРО)

№ п/п	Наименование раздела дисциплины	Вид СРО	Трудоемкость, ак. ч
1	Общие сведения о программных и программно-аппаратных методах и средствах обеспечения информационной безопасности	Проработка материалов по лекциям, учебникам, учебным пособиям	3,15
		Подготовка к практическим и лабораторным занятиям	2
		Домашнее задание	3
		Подготовка к коллоквиуму	3

2	Разграничение доступа	Проработка материалов по лекциям, учебникам, учебным пособиям	2
		Подготовка к практическим и лабораторным занятиям	2
		Домашнее задание	3
		Подготовка к коллоквиуму	3
3	Аутентификация	Проработка материалов по лекциям, учебникам, учебным пособиям	2
		Подготовка к практическим и лабораторным занятиям	3
		Домашнее задание	4
		Подготовка к коллоквиуму	2
4	Подсистема регистрации и учета	Проработка материалов по лекциям, учебникам, учебным пособиям	4
		Подготовка к практическим и лабораторным занятиям	4
		Домашнее задание	6
		Подготовка доклада	4
5	Защита программ и данных от несанкционированного копирования	Проработка материалов по лекциям, учебникам, учебным пособиям	4
		Подготовка к практическим и лабораторным занятиям	4
		Домашнее задание	6
		Подготовка доклада	4
6	Защита от вредоносных воздействий компьютерных вирусов и программных закладок	Проработка материалов по лекциям, учебникам, учебным пособиям	4,1
		Подготовка к практическим и лабораторным занятиям	3
		Домашнее задание	8
		Подготовка доклада	2

6 Учебно-методическое и информационное обеспечение дисциплины

6.1. Основная литература

1. Программно-аппаратные средства защиты информации : учебное пособие / Л. Х. Мифтахова, А. Р. Касимова, В. Н. Красильников [и др.]. – Санкт-Петербург : Интермедия, 2018. – 408 с. – ISBN 978-5-4383-0157-8. – Текст : электронный // Лань : электронно-библиотечная система. – URL: https://e.lanbook.com/book/103200

2. Маршаков, Д. В. Программно-аппаратные средства защиты информации : учебное пособие / Д. В. Маршаков, Д. В. Фатхи. – Ростов-на-Дону : Донской ГТУ, 2021. – 228 с. – ISBN 978-5-7890-1878-1. – Текст : электронный // Лань : электронно-библиотечная система. – URL: https://e.lanbook.com/book/237770

3. Фомин, Д. В. Информационная безопасность и защита информации: специализированные аттестованные программные и программно-аппаратные средства : методические указания / Д. В. Фомин. – Благовещенск : АмГУ, 2017. – 240 с. – Текст : электронный // Лань : электронно-библиотечная система. – URL: https://e.lanbook.com/book/156494

4. Костин, В. Н. Методы и средства защиты компьютерной информации: аппаратные и программные средства защиты информации : учебное пособие / В. Н. Костин. – Москва : МИСИС, 2018. – 21 с. – ISBN 978-5-906953-22-3. – Текст : электронный // Лань : электронно-библиотечная система. – URL: https://e.lanbook.com/book/116744

6.2. Дополнительная литература

1. Защита программ и данных : учебное пособие. – Санкт-Петербург : СПбГУТ им. М.А. Бонч-Бруевича, 2020 – Часть 2 : Способы защиты анализа – 2020. – 52 с. – Текст : электронный // Лань : электронно-библиотечная система. – URL: https://e.lanbook.com/book/180082

2. Защита программ и данных : учебное пособие. – Санкт-Петербург : СПбГУТ им. М.А. Бонч-Бруевича, 2020 – Часть 1 : Способы анализа – 2020. – 72 с. – Текст : электронный // Лань : электронно-библиотечная система. – URL: https://e.lanbook.com/book/180081

3. Программно-аппаратные средства защиты информации : учебно-методическое пособие / С. И. Штеренберг, А. М. Гельфанд, Д. В. Рыжаков, Р. А. Фатхутдинов. – Санкт-Петербург : СПбГУТ им. М.А. Бонч-Бруевича, 2017. – 98 с. – Текст : электронный // Лань : электронно-библиотечная система. – URL: https://e.lanbook.com/book/180093

4. Воробьева, А. А. История развития программно–аппаратных средств защиты информации : учебное пособие / А. А. Воробьева, И. С. Пантюхин. – Санкт-Петербург : НИУ ИТМО, 2017. – 62 с. – Текст : электронный // Лань : электронно-библиотечная система. – URL: https://e.lanbook.com/book/110499

6.3 Перечень учебно-методического обеспечения для самостоятельной работы обучающихся

1. 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

2. Программно-аппаратные средства обеспечения информационной безопасности [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. - 20 с. http://biblos.vsuet.ru/ProtectedView/Book/ViewBook/1420

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

При изучении дисциплины используется программное обеспечение, современные профессиональные базы данных и информационные справочные системы: ЭИОС университета, в том числе на базе программной платформы «Среда электронного обучения 3KL», автоматизированная информационная база «Интернет-тренажеры», «Интернет-экзамен» и др.

При освоении дисциплины используется лицензионное и открытое программное обеспечение – ОС Microsoft Windows, ОС ALT Linux, Microsoft Office Professional Plus, VMWare Player, Oracle VM VirtualBox.

Блок управления комплекса радиоконтроля и поиска радиопередающих устройств

«ОМЕГА» (переносной), МУ защиты ресурсов сети от внутренних и внешних атак CISCO ASA5505-KB, переносной комплекс для автоматизации измерений при проведении исследований и контроля технических средств ЭВТ «НАВИГАТОР-ПЗГ»; средство активной защиты информации от утечки за счет побочных электромагнитных излучений и наводок «СОНАТА-РЗ.1»; система защиты речевой информации «Соната-АВ-4Б» (Центральный блок питания и управления + Размыкатели в составе СВАЗ Соната АВ); профессиональный обнаружитель скрытых видеокамер СОКОЛ-М (переносной); портативный обнаружитель закладок Protect1203 (переносной); устройство активной защиты информации «ВЕТО-М»; электронный замок Samsung SHS-2920. Страж NT вер.3.0 Сертификат ФСТЭК № 2145 30.07.2013 г.; Ревизор 1XP Сертификат ФСТЭК № 989 08.02.2015 г.; Ревизор 2XP Сертификат ФСТЭК № 990 08.02.2015 г.; Фикс 2.0.2 Сертификат ФСТЭК №1548 15.01.2015 г.; Ревизор сети вер.3.0 Сертификат ФСТЭК №3413 02.06.2015 г.; СЗИ Панцирь К Сертификат ФСТЭК №1973 09.12.2015 г.; СЗИ Dallas Lock 8.0 К Сертификат ФСТЭК №2720 25.09.2015; СЗИ Dallas Lock 8.0 С Сертификат ФСТЭК №2945 16.08.2013.

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. Меди-

		аплеер 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:

- 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».

ОЦЕНОЧНЫЕМАТЕРИАЛЫ

ДЛЯ ПРОМЕЖУТОЧНОЙ АТТЕСТАЦИИ

по дисциплине

Программно-аппаратные средства обеспечения информационной безопасности

1 Перечень компетенций с указанием этапов их формирования

№ п/п	Код компетенции	Формулировка компетенции	Код и наименование индикатора достижения компетенции
1	ОПК-15	Способностью осуществлять администрирование и контроль функционирования средств и систем защиты информации автоматизированных систем, инструментальный мониторинг защищенности автоматизированных систем	ИД1$_{ОПК-15}$ – обладает способностью применять специализированные технические средства защиты информации, администрирование программного обеспечения в автоматизированных системах
			ИД2$_{ОПК-15}$ – обладает способностью осуществлять инструментальный мониторинг защищенности автоматизированных систем при помощи методов и технологий защиты информации

Код и наименование индикатора достижения компетенции	Результаты обучения (показатели оценивания)
ИД1$_{ОПК-15}$ – обладает способностью применять специализированные технические средства защиты информации, администрирование программного обеспечения в автоматизированных системах	Знает: основные средства и способы обеспечения информационной безопасности
	Умеет: проектировать и администрировать компьютерные сети
	Владеет: навыками использования программно - аппаратных средств обеспечения безопасности компьютерных сетей
ИД2$_{ОПК-15}$ – обладает способностью осуществлять инструментальный мониторинг защищенности автоматизированных систем при помощи методов и технологий защиты информации	Знает: принципы построения систем защиты информации при помощи методов и технологий защиты информации
	Умеет: осуществлять инструментальный мониторинг безопасности компьютерной сети
	Владеет: навыками эксплуатации программно-аппаратных средств обеспечения автоматизированных систем

2 Паспорт оценочных материалов по дисциплине

№ п/п	Разделы дисциплины	Код и наименование индикатора достижения компетенции	Оценочные материалы		Технология/процедура оценивания (способ контроля)
			наименование	№№ заданий	
1	Общие сведения о программных и программно-аппаратных методах и средствах обеспечения информационной безопасности	ИД1$_{ОПК-15}$ – обладает способностью применять специализированные технические средства защиты информации, администрирование программного обеспечения в автоматизированных системах	Вопросы к экзамену	1-80	Проверка преподавателем (уровневая шкала)
			Банк тестовых заданий	81-90	Бланочное тестирование (процентная шкала)
			Задания для практических работ	91-100	Проверка преподавателем (уровневая шкала)
			Домашнее задание	101-110	Проверка преподавателем (уровневая шкала)
2	Разграничение доступа	ИД1$_{ОПК-15}$ – обладает способностью применять специализированные технические средства защиты информации, администрирование программного обеспечения в автоматизированных системах	Вопросы к экзамену	1-80	Проверка преподавателем (уровневая шкала)
			Банк тестовых заданий	81-90	Бланочное тестирование (процентная шкала)
			Задания для практических работ	91-100	Проверка преподавателем (уровневая шкала)
			Домашнее задание	101-110	Проверка преподавателем (уровневая шкала)
3	Разграничение доступа	ИД1$_{ОПК-15}$ – обладает способностью применять специали-	Вопросы к экзамену	1-80	Проверка преподавателем (уровневая шкала)
			Банк тестовых заданий	81-90	Бланочное тестирование (процентная шкала)

		зированные технические средства защиты информации, администрирование программного обеспечения в автоматизированных системах	Задания для практических работ	91-100	Проверка преподавателем (уровневая шкала)
			Домашнее задание	101-110	Проверка преподавателем (уровневая шкала)
4	Аутентификация	ИД1$_{ОПК-15}$ – обладает способностью применять специализированные технические средства защиты информации, администрирование программного обеспечения в автоматизированных системах	Вопросы к экзамену	1-80	Проверка преподавателем (уровневая шкала)
			Банк тестовых заданий	81-90	Бланочное тестирование (процентная шкала)
			Задания для практических работ	91-100	Проверка преподавателем (уровневая шкала)
			Домашнее задание	101-110	Проверка преподавателем (уровневая шкала)
	Подсистема регистрации и учета	ИД1$_{ОПК-15}$ – обладает способностью применять специализированные технические средства защиты информации, администрирование программного обеспечения в автоматизированных системах	Вопросы к экзамену	1-80	Проверка преподавателем (уровневая шкала)
			Банк тестовых заданий	81-90	Бланочное тестирование (процентная шкала)
			Задания для практических работ	91-100	Проверка преподавателем (уровневая шкала)
			Домашнее задание	101-110	Проверка преподавателем (уровневая шкала)
	Защита программ и данных от несанкционированного копирования	ИД2$_{ОПК-15}$ – обладает способностью осуществлять инструментальный мониторинг защищенности автоматизированных систем при помощи методов и технологий защиты информации	Вопросы к экзамену	1-80	Проверка преподавателем (уровневая шкала)
			Банк тестовых заданий	81-90	Бланочное тестирование (процентная шкала)
			Задания для практических работ	91-100	Проверка преподавателем (уровневая шкала)
			Домашнее задание	101-110	Проверка преподавателем (уровневая шкала)

	Защита от вредоносных воздействий компьютерных вирусов и программных закладок	ИД2$_{ОПК-15}$ – обладает способностью осуществлять инструментальный мониторинг защищенности автоматизированных систем при помощи методов и технологий защиты информации	Вопросы к экзамену	1-80	Проверка преподавателем (уровневая шкала)
			Банк тестовых заданий	81-90	Бланочное тестирование (процентная шкала)
			Задания для практических работ	91-100	Проверка преподавателем (уровневая шкала)
			Домашнее задание	101-110	Проверка преподавателем (уровневая шкала)

3 Оценочные материалы для промежуточной аттестации

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

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

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

Каждый билет включает 3 контрольных вопроса, из них:

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

3.1 Вопросы к экзамену.

ОПК-15 Способностью осуществлять администрирование и контроль функционирования средств и систем защиты информации автоматизированных систем, инструментальный мониторинг защищенности автоматизированных систем (ИД1$_{ОПК-15}$ – обладает способностью применять специализированные технические средства защиты информации, администрирование программного обеспечения в автоматизированных системах, ИД2$_{ОПК-15}$ – обладает способностью осуществлять инструментальный мониторинг защищенности автоматизированных систем при помощи методов и технологий защиты информации).

№ задания	Формулировка вопроса
1	Дайте определение понятию компьютерной безопасности?
2	Назовите ключевые аспекты информационной безопасности?
3	Проведите содержательный анализ понятия "информация".
4	Дайте определение понятию конфиденциальность информации.
5	Дайте определение понятию целостность информации.
6	Дайте определение понятию доступность информации.
7	Назовите основные принципы создания и эксплуатации защищенных компьютерных систем (в которых обеспечивается безопасность информации).
8	Назовите методы и механизмы, непосредственно обеспечивающие конфиденциальность, целостность и доступность данных и дайте их характеристику.
9	Назовите методы и механизмы обеспечения компьютерной безопасности общесистемного характера и дайте их характеристику.
10	Назовите методы и механизмы обеспечения компьютерной безопасности инфраструктурного характера и дайте их характеристику.
11	Назовите методы и механизмы обеспечения компьютерной безопасности обеспечивающего (профилактирующего) характера и дайте их характеристику.
12	Дайте определение понятию угроза безопасности компьютерной системы.
13	Перечислите основные типы источников угроз безопасности компьютерной системы и дайте им характеристику.

14	Перечислите основные типы уязвимостей компьютерной системы и дайте им характеристику.
15	Перечислите основные типы каналов реализации угроз безопасности компьютерной системы и дайте им характеристику.
16	Перечислите основные типы источников угроз безопасности компьютерной системы и дайте им характеристику.
17	Перечислите основные типы ущербов от угроз безопасности компьютерной системы и дайте им характеристику.
18	Перечислите существующие в настоящее время отечественные и международные базы знаний уязвимостей программных систем.
19	Перечислите базовые метрики калькулятора опасности уязвимостей CVSS V2 ФСТЭК России.
20	Перечислите временные метрики калькулятора опасности уязвимостей CVSS V2 ФСТЭК России.
21	Перечислите контекстные метрики калькулятора опасности уязвимостей CVSS V2 ФСТЭК России.
22	Дайте определение понятию политика безопасности компьютерной системы.
23	Дайте определение понятию модель безопасности компьютерной системы.
24	Перечислите основные задачи решаемые политикой безопасности компьютерной системы.
25	Перечислите составляющие субъектно-объектной модели компьютерной системы.
26	Дайте характеристику процедуре порождения субъектов доступа.
27	Дайте определение понятию потока информации между объектами доступа.
28	Дайте характеристику понятию функционально-ассоциированный объект.
29	Дайте характеристику понятию ассоциированные объекты-данные.
30	Дайте характеристику понятию информационный ресурс.
31	Дайте определение понятию доступ субъекта к объекту.
32	Дайте определение понятию правила разграничения доступа субъектов к объектам.
33	Перечислите аксиоматические условий функционирования и структуры защищенных компьютерных систем.
34	Дайте определение понятию монитора безопасности компьютерной системы.
35	Перечислите обязательные требования к монитору безопасности компьютерной системы и дайте им характеристику.
36	Обоснуйте требование наличия в защищенной компьютерной системе доверенного пользователя (администратора системы).
37	Дайте определение общего критерия безопасности компьютерной системы обеспечивающего гарантии выполнения политики безопасности.
38	Охарактеризуйте модель дискреционного доступа Хартсона.
39	Перечислите основные компоненты модели Харисона-Руззо-Ульмана (HRU-модель).
40	Перечислите и охарактеризуйте основные операторы дискреционной модели.
41	Сформулируйте основной критерий безопасности HRU модели.
42	Перечислите и охарактеризуйте основные операторы модели типизированной матрицы доступа.
43	Перечислите и охарактеризуйте основные операторы модели TAKE-GRANT.
44	Перечислите и охарактеризуйте основные операторы расширенной модели TAKE-GRANT.
45	Дайте определение неявного информационного потока.
46	Перечислите основные компоненты мандатной модели управления доступом.
47	Сформулируйте основные правила мандатной модели управления доступом гарантирующих безопасность компьютерной системы
48	Дайте определение понятию решетка уровней безопасности мандатной модели управления доступом.
39	Дайте определение понятию основной критерий безопасности мандатной модели управления доступом на основе понятий решетка и функция уровней безопасности.
50	Перечислите основные компоненты модели Белла-ЛаПадулы и охарактеризуйте их.
51	Сформулируйте основную теорему безопасности модели Белла-ЛаПадулы.
52	Сформулируйте проблему переходных процессов, изменяющих доверительные характеристики (уровни безопасности) субъектов и объектов доступа модели Белла-ЛаПадулы.
53	Сформулируйте концептуальное описание Z- системы МакЛина.
54	Сформулируйте определение понятия функции безопасного перехода модели Белла-ЛаПадулы.
55	Дайте определение критерия безопасности МакЛина.

56	Сформулируйте основные положения расширенной модели Белла-ЛаПадулы включающей методологию и техники совместного (группового) доступа.
57	Сформулируйте проблему "троянских программ" применительно к модели Белла-ЛаПадулы.
58	Сформулируйте общий принцип тематической политики безопасности.
59	Перечислите основные способы тематической классификации и дайте им характеристику.
60	Дайте определение общему правилу тематического доступа.
61	Дайте характеристику понятию решетки безопасности при тематическом доступе
62	Дайте определение понятию мультирубрицированный иерархический тематический классификатор.
63	Дайте определение понятию листовое тематическое множество.
64	Сформулируйте основные положения модели тематико-иерархического разграничения доступа.
65	Дайте определение понятию роль в ролевых моделях управления доступом (RBAC - модели).
66	Охарактеризуйте двухэтапную процедуру организации системы ролевого разграничения доступа.
67	Перечислите и охарактеризуйте основные компоненты формальной спецификации ролевой модели управления доступом.
68	Перечислите основные разновидности ролевых моделей управления доступом.
69	Сформулируйте определение основного критерия безопасности ролевого доступа.
70	Дайте характеристику иерархической системе ролей RBAC модели.
71	Дайте характеристику понятию статическое распределение обязанностей (взаимоисключающие роли)
72	Дайте характеристику понятию динамическое распределение обязанностей (взаимоисключающие роли)
73	Сформулируйте основные положения процедуры группирование ролей и полномочий.
74	Дайте определение понятию целостность информации.
75	Охарактеризуйте основные положения дискреционной модели обеспечения целостности Кларка-Вильсона
76	Сформулируйте основные правила функционирования системы гарантирующей целостность дискреционной модели управления доступом.
77	Охарактеризуйте основные положения мандатной модели обеспечения целостности Кена Биба
78	Приведите основные правила мандатной модели обеспечения целостности Кена Биба.
79	Охарактеризуйте метод совместного использования инверсных моделей Белла-ЛаПадулы и К.Биба на основе двух различных решеток безопасности.
80	Охарактеризуйте метод совместного использования инверсных моделей Белла-ЛаПадулы и К.Биба на основе одной общей решетки уровней безопасности (конфиденциальности/целостности)

3.2Тесты (тестовые задания)

ОПК-15 Способностью осуществлять администрирование и контроль функционирования средств и систем защиты информации автоматизированных систем, инструментальный мониторинг защищенности автоматизированных систем (ИД1$_{ОПК-15}$ – обладает способностью применять специализированные технические средства защиты информации, администрирование программного обеспечения в автоматизированных системах, ИД2$_{ОПК-15}$ – обладает способностью осуществлять инструментальный мониторинг защищенности автоматизированных систем при помощи методов и технологий защиты информации).

№ задания	Тестовое задание с вариантами ответов
81	Программно-аппаратные средства защиты информации — это сервисы безопасности, встроенные в... Куда? 1. системный блок **2. сетевые операционные системы** 3. Microsoft Office 2013 4. операционную систему MS DOS
82	Что относится к аппаратным средствам защиты информации? **1. электронные устройства** 2. электронно-механические устройства 3. механические средства

83	Под этим применительно к обеспечению информационной безопасности компьютерной сети, понимают однозначное распознавание уникального имени субъекта компьютерной сети. **1. аутентификация** 2. идентификация 3. протоколирование 4. аудит
84	Что является дополнительным методом защиты шифруемых данных и проверки их целостности **1. цифровая подпись** 2. аудит 3. протоколирование 4. ключ
85	Характеризуется тем, что при шифровании используются два ключа: первый ключ делается общедоступным (публичным) и используется для шифровки, а второй является закрытым (секретным) и используется для расшифровки 1. симметричное шифрование **2. ассиметричное шифрование** 3. цифровая подпись
86	Как называют средство разграничения доступа клиентов из одного сетевого множества к серверам, принадлежащим другому сетевому множеству. 1. экран 2. шлюз **3. файервол** 4. мост
87	Они проверяют используемые приложения, ищут «дыры», которыми могли бы воспользоваться хакеры, и предупреждают администратора о зонах риска системы. **1. сканеры безопасности** 2. брандмауэры 3. серверы
88	Это механизм активного анализа, который запускает имитации атак, тем самым проверяя уязвимость 1. зондирование **2. сканирование** 3. поиск 4. протоколирование
89	Что является одним из главных требований к современным сетевым сканерам уязвимостей, помимо собственно безопасности? **1. поддержка различных операционных систем** 2. способность обнаруживать все новые вирусы 3. мультиязычность
90	Где размещена информация на сертифицированные средства защиты информации? 1. на сайте Госстандарта России 2. на сайте Правительства России **3. на сайте ФСТЭК России** 4. на сайте Администрации Президента России

3.3 Задания для практических работ (типовые задачи)

ОПК-15 Способностью осуществлять администрирование и контроль функционирования средств и систем защиты информации автоматизированных систем, инструментальный мониторинг защищенности автоматизированных систем (ИД1$_{ОПК-15}$ – обладает способностью применять специализированные технические средства защиты информации, администрирование программного обеспечения в автоматизированных системах, ИД2$_{ОПК-15}$ – обладает способностью осуществлять инструментальный мониторинг защищенности автоматизированных систем при помощи методов и технологий защиты информации).

№ задания	Условие задачи (формулировка задания)
91	Пусть имеется два субъекта: s1 (доверенный пользователь, admin) и s2 (обычный пользователь, user). Пусть имеется два каталога (объекты) o1 и o2, владельцами которых являются пользователи s1 и s2, соответственно. В каталоге имеется объект o3 с секретной информацией.

	Права доступа в системе заданы исходным состоянием матрицы доступа: ***o***1- secret ***o***2 - no secret ***o***3 - secret ***s***1 *own,r,w,e* *r,w,e own,* *r,w,e* ***s***2 *own,r,w,e* Построить сценарий атаки с помощью троянской программы в системах, функционирующих на основе модели HRU
92	Пусть имеется два субъекта: s1 (доверенный пользователь, admin) и s2 (обычный пользователь, user). Пусть имеется два каталога (объекты) o1 и o2, владельцами которых являются пользователи s1 и s2, соответственно. В каталоге имеется объект o3 с секретной информацией. Права доступа в системе заданы исходным состоянием матрицы доступа: ***o***1- secret ***o***2 - no secret ***o***3 - secret ***s***1 *own,r,w,e* *r,* *r,w,e* ***s***2 *own,r,w,e* Построить сценарий атаки с помощью троянской программы в системах, функционирующих на основе модели HRU
93	Пусть в системе, функционирующей на основе модели с типизованной матрицей доступа, имеется три типа сущностей (субъектов и объектов доступа) – u, ω и ν . Пусть в начальном состоянии системы имеется субъект s1 типа u - (s1: u). Осуществляется переход системы в новое состояние посредством следующей команды: α(s1:u, s2:ω, o1:ν): Create object o1 of type ν ; Inter r into [s1, o1] ; Create subject s2 of type ω ; Inter r' into [s2, o1] ; Create subject s3 of type u ; Inter r'' into [s3, o1] ; end α при выполнении которой создается объект o1 типа ν, на него устанавливаются права r для субъекта s1, инициализируются дополнительные субъекты - s2 типа ω и s3 типа u, им предоставляются права доступа r' и на r'' объект o1, соответственно. Построить по команде α граф отношений наследственности.
94	Пусть в системе, функционирующей на основе модели с типизованной матрицей доступа TAM, имеется два субъекта доступа: субъект s1 типа a - (s1: a) доверенного пользователя (admin); субъект s2 типа u - (s2: u) обычного пользователя (user); а также три объекта доступа: каталог o1 типа ν (secret) – (o1: ν), владельцем которого является пользователь s1 ("own"∈ rs1,o1), несекретный каталог o2 типа η (no secret) – (o2: η), владельцем которого является пользователь s2 ("own"∈ rs2,o2), секретный файл o3 типа ν – (o3: ν) в каталоге o1, владельцем которого также является пользователь s1 ("own"∈ rs1,o3). Пользователь s1 имеет также права чтения, записи и запуска на объект o2 ({"read","write","execute"} ⊆ rs1,o2). В исходном состоянии Графа наследственности имеется четыре вершины. Построить граф отношений наследственности по сценарию атаки троянским конем со стороны пользователя s2 на секретный файл o3.
95	В системе, функционирующей на основе модели с типизованной матрицей доступа TAM и по условиям задачи **114**, предложить возможное разрешение проблемы атак троянским конем на основе ограничений на команды переходов по соотношению дочерних и родительских типов. Дайте физическое обоснование решения и подтвердите его на графе отношений наследственности.
96	Пусть имеется система субъектов и объектов доступа, представленная графом доступов Γ_0 (O, S, E), в которой сущности x и y связаны tg-путем. Построить систему команд перехода передачи субъекту x прав доступа α на объект s от субъекта y.
97	Для иллюстрации возможности передачи прав доступа по tg-пути независимо от направления прав t и g, изменяются в условиях задачи 116 направление права между субъектами s1 и s2. Задание: построить систему команд перехода передачи субъекту x прав доступа α на объект s от субъекта y.
98	Пусть имеется система субъектов и объектов доступа, представленная графом доступов Γ_0 (O, S, E). Установленная для системы политика безопасности запрещает любым субъектам (владельцам) предоставлять право α на "свои" объекты другим субъектам (но не запрещает субъектам, которые владеют правами t ("брать") на какие-либо субъекты брать у них права на их

	объекты). Кроме субъекта s, субъект u может быть связан tg-путем с другими субъектами. Построить систему команд получения субъектом s прав доступа α на объект w от субъекта u, при условии того, что команда grants(α, u, s, w) не может быть задействована.
99	Пусть имеется система субъектов и объектов доступа, представленная Графом доступов Γ_0 (O, S, E), Пусть неявные каналы чтения, генерируемые различными командами "де-факто" имеют следующую стоимость: - rspy = 1, rpost = 2, rfind = 3 и rpass = 4. Применяя команды "де-факто" сгенерировать все возможные неявные каналы чтения субъектом x информации из субъекта y, и сравнить их стоимость.
100	Пусть имеется система субъектов и объектов доступа, представленная Графом доступов Γ_0 (O, S, E), Пусть неявные каналы чтения, генерируемые различными командами "де-факто" имеют следующую стоимость: - rspy = 1, rpost = 2, rfind = 3 и rpass = 4. Построить систему команд получения субъектом s прав доступа α на объект w от субъекта u, при условии того, что команда grants(α, u, s, w) не может быть задействована.

3.4 Домашнее задание (типовые задачи)

ОПК-15 Способностью осуществлять администрирование и контроль функционирования средств и систем защиты информации автоматизированных систем, инструментальный мониторинг защищенности автоматизированных систем ($ИД1_{ОПК-15}$ – обладает способностью применять специализированные технические средства защиты информации, администрирование программного обеспечения в автоматизированных системах, $ИД2_{ОПК-15}$ – обладает способностью осуществлять инструментальный мониторинг защищенности автоматизированных систем при помощи методов и технологий защиты информации).

№ задания	Формулировка задания
101	Реферат на тему "Модели информационного невмешательства и информационной невыводимости"
102	Реферат на тему "Нейтрализация скрытых каналов утечки информации на основе технологий представлений и разрешенных процедур"
103	Реферат на тему " Технологии параллельного выполнения транзакций в клиент-серверных системах как модели обеспечения целостности данных"
104	Реферат на тему "Резервирование, архивирование и журнализация данных"
105	Реферат на тему "Технологии репликации данных"
106	Реферат на тему "Модели распределенных систем в процессах разграничения доступа"
107	Реферат на тему " Зональная модель разграничения доступа к информации в распределенных компьютерных системах "Теоретико-графовые модели комплексной оценки защищенности"
108	Реферат на тему " Теоретико-графовая модель системы индивидуальногрупповых назначений доступа к иерархически организованным объектам"
109	Реферат на тему "Пространственно-векторная модель и характеристики системы рабочих групп пользователей"
110	Реферат на тему "Модель разграничения доступа на основе идентификационных данных (Identity-based Access Control)"

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

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

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

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

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

Результаты обучения по этапам формирования компетенций	Предмет оценки (продукт или процесс)	Показатель оценивания	Критерии оценивания сформированности компетенций	Шкала оценивания	
				Академическая оценка или баллы	Уровень освоения компетенции
ОПК-15 Способностью осуществлять администрирование и контроль функционирования средств и систем защиты информации автоматизированных систем, инструментальный мониторинг защищенности автоматизированных систем					
ИД1$_{ОПК-15}$ – обладает способностью применять специализированные технические средства защиты информации, администрирование программного обеспечения в автоматизированных системах, ИД2$_{ОПК-15}$ – обладает способностью осуществлять инструментальный мониторинг защищенности автоматизированных систем при помощи методов и технологий защиты информации					
Знает: основные средства и способы обеспечения информационной безопасности Знает: принципы построения систем защиты информации при помощи методов и технологий защиты информации	Результаты текущего тестирования	Правильность ответов при тестировании	Обучающийся ответил на 85-100 % вопросов	Отлично	Освоена / повышенный
			Обучающийся ответил на 70-84 % вопросов	Хорошо	Освоена / повышенный
			Обучающийсяответил на 50-69 % вопросов	Удовлетворительно	Освоена / базовый
			Обучающийся ответил на 0-49 % вопросов	неудовлетворительно	Не освоена / недостаточный
	Вопросы к экзамену	Правильность ответов	Обучающийсядал исчерпывающий ответ на вопрос, не допустил ошибок. Студент владеет знаниями и умениями по дисциплине в полном объеме	Отлично	Освоена / повышенный
			Обучающийсядал подробный и полный ответ, допустил не более 1 ошибки. Студент владеет знаниями и умениями по дисциплине в полном объеме	Хорошо	Освоена / повышенный
			Обучающийсядал поверхностный ответ на вопрос, допустил более 2 ошибок	Удовлетворительно	Освоена / базовый
			Обучающийсяне смог правильно ответить на вопрос, допустил ошибку в анализе задания	неудовлетворительно	Не освоена / недостаточный
Умеет: проектировать и администрировать компьютерные сети Умеет: осуществлять инструментальный мониторинг безопасности компьютерной сети	Задания для практических работ	Правильность и полнота выполнения задания	Обучающийся правильно выбрал инструменты для решения задачи, систематизировал и наглядно представил полученные данные, сделал развернутые выводы	Отлично	Освоена / повышенный
			Обучающийся правильно выбрал инструменты для решения задачи, систематизировал и наглядно представил полученные данные, сделал краткие выводы	Хорошо	Освоена / повышенный
			Обучающийся правильно выбрал инструменты для решения задачи, но не смог грамотно их применить, выводы отсутствуют	Удовлетворительно	Освоена / базовый

			Обучающийся не смог правильно выбрать инструменты для решения задачи	неудовлетворительно	Не освоена / недостаточный
Владеет: навыками использования программно - аппаратных средств обеспечения безопасности компьютерных сетей Владеет: навыками эксплуатации программно-аппаратных средств обеспечения автоматизированных систем	Домашнее задание	Правильность и полнота выполнения задания	Обучающийся разносторонне проанализировал ситуацию, выбрал верную методику решения, сделал развернутые выводы, не допустил ошибок в расчетах	Отлично	Освоена / повышенный
			Обучающийся разносторонне проанализировал ситуацию, полностью выполнил задание, сделал вывод, допустил не более 1 ошибки в расчетах	Хорошо	Освоена / повышенный
			Обучающийся поверхностно проанализировал ситуацию, выполнил задание, сделал вывод, допустил не более 2 ошибок в расчетах	Удовлетворительно	Освоена / базовый
			Обучающийся не смог правильно решить задачу, допустил ошибку в анализе ситуации	неудовлетворительно	Не освоена / недостаточный