УТВЕРЖДАЮ:
Директор института ИРИТ

_____Мякиньков А.В.
«03» июня 2024 г.

Лист актуализации рабочей программы дисциплины
«Б1.Б.39 Программно-аппаратные средства защиты информации»
индекс по учебному плану, наименование

для подготовки **специалистов**
Направление: 10.05.03 «Информационная безопасность автоматизированных систем»
Направленность: Безопасность открытых информационных систем
Форма обучения: очная
Год начала подготовки: 2023, 2024
Курс 4
Семестр 8

В рабочую программу 2022 г. вносятся изменения:

1) Таблицу 7.1 читать в следующей редакции:

№	Наименование ЭБС	Ссылка к ЭБС
1	Консультант студента	http://www.studentlibrary.ru/
2	Лань	https://e.lanbook.com/
3	Юрайт	https://biblio-online.ru/
4	TNT-ebook	https://www.tnt-ebook.ru/

2) Пункт 9 читать в следующей редакции:

Для контактной и самостоятельной работы обучающихся выделены помещения, оснащённые компьютерной техникой с подключением к сети "Интернет" и обеспечением доступа в электронную информационно-образовательную среду организации:

Наименование помещений для проведения всех видов учебной деятельности, предусмотренной учебным планом образовательной программы, в том числе помещения для самостоятельной работы, с указанием перечня основного оборудования, учебно-наглядных пособий и используемого программного обеспечения	Адрес места нахождения помещений для проведения всех видов учебной деятельности, предусмотренной учебным планом образовательной программы
Лаборатория «Программно-аппаратных средств и технической защиты информации» №6039 учебно-лабораторного корпуса №6 для проведения учебных занятий **Оснащенность оборудованием и техническими средствами обучения:** 1.Учебный лабораторный стенд "Блочное кодирование" – 1 шт. 2.Учебный лабораторный стенд "Основы криптографии" – 1 шт. 3.Учебный лабораторный стенд "Биометрическая аутентификация" – 2 шт. 4.Учебный лабораторный стенд "Доверенная загрузка (Соболь)" – 1	603163, Нижегородская область, г. Нижний Новгород, Казанское шоссе, д.12

шт. 5.Учебный лабораторный стенд "Доверенная загрузка (Аккорд)" – 1 шт. 6.Учебный лабораторный стенд "Криптоконтейнеры и ЭЦП" – 2 шт. 7. Для ивалидов и лиц с ОВЗ: переносной радиокласс, клавиатура адаптированная 8. МФУ Brother LC 9. Посадочных мест - 16. **Программное обеспечение:** Распространяемое по свободной лицензии: 1.Операционная система Ubuntu Linux 20 2. GNS3 3. Snort 4. Wareshark 5. OpenVPN 6. Libre Office 7. OpenVPN 8. IP scanner	
Мультимедийная аудитория №6421 учебно-лабораторного корпуса №6 для проведения учебных занятий **Оснащенность оборудованием и техническими средствами обучения:** 1. Доска меловая – 1 шт. 3. Экран – 1 шт. 4. Мультимедийный проектор Epson X12 – 1 шт. 5. Компьютер PC MB Asus на чипсете Nvidia/AMDAthlonXII CPU 2.8Ggz/ RAM 4 Ggb/SVGAStandartGraphics +Ge-FORCE Nvidia GT210/HDD 250Ggb,SATAinterface, монитор 19”, с выходом на проектор. 6. Рабочее место студента - 30 7. Рабочее место для преподавателя – 1 шт. **Программное обеспечение:** 1. Windows 7 32 bit корпоративная; VL 49477S2 2. Adobe Acrobat Reader DC-Russian (беспл.) 3. Microsoft Office Professional Plus 2007 (лицензия № 42470655); 4. Dr.Web (С/н ZNFC-CR5D-5U3U-JKGP от 20.05.2024, до 30.05.25)	603163, Нижегородская область, г. Нижний Новгород, Казанское шоссе, д.12

Программа 2022 г. актуализирована для 2023, 2024 г. начала подготовки.

Разработчик (и): __Капранов С.Н., к.т.н., доцент_____
(ФИО, ученая степень, ученое звание)

«_17_»_05___2024г.

Рабочая программа пересмотрена и одобрена на заседании кафедры ИБВСС протокол № _9___ от «_17_» ___05___2024_г.

И.о. заведующий кафедрой _____Ляхманов Д.А.

Лист актуализации принят на хранение:

Заведующий выпускающей кафедрой ИБВСС _____«03» июня 2024 г.

Методический отдел УМУ:_____ «03» июня 2024 г.

МИНОБРНАУКИ РОССИИ
федеральное государственное бюджетное образовательное учреждение
высшего образования
«Нижегородский государственный технический университет
им. Р.Е. Алексеева» (НГТУ)

Учебно-научный институт радиоэлектроники и информационных технологий (ИРИТ)
(Полное и сокращенное название института, реализующего данное направление)

УТВЕРЖДАЮ:
Директор института:
_____ Мякиньков А.В.
подпись ФИО
22 апреля 2023г

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ

Б1.Б.39 Программно-аппаратные средства защиты информации
(индекс и наименование дисциплины по учебному плану)
для подготовки специалистов

Направление подготовки: 10.05.03 «Информационная безопасность автоматизированных систем»

Направленность: Безопасность открытых информационных систем

Форма обучения: очная
Год начала подготовки 2022

Выпускающая кафедра ИБВСС

Кафедра-разработчик ИБВСС

Объем дисциплины 108/3
часов/з.е
Промежуточная аттестация Зачет

Разработчик: Капранов С.Н., к.т.н., доцент

Нижний Новгород

2023 г

Рабочая программа дисциплины: разработана в соответствии с Федеральным государственным образовательным стандартом высшего образования (ФГОС ВО 3++) по направлению подготовки «Информационная безопасность автоматизированных систем», утвержденного приказом МИНОБРНАУКИ РОССИИ от 26 ноября 2020 г. № 1457 на основании учебного плана, принятого УМС НГТУ

протокол от 20.04.2023 № 18.

Рабочая программа одобрена на заседании кафедры протокол от _01.04.2023_ № 4
Зав. кафедрой к.т.н, доцент Ляхманов Д,А. _____
(подпись)

Программа рекомендована к утверждению ученым советом института ИРИТ, Протокол от 21.04.2023_____№_4_

Рабочая программа зарегистрирована в УМУ, регистрационный № 10.05.03-б-38
Начальник МО _____ Н.Р. Булгакова

Заведующая отделом комплектования НТБ _____ Н.И. Кабанина
(подпись)

СОДЕРЖАНИЕ

1. ЦЕЛИ И ЗАДАЧИ ОСВОЕНИЯ ДИСЦИПЛИНЫ

1.1 Цель освоения дисциплины

Целью освоения дисциплины является освоение дисциплинарных компетенций в области защиты информации в компьютерных системах при помощи программно-аппаратных средств.

1.2 Задачи освоения дисциплины (модуля)

Дисциплина «Программно-аппаратные средства защиты информации» способствует подготовке студентов к решению следующих профессиональных задач:

1. Изучение программно-аппаратных средств, реализующих отдельные функциональные требования по защите;
2. Исследование методов и средств хранения ключевой информации;
3. Исследование методов и средств ограничения доступа к компонентам вычислительных систем;
4. Исследование методов защиты от вредоносных программ;
5. Исследование методов защиты программ от изменения и контролю целостности;
6. Освоение технологии сертификации программно-аппаратных средств на соответствие требованиям информационной безопасности.

2. МЕСТО ДИСЦИПЛИНЫ В СТРУКТУРЕ ОБРАЗОВАТЕЛЬНОЙ ПРОГРАММЫ

Учебная дисциплина «Программно-аппаратные средства защиты информации» Б1.Б.39 включена в обязательный перечень дисциплин обязательной части образовательной программы вне зависимости от ее направленности (профиля). Дисциплина реализуется в соответствии с требованиями ФГОС, ОП ВО и УП, по направлению подготовки 10.05.03.

Дисциплина относиться к дисциплинам блока защиты информации программы специалитета и базируется на дисциплине «Методы и средства криптографической защиты информации».

Дисциплина «Программно-аппаратные средства защиты информации» является основополагающей для прохождения практики: преддипломная.

3. КОМПЕТЕНЦИИ ОБУЧАЮЩЕГОСЯ, ФОРМИРУЕМЫЕ В РЕЗУЛЬТАТЕ ОСВОЕНИЯ ДИСЦИПЛИНЫ (МОДУЛЯ)[1]

Дисциплина «Программно-аппаратные средства защиты информации» формирует компетенцию ОПК-5.2, ОПК-5.3, ОПК-10, ОПК-15 совместно с дисциплинами и практиками, указанными в таблице 3.1.

Таблица 3.1 - Формирование компетенций дисциплинам

Наименование дисциплин, формирующих компетенцию совместно	Семестры, формирования дисциплины Компетенции берутся из Учебного плана по направлению подготовки специалиста»										
	1	*2*	*3*	*4*	*5*	*6*	*7*	*8*	*9*	*10*	*11*
ОПК-5.2 (Способен разрабатывать и эксплуатировать системы защиты информации открытых информационных систем)											
Защита программ и данных											
Программно-аппаратные средства защиты информации											
Подготовка и защита ВКР											

Наименование дисциплин, формирующих компетенцию совместно	Семестры, формирования дисциплины Компетенции берутся из Учебного плана по направлению подготовки специалиста»										
	1	*2*	*3*	*4*	*5*	*6*	*7*	*8*	*9*	*10*	*11*
ОПК-5.3 (Способен осуществлять контроль обеспечения информационной безопасности и проводить верификацию данных в открытых информационных системах)											
Методы и средства криптографической защиты информации											
Программно-аппаратные средства защиты информации											
Подготовка и защита ВКР											

Наименование дисциплин, формирующих компетенцию совместно	Семестры, формирования дисциплины Компетенции берутся из Учебного плана по направлению подготовки специалиста»										
	1	*2*	*3*	*4*	*5*	*6*	*7*	*8*	*9*	*10*	*11*
ОПК-10 (Способен использовать средства криптографической защиты информации при решении задач профессиональной деятельности)											
Методы и средства криптографической защиты информации											
Программно-аппаратные средства защиты информации											
Подготовка и защита ВКР											

Наименование дисциплин, формирующих компетенцию совместно	Семестры, формирования дисциплины Компетенции берутся из Учебного плана по направлению подготовки специалиста»										
	1	*2*	*3*	*4*	*5*	*6*	*7*	*8*	*9*	*10*	*11*

Наименование дисциплин, формирующих компетенцию совместно	Семестры, формирования дисциплины Компетенции берутся из Учебного плана по направлению подготовки специалиста»										
	1	*2*	*3*	*4*	*5*	*6*	*7*	*8*	*9*	*10*	*11*
ОПК-15 (Способен осуществлять администрирование и контроль функционирования средств и систем защиты информации автоматизированных систем, инструментальный мониторинг защищенности автоматизированных систем)											
Защита информации от утечек по техническим каналам											
Программно-аппаратные средства защиты информации											
Подготовка и защита ВКР											

Таблица 3.2 - Перечень планируемых результатов обучения по дисциплине, соотнесенных с планируемыми результатами освоения

Код и наименование компетенции	**Код и наименование индикатора достижения компетенции**	**Планируемые результаты обучения по дисциплине**			**Оценочные средства**	
					Текущего контроля	**Промежуточной аттестации**
ОПК-5.2 Способен разрабатывать и эксплуатировать системы защиты информации открытых информационных систем	ИОПК-5.2.1. Применяет программно-аппаратные комплексы защиты информации для обеспечения информационной безопасности в открытых информационных системах	***Знать:*** – программно-аппаратные средства обеспечения информационной безопасности; – особенности применения программных и программно-аппаратных средств защиты информации в открытых информационных системах;	***Уметь:*** – изучать новые образцы программно-аппаратные средства обеспечения информационной безопасности; – проводить выбор программно-аппаратных средств обеспечения информационной безопасности для обеспечения требуемого уровня защищенности открытой информационной системы; – конфигурирова	***Владеть:*** – навыками разработки архитектуры системы защиты информации открытой информационной системы; – навыками разработки программных и программно-аппаратных средств защиты информации открытых информационных систем.	Набор индивидуальных заданий (1-2) (лабораторных работ)	Набор экзаменационных билетов

			ть параметры системы защиты информации в соответствии с ее эксплуатационной документацией;			
ОПК-5.3. Способен осуществлять контроль обеспечения информационной безопасности и проводить верификацию данных в открытых информационных системах	ИОПК-5.3.2. Применяет программно-аппаратные комплексы защиты информации для контроля информационной безопасности в открытых информационных системах	***Знать:*** – программно-аппаратные средства обеспечения информационной безопасности; – особенности применения программных и программно-аппаратных средств защиты информации в открытых информационных системах; – основные категории требований к программной и программно-аппаратной реализации	***Уметь:*** – изучать новые образцы программно-аппаратных средств обеспечения информационной безопасности; – проводить выбор программно-аппаратных средств обеспечения информационной безопасности для обеспечения требуемого уровня защищенности открытой информационно	***Владеть:*** – навыками разработки архитектуры системы защиты информации открытой информационной системы; – навыками разработки программных и программно-аппаратных средств защиты информации открытых информационной систем. – методами и средствами контроля защищенности информации для	Набор индивидуальных заданий (1-2) (лабораторных работ)	Набор экзаменационных билетов

		средств обеспечения информационной безопасности.	й системы; –конфигурировать параметры системы защиты информации в соответствии с ее эксплуатационной документацией;	различных подсистем защиты		
ОПК-10. Способен использовать средства криптографической защиты информации при решении задач профессиональной деятельности	ИОПК-10.2. Применяет программно-аппаратные средства криптографической защиты информации для обеспечения секретности и целостности информации в открытых информационных системах	***Знать:*** программно - аппаратные криптографические средства обеспечения информационной безопасности (ИОПК-10.2.) – особенности применения программных и программно-аппаратных криптографических средств защиты информации в открытых информационных системах (ИОПК -10.2.)	***Уметь:*** - проводить выбор программно-аппаратных средств обеспечения информационной безопасности для обеспечения требуемого уровня защищенности открытой информационной системы (ИОПК-10.2.) ;	***Владеть:*** - методами и средства контроля защищенности информации для различных подсистем криптографических защиты информации(ИОПК-10.2.)	Набор индивидуальных заданий (1-2) (лабораторных работ)	Набор экзаменационных билетов

ОПК-15. Способен осуществлять администрирование и контроль функционирования средств и систем защиты информации автоматизированных систем, инструментальный мониторинг защищенности автоматизированных систем	ИОПК-15.1. Проводит контрольные проверки работоспособности применяемых программно-аппаратных, криптографических и технических средств защиты информации.	***Знать:*** -особенности администрирования программных и программно-аппаратных средств защиты информации в открытых информационных системах (ИОПК-15.1.)	***Уметь:*** - конфигурировать параметры системы защиты информации в соответствии с ее эксплуатационной документацией и проводить контрольные проверки работоспособности применяемых программно-аппаратных и криптографических средств защиты информации (ИОПК-15.1.);	***Владеть:*** - методами и средства контроля защищенности информации для различных подсистем защиты, в том числе программно-аппаратных и криптографических (ИОПК-15.1.)	Набор индивидуальных заданий (1-2) (лабораторных работ)	Набор экзаменационных билетов

4. СТРУКТУРА И СОДЕРЖАНИЕ ДИСЦИПЛИНЫ

4.1 Распределение трудоёмкости дисциплины по видам работ по семестрам

Общая трудоёмкость дисциплины составляет 3 зач. ед. 108 часов, распределение часов по видам работ семестрам представлено в таблице 4.1.

Таблица 4.1 - Распределение трудоёмкости дисциплины по видам работ по семестрам для студентов очного обучения

Вид учебной работы	**Трудоёмкость в час**	
	Всего час.	**В т.ч. по семестрам**
		8 сем
Формат изучения дисциплины	с использованием элементов электронного обучения	
Общая трудоёмкость дисциплины по учебному плану	**108**	**108**
1. Контактная работа:	**55**	**55**
1.1 Аудиторная работа, в том числе:	**51**	**51**
занятия лекционного типа (Л)	34	34
занятия семинарского типа (ПЗ-семинары, практ. занятия и др)		
лабораторные работы (ЛР)	17	17
1.2 Внеаудиторная, в том числе	**4**	**4**
курсовая работа (проект) (КР/КП) (консультация, защита)		
текущий контроль, консультации по дисциплине	4	4
контактная работа на промежуточном контроле (КРА)		
2. Самостоятельная работа (СРС)	**53**	**53**
реферат/эссе (подготовка)		
расчётно-графическая работа (РГР) (подготовка)		
контрольная работа		
курсовая работа/проект (КР/КП) (подготовка)		
самостоятельное изучение разделов, самоподготовка (проработка и повторение лекционного материала и материала учебников и учебных пособий, подготовка к лабораторным и практическим занятиям, коллоквиум и т.д.)	53	53
Подготовка к зачету	-	-

4.2 Содержание дисциплины, структурированное по темам

Таблица 4.1 - Содержание дисциплины, структурированное по темам для студентов очного обучения

Планируемые (контролируемые) результаты освоения: код УК; ОПК; ПК и индикаторы достижения компетенций	Наименование разделов, тем	Виды учебной работы (час)					Вид СРС	Наименование используемых активных и интерактивных образовательных технологий	Реализация в рамках Практической подготовки (трудоемкость в часах)	Наименование разработанного Электронного курса (трудоемкость в часах)
		Контактная работа				Самостоятельная работа студентов (час)				
		Лекции (час)	Лабораторные работы (час)	Практические занятия (час)	КСР					
Раздел 1. Теоретические аспекты применения программно-аппаратных средств обеспечения информационной безопасности										
ОПК-5.2 - ОПК-5.2.1 ОПК-5.3 - ОПК-5.3.2 ОПК-10 - ОПК-10.1 ОПК-15 - ОПК-15.1	**Тема 1.1** Понятие политики безопасности. Описание типовых политик безопасности. Угрозы безопасности компьютерных систем. Обеспечение гарантий выполнения политики безопасности.	4			1	2	Подготовка к лекциям [6.1.1]	Разбор конкретных ситуаций		
	Тема 1.2 Модель компьютерной системы. Понятие монитора безопасности. Концепция диспетчера доступа. Дискреционный доступ. Реализация разграничения доступа к внешним устройствам. Мандатный доступ, его	4				2	Подготовка к лекциям [6.1.1]			

Планируемые (контролируемые) результаты освоения: код УК; ОПК; ПК и индикаторы достижения компетенций	Наименование разделов, тем	Виды учебной работы (час)					Вид СРС	Наименование используемых активных и интерактивных образовательных технологий	Реализация в рамках Практической подготовки (трудоемкость в часах)	Наименование разработанного Электронного курса (трудоемкость в часах)
		Контактная работа				Самостоятельная работа студентов (час)				
		Лекции (час)	Лабораторные работы (час)	Практические занятия (час)	КСР					
	реализация для файлов, папок и процессов. Управление потоками информации. Метод генерации изолированной программной среды при проектировании механизмов гарантированного поддержания политики безопасности. Модели безопасного взаимодействия в КС. .									
	Тема 1.3 Процедура идентификации и аутентификации: защита на уровне расширений Bios, защита на уровне загрузчиков операционной среды	4				2	Подготовка к лекциям [6.1.1, 6.1.2, 6.1.3]			
	Итого по 1 разделу	**12**			**1**	**6**				
Раздел 2. Программно-аппаратные средства обеспечения информационной безопасности										

Планируемые (контролируемые) результаты освоения: код УК; ОПК; ПК и индикаторы достижения компетенций	Наименование разделов, тем	Виды учебной работы (час)					Вид СРС	Наименование используемых активных и интерактивных образовательных технологий	Реализация в рамках Практической подготовки (трудоемкость в часах)	Наименование разработанного Электронного курса (трудоемкость в часах)
		Контактная работа				Самостоятельная работа студентов (час)				
		Лекции (час)	Лабораторные работы (час)	Практические занятия (час)	КСР					
ОПК-5.2 - ОПК-5.2.1 ОПК-5.3 - ОПК-5.3.2 ОПК-10 - ОПК-10.1 ОПК-15 - ОПК-15.1	**Тема 2.1** Основные принципы создания программно-аппаратных средств обеспечения информационной безопасности. Программно-аппаратные средства, реализующие отдельные функциональные требования по защите, их принципы действия и технологические особенности. Взаимодействие с общесистемными компонентами вычислительных систем. Методы и средства ограничения доступа к компонентам вычислительных систем.	4		8		2	Подготовка к лекциям [6.1.1, 6.1.2, 6.1.3]	Разбор конкретных ситуаций	8	
	Тема 2.2 Методы и средства привязки	4			1	2	Подготовка к лекциям [6.1.1,			

Планируемые (контролируемые) результаты освоения: код УК; ОПК; ПК и индикаторы достижения компетенций	Наименование разделов, тем	Виды учебной работы (час)					Вид СРС	Наименование используемых активных и интерактивных образовательных технологий	Реализация в рамках Практической подготовки (трудоемкость в часах)	Наименование разработанного Электронного курса (трудоемкость в часах)
		Контактная работа				Самостоятельная работа студентов (час)				
		Лекции (час)	Лабораторные работы (час)	Практические занятия (час)	КСР					
	программного обеспечения к аппаратному окружению и физическим носителям. Управление ключами криптографическими ключами. Методы и средства хранения ключевой информации.						6.1.2, 6.1.3]			
	Тема 2.3 Защита программ от изучения. Способы встраивания средств защиты в программное обеспечение. Защита от разрушающих программных воздействий и вредоносного программного обеспечения. Защита программ от	4			1	2	Подготовка к лекциям [6.1.1, 6.1.2, 6.1.3]		9	

Планируемые (контролируемые) результаты освоения: код УК; ОПК; ПК и индикаторы достижения компетенций	Наименование разделов, тем	Виды учебной работы (час)					Вид СРС	Наименование используемых активных и интерактивных образовательных технологий	Реализация в рамках Практической подготовки (трудоемкость в часах)	Наименование разработанного Электронного курса (трудоемкость в часах)
		Контактная работа				Самостоятельная работа студентов (час)				
		Лекции (час)	Лабораторные работы (час)	Практические занятия (час)	КСР					
	изменения и контроль целостности.									
	Тема 2.4 Средства контроля защищенности информации для различных подсистем защиты	4			1	2	Подготовка к лекциям [6.1.1, 6.1.2, 6.1.3]			
	Тема лабораторной работы: «Знакомство с eToken API»		4			4				
	Тема лабораторной работы: «Работа с сертификатами X.509 на eToken»		4			4				
	Тема лабораторной работы: «Объекты eToken»		4			4				
	Тема лабораторной работы: «Шифрование данных с помощью eToken»		5			3				

Планируемые (контролируемые) результаты освоения: код УК; ОПК; ПК и индикаторы достижения компетенций	Наименование разделов, тем	Виды учебной работы (час)					Вид СРС	Наименование используемых активных и интерактивных образовательных технологий	Реализация в рамках Практической подготовки (трудоемкость в часах)	Наименование разработанного Электронного курса (трудоемкость в часах)
		Контактная работа				Самостоятельная работа студентов (час)				
		Лекции (час)	Лабораторные работы (час)	Практические занятия (час)	КСР					
	Итого по 2 разделу	**16**	17		**1**	**23**				
Раздел 3. Программно-аппаратные средства обеспечения информационной безопасности										
ОПК-5.2 - ОПК-5.2.1 ОПК-5.3 - ОПК-5.3.2 ОПК-10 - ОПК-10.1 ОПК-15 - ОПК-15.1	**Тема 3.1** Роль стандартов информационной безопасности. Документы Государственной технической комиссии России.	2				2	Подготовка к лекциям [6.1.1, 6.1.2, 6.1.3]	Разбор конкретных ситуаций		
	Тема 3.2 Задачи и технология сертификации программно-аппаратных средств на соответствие требованиям информационной безопасности. Основные категории требований к программной и программно-аппаратной реализации средств	2				2	Подготовка к лекциям [6.1.1, 6.1.2, 6.1.3]	Разбор конкретных ситуаций		

Планируемые (контролируемые) результаты освоения: код УК; ОПК; ПК и индикаторы достижения компетенций	Наименование разделов, тем	Виды учебной работы (час)					Вид СРС	Наименование используемых активных и интерактивных образовательных технологий	Реализация в рамках Практической подготовки (трудоемкость в часах)	Наименование разработанного Электронного курса (трудоемкость в часах)
		Контактная работа				Самостоятельная работа студентов (час)				
		Лекции (час)	Лабораторные работы (час)	Практические занятия (час)	КСР					
	обеспечения информационной безопасности. Показатели защищенности средств вычислительной техники от несанкционированного доступа. Требования к процессу сертификации продукта информационных технологий									
	Тема 3.1 Классы защищенности автоматизированных систем.	2				2	Подготовка к лекциям [6.1.1, 6.1.2, 6.1.3]	Разбор конкретных ситуаций		
	Итого по 3 разделу	**6**			**3**	**6**				
	Подготовка к зачету					**18**				
	Итого за семестр	**34**	**17**		**4**	**53**			17	

5. ТЕКУЩИЙ КОНТРОЛЬ УСПЕВАЕМОСТИ И ПРОМЕЖУТОЧНАЯ АТТЕСТАЦИЯ ПО ИТОГАМ ОСВОЕНИЯ ДИСЦИПЛИНЫ.

5.1 Типовые контрольные задания или иные материалы, необходимые для оценки знаний, умений и навыков и (или) опыта деятельности

Для выполнения процедур оценивания составлен паспорт оценочных средств.

Перечень вопросов, выносимых на промежуточную аттестацию (зачет)

1. Понятие политики безопасности. Описание типовых политик безопасности.
2. Угрозы безопасности компьютерных систем.
3. Понятие монитора безопасности. Концепция диспетчера доступа.
4. Дискреционный доступ. Реализация разграничения доступа к внешним устройствам.
5. Мандатный доступ, его реализация для файлов, папок и процессов. Управление потоками информации.
6. Метод генерации изолированной программной среды.
7. Принципы создания программно-аппаратных средств обеспечения информационной безопасности.
8. Методы и средства ограничения доступа к компонентам вычислительных систем.
9. Методы и средства привязки программного обеспечения к аппаратному окружению и физическим носителям.
10. Управление ключами криптографическими ключами. Методы и средства хранения ключевой информации.
11. Защита программ от изучения. Способы встраивания средств защиты в программное обеспечение.
12. Защита от разрушающих программных воздействий и вредоносного программного обеспечения.
13. Защита программ от изменения и контроль целостности.
14. Средства контроля защищенности информации для различных подсистем защиты.
15. Стандарты информационной безопасности.
16. Сертификация программно-аппаратных средств.
17. Требования к программной и программно-аппаратной реализаций средств обеспечения информационной безопасности.
18. Показатели защищенности средств вычислительной техники от несанкционированного доступа.
19. Классы защищенности автоматизированных систем.
20. Требования к процессу сертификации продукта информационных технологий

Комплект оценочных средств является неотъемлемой частью ФОС и хранится на кафедре «Информатика и системы управления».

5.2 Описание показателей и критериев контроля успеваемости, описание шкал оценивания

Для оценки знаний, умений, навыков и формирования компетенции по дисциплине применяется традиционная система контроля и оценки успеваемости студентов.

При промежуточном контроле успеваемость студентов оценивается по четырехбалльной системе «отлично», «хорошо», «удовлетворительно», «неудовлетворительно».

Таблица 5.4 – Критерии оценивания результата обучения по дисциплине и шкала оценивания

Код и наименование компетенции	**Код и наименовани индикатора достижения компетенции**	**Критерии оценивания результатов обучения**			
		Оценка **«неудовлетворительно»** / «не зачтено» 0-59% от max рейтинговой оценки контроля	Оценка **«удовлетворительно»** / «зачтено» 60-74% от max рейтинговой оценки контроля	Оценка **«хорошо»** / «зачтено» 75-89% от max рейтинговой оценки контроля	Оценка **«отлично»** / «зачтено» 90-100% от max рейтинговой оценки контроля
ОПК-5.2. Способен разрабатывать и эксплуатировать системы защиты информации открытых информационных систем	ИОПК-5.2.1. Применяет программно-аппаратные комплексы защиты информации для обеспечения информационной безопасности в открытых информационных системах	Изложение учебного материала бессистемное, неполное, не освоены базовые принципы программно-аппаратной защиты информации; не во всех случаях правильно оперирует основными понятиями в области информационной безопасности; не отвечает на задаваемые вопросы	Фрагментарные, поверхностные знания базовых принципов программно-аппаратной защиты информации; не во всех случаях находит правильные ответы на задаваемые вопросы по защите информации	Знает материал на достаточно хорошем уровне; представляет основные концепции программно-аппаратной защиты информации; подтверждает теоретические знания отдельными практическими примерами по защите информации в автоматизированных системах; дает ответы на задаваемые вопросы	Имеет глубокие знания всего материала по программно-аппаратной защите информации; дает развернутые ответы на задаваемые вопросы; имеет собственные суждения о решении задач защите данных
ОПК-5.3. Способен осуществлять контроль обеспечения	ИОПК-5.3.2. Применяет программно-	Изложение учебного материала бессистемное,	Фрагментарные, поверхностные знания базовых принципов	Знает материал на достаточно хорошем уровне;	Имеет глубокие знания всего материала по

информационной безопасности и проводить верификацию данных в открытых информационных системах	аппаратные комплексы защиты информации для контроля информационной безопасности в открытых информационных системах	неполное, не освоены базовые принципы программно-аппаратной защиты информации; не во всех случаях правильно оперирует основными понятиями в области информационной безопасности; не отвечает на задаваемые вопросы	программно-аппаратной защиты информации; не во всех случаях находит правильные ответы на задаваемые вопросы по защите информации	представляет основные концепции программно-аппаратной защиты информации; подтверждает теоретические знания отдельными практическими примерами по защите информации в автоматизированных системах; дает ответы на задаваемые вопросы	программно-аппаратной защите информации; дает развернутые ответы на задаваемые вопросы; имеет собственные суждения о решении задач защите данных
ОПК-10. Способен использовать средства криптографической защиты информации при решении задач профессиональной деятельности	ИОПК-10.1. Применяет криптографические алгоритмы и протоколы для обеспечения секретности и целостности информации в открытых информационных системах	Изложение учебного материала бессистемное, неполное, не освоены базовые принципы программно-аппаратной защиты информации; не во всех случаях правильно оперирует основными понятиями в области информационной безопасности; не отвечает на задаваемые вопросы	Фрагментарные, поверхностные знания базовых принципов программно-аппаратной защиты информации; не во всех случаях находит правильные ответы на задаваемые вопросы по защите информации	Знает материал на достаточно хорошем уровне; представляет основные концепции программно-аппаратной защиты информации; подтверждает теоретические знания отдельными практическими примерами по защите информации в	Имеет глубокие знания всего материала по программно-аппаратной защите информации; дает развернутые ответы на задаваемые вопросы; имеет собственные суждения о решении задач защите данных

				автоматизированных системах; дает ответы на задаваемые вопросы	
ОПК-11. Способен разрабатывать компоненты систем защиты информации автоматизированных систем	ИОПК-11.1. Применяет криптографические методы для создания компонентов систем защиты информации открытых информационных систем.	Изложение учебного материала бессистемное, неполное, не освоены базовые принципы программно-аппаратной защиты информации; не во всех случаях правильно оперирует основными понятиями в области информационной безопасности; не отвечает на задаваемые вопросы	Фрагментарные, поверхностные знания базовых принципов программно-аппаратной защиты информации; не во всех случаях находит правильные ответы на задаваемые вопросы по защите информации	Знает материал на достаточно хорошем уровне; представляет основные концепции программно-аппаратной защиты информации; подтверждает теоретические знания отдельными практическими примерами по защите информации в автоматизированных системах; дает ответы на задаваемые вопросы	Имеет глубокие знания всего материала по программно-аппаратной защите информации; дает развернутые ответы на задаваемые вопросы; имеет собственные суждения о решении задач защите данных

Таблица 5.5 - Критерии оценивания

Оценка	Критерии оценивания
Высокий уровень «5» (отлично)	оценку **«отлично»** заслуживает студент, освоивший знания, умения, компетенции и теоретический материал без пробелов; выполнивший все задания, предусмотренные учебным планом на высоком качественном уровне; практические навыки профессионального применения освоенных знаний сформированы.
Средний уровень «4» (хорошо)	оценку **«хорошо»** заслуживает студент, практически полностью освоивший знания, умения, компетенции и теоретический материал, учебные задания не оценены максимальным числом баллов, в основном сформировал практические навыки.
Пороговый уровень «3» (удовлетворительно)	оценку **«удовлетворительно»** заслуживает студент, частично с пробелами освоивший знания, умения, компетенции и теоретический материал, многие учебные задания либо не выполнил, либо они оценены числом баллов близким к минимальному, некоторые практические навыки не сформированы.
Минимальный уровень «2» (неудовлетворительно)	оценку «неудовлетворительно» заслуживает студент, не освоивший знания, умения, компетенции и теоретический материал, учебные задания не выполнил, практические навыки не сформированы.

6. УЧЕБНО-МЕТОДИЧЕСКОЕ ОБЕСПЕЧЕНИЕ ДИСЦИПЛИНЫ

6.1 Учебная литература

6.1.1. Потерпеев, Г. Ю. Безопасность операционных систем : учебное пособие / Г. Ю. Потерпеев, В. С. Нефедов, А. А. Криулин. — Москва : РТУ МИРЭА, 2021. — 93 с. — ISBN 978-5-7339-1393-3. — Текст : электронный // Лань : электронно-библиотечная система. — URL: https://e.lanbook.com/book/182416

6.1.2. Нестеров, С. А. Основы информационной безопасности : учебник для вузов / С. А. Нестеров. — Санкт-Петербург : Лань, 2021. — 324 с. — ISBN 978-5-8114-6738-9. — Текст : элек-тронный // Лань : электронно-библиотечная система. — URL: https://e.lanbook.com/book/165837

6.2 Справочно-библиографическая литература

— *учебники и учебные пособия*

6.1.3. Никифоров, С. Н. Методы защиты информации. Шифрование данных : учебное пособие / С. Н. Никифоров. — 2-е изд., стер. — Санкт-Петербург : Лань, 2019. — 160 с. — ISBN 978-5-8114-4042-9. — Текст : электронный // Лань : электронно-библиотечная система. — URL: https://e.lanbook.com/book/114699

6.3 Методические указания, рекомендации и другие материалы к занятиям

Методические указания по выполнению лабораторных работ по дисциплине Программно-аппаратные средства защиты информации в электронном варианте находятся на кафедре «Информационная безопасность вычислительных систем и сете. Электронные варианты методических указаний по выполнению лабораторных работ отправляются на электронные адреса групп.

6.1.4. Программно-аппаратные средства защиты информации [Электронные текстовые данные]: метод. указания к лабораторным работам по дисциплине «Программно-аппаратные средства защиты информации» для студентов направления подготовки

10.05.03 «Информационная безопасность автоматизированных систем» дневной формы обучения / НГТУ; Сост.: С.Н. Капранов. Н. Новгород, 2021.

7. ИНФОРМАЦИОННОЕ ОБЕСПЕЧЕНИЕ ДИСЦИПЛИНЫ

Учебный процесс по дисциплине обеспечен необходимым комплектом свободно распространяемого программного обеспечения (состав по дисциплине определен в настоящей РПД и подлежит обновлению при необходимости).

7.1 Перечень информационных справочных систем

Таблица 7.1 - Перечень электронных библиотечных систем

№	Наименование ЭБС	Ссылка к ЭБС
1	«Консультант студента - Электронная библиотека технического вуза»	http://www.studentlibrary.ru/
2	Лань	https://e.lanbook.com/
3	«Юрайт» (коллекция «Легендарные книги»)	https://urait.ru/
4	«Техэксперт» - «Нормы, правила, стандарты и законодательство России»	https://www.nntu.ru/frontend/web/ngtu/files/org_structura/library/resurvsy/tehekspert.pdf

7.2 Перечень свободно распространяемого программного обеспечения

Таблица 7.2 – Программное обеспечение, используемое студентами очного обучения

Программное обеспечение, используемое в университете на договорной основе	Программное обеспечение свободного распространения
1. Windows 7 32 bit корпоративная VL 49477S2 2. Microsoft Office Professional Plus 2007 (лицензия № 42470655); 3. Dr.Web (с/н GMN9-DSLH-G4U1-LW6H от 11.05.23 4. Microsoft Windows 7 MSDN (подписка DreamSpark Premium, договор № Tr113003 от 25.09.14)	Adobe Acrobat Reader (https://acrobat.adobe.com/ru/ru/acrobat/pdf-reader.html) Linux (https://www.linux.com/) OpenOffice (FreeWare) https://www.openoffice.org/ru/ JDK 8 и выше (https://adoptopenjdk.net/) Фреймворк Java Spring 5 (https://spring.io/projects/spring-framework) Eclipse (https://www.eclipse.org/) Intellij Idea (https://www.jetbrains.com/ru-ru/idea/) git (https://git-scm.com/), github (https://github.com/) Maven (https://maven.apache.org/), Gradle (https://gradle.org/) Редактор блок-схем (https://app.diagrams.net/) Microsoft Visual Studio 2017 Community Edition (https://visualstudio.microsoft.com/ru/vs/community/) Adobe Acrobat Reader DC-Russian (беспл.) Операционная система Ubuntu Linux 20, GNS3, Snort, Wareshark, OpenVPN, Libre Office, OpenVPN, IP scanner

7.3 Перечень современных профессиональных баз данных и информационных справочных систем

В таблице 7.4 указан перечень профессиональных баз данных и информационных справочных систем, к которым обеспечен доступ (удаленный доступ). Данный перечень подлежит обновлению в соответствии с требованиями ФГОС ВО.

В данном разделе могут быть приведены ресурсы (ссылки на сайты), на которых можно найти полезную для курса информацию, в т.ч. статистические или справочные данные, учебные материалы, онлайн курсы и т.д.

Таблица 7.4 – Перечень современных профессиональных баз данных и информационных справочных систем

№	Наименование профессиональной базы данных, информационно-справочной системы	Доступ к ресурсу (удаленный доступ с указанием ссылки/доступ из локальной сети университета)
1	2	3
1	База данных издательства Wiley	https://onlinelibrary.wiley.com/
2	База данных Polpred	http://www.polpred.com
3	Научная электронная библиотека ELIBRARY.RU	http://elibrary.ru
4	База данных стандартов и регламентов РОССТАНДАРТ	https://www.rst.gov.ru/portal/gost/home/standarts
5	Перечень профессиональных баз данных и информационных справочных систем	https://cyberpedia.su/21x47c0.html
6	Каталог паттернов проектирования	https://refactoring.guru/ru/design-patterns/catalog

8. ОБРАЗОВАТЕЛЬНЫЕ РЕСУРСЫ ДЛЯ ИНВАЛИДОВ И ЛИЦ С ОВЗ

В таблице 8.1 указан перечень образовательных ресурсов, имеющих формы, адаптированные к ограничениям их здоровья, а также сведения о наличии специальных технических средств обучения коллективного и индивидуального пользования. При заполнении таблицы может быть использована информация, размещенная в подразделе «Доступная среда» специализированного раздела сайта НГТУ «Сведения об образовательной организации» https://www.nntu.ru/sveden/ovz/.

Таблица 8.1 - Образовательные ресурсы для инвалидов и лиц с ОВЗ

№	Перечень образовательных ресурсов, приспособленных для использования инвалидами и лицами с ОВЗ	Сведения о наличии специальных технических средств обучения коллективного и индивидуального пользования
1	ЭБС «Консультант студента»	Версия для слабовидящих, прослушивание с помощью синтезатора речи
2	ЭБС «Лань»	Версия для слабовидящих, прослушивание с помощью синтезатора речи
3	«Юрайт» (коллекция «Легендарные книги»)	Версия для слабовидящих

9. МАТЕРИАЛЬНО-ТЕХНИЧЕСКОЕ ОБЕСПЕЧЕНИЕ, НЕОБХОДИМОЕ ДЛЯ ОСУЩЕСТВЛЕНИЯ ОБРАЗОВАТЕЛЬНОГО ПРОЦЕССА ПО ДИСЦИПЛИНЕ

Учебные аудитории для проведения занятий по дисциплине, оснащены оборудованием и техническими средствами обучения

В таблице 9.1 перечислены:

- учебные аудитории для проведения учебных занятий, оснащенные оборудованием и техническими средствами обучения;
- помещения для самостоятельной работы обучающихся, которые должны оснащены компьютерной техникой с возможностью подключения к сети «Интернет» и обеспечением доступа в электронную информационно-образовательную среду НГТУ.

Таблица 9.1 - Оснащенность аудиторий и помещений для самостоятельной работы студентов по дисциплине

№	Наименование аудиторий и помещений для самостоятельной работы	Оснащенность аудиторий помещений и помещений для самостоятельной работы	Перечень лицензионного программного обеспечения. Реквизиты подтверждающего документа
1	1	2	3
1	Учебная аудитория № 6421 учебно-лабораторного корпуса № 6 для проведения учебных занятий. 603163, Нижегородская область, г. Нижний Новгород, Казанское шоссе, д.12	1. Доска меловая – 1 шт. 3. Экран – 1 шт. 4. Мультимедийный проектор Epson X12 – 1 шт. 5. Компьютер PC MB Asus на чипсете Nvidia/AMDAthlonXII CPU 2.8Ggz/ RAM 4 Ggb/SVGAStandartGraphics +Ge-FORCE Nvidia GT210/HDD 250Ggb,SATAinterface, монитор 19”, с выходом на проектор. 6. Рабочее место студента - 74 7. Рабочее место для преподавателя – 1 шт.	1. Windows 7 32 bit корпоративная; VL 49477S2 2. Adobe Acrobat Reader DC-Russian (беспл.) 3. Microsoft Office Professional Plus 2007 (лицензия № 42470655); 4. Dr.Web (с/н GMN9-DSLH-G4U1-LW6H от 11.05.23 до 28.05.24)
2	Лаборатория «Программно-аппаратных средств и технической защиты информации» - учебная аудитория № 6039 учебно-лабораторного корпуса № 6 для проведения учебных занятий и практической подготовки обучающихся 603163, Нижегородская область, г. Нижний Новгород, Казанское шоссе, д.12	1.Учебный лабораторный стенд "Блочное кодирование" – 1 шт. 2.Учебный лабораторный стенд "Основы криптографии" – 1 шт. 3.Учебный лабораторный стенд "Биометрическая аутентификация" – 2 шт. 4.Учебный лабораторный стенд "Доверенная загрузка (Соболь)" – 1 шт. 5.Учебный лабораторный стенд "Доверенная загрузка (Аккорд)" – 1 шт. 6.Учебный лабораторный стенд "Криптоконтейнеры и ЭЦП" – 2 шт. 7. МФУ Brother LC 8. Посадочных мест - 16.	Распространяемое по свободной лицензии: 1.Операционная система Ubuntu Linux 20 2. GNS3 3. Snort 4. Wareshark 5. OpenVPN 6. Libre Office 7. Splunk 8. Zeek Network Security Monitor 9. Security Onion 10. OpenVPN 11. IP scanner 12. Nemesis 13. Eyercap
3	Помещение для самостоятельной работы обучающихся № 6545 учебно-лабораторного корпуса № 6 для проведения научно-исследовательской работы обучающихся, курсового и дипломного проектирования. 603163, Нижегородская область, г. Нижний Новгород, Казанское шоссе, д.12	1. Рабочие места, оснащенные ПК на базеCore 2 Duo с мониторами – 5 шт. 2. Рабочее место преподавателя, оснащенное ПК на базе Intel Core i5 с монитором – 1 шт. 3. Доска интерактивная ScreenMedia-M. ПК подключены к сети «Интернет» и обеспечивают доступ в электронную информационно-образовательную среду университета. 4. Посадочных мест - 12, шесть оснащены ПК. 5. Принтер Xerox Phaser 3300 MFP	1. Microsoft Windows 7 MSDN реквизиты договора - подписка (подписка DreamSpark Premium, договор № 0509/КМР от 15.10.18), 2. Бесплатное ПО: Пакет программ Open Office, True Conf, Браузер Google Chrome, Браузер Mozilla Firefox, Браузер Opera, McAfee Security Scan, Adobe Acrobat Reader DC

10. МЕТОДИЧЕСКИЕ РЕКОМЕНДАЦИИ ОБУЧАЮЩИМСЯ ПО ОСВОЕНИЮ ДИСЦИПЛИНЫ

10.1 Общие методические рекомендации для обучающихся по освоению дисциплины, образовательные технологии

Дисциплина реализуется посредством проведения контактной работы с обучающимися (включая проведение текущего контроля успеваемости), самостоятельной работы обучающихся и промежуточной аттестации.

При преподавании дисциплины «Программно-аппаратные средства защиты информации», используются современные образовательные технологии, позволяющие повысить активность студентов при освоении материала курса и предоставить им возможность эффективно реализовать

часы самостоятельной работы.

Весь лекционный материал курса сопровождается компьютерными презентациями, в которых наглядно преподносятся материал различных разделов курса и что дает возможность обсудить материал со студентами во время чтения лекций, активировать их деятельность при освоении материала. Электронные материалы лекций в период дистанционного обучения отправляются по электронной почте на адреса групп и могут быть получены до чтения лекций и проработаны студентами в ходе самостоятельной работы.

На лекциях, лабораторных занятиях реализуются интерактивные технологии, приветствуются вопросы и обсуждения, используется личностно-ориентированный подход, технология работы в малых группах, что позволяет студентам проявить себя, получить навыки самостоятельного изучения материала, выровнять уровень знаний в группе.

Все вопросы, возникшие при самостоятельной работе над домашним заданием подробно разбираются на лабораторных занятиях и лекциях. Проводятся индивидуальные и групповые консультации с использованием современных информационных технологий: электронная почта, мессенджеры, Zoom, Discord.

Инициируется активность студентов, поощряется задание любых вопросов по материалу, практикуется индивидуальный ответ на вопросы студента, рекомендуются методы успешного самостоятельного усвоения материала в зависимости от уровня его базовой подготовки.

Для оценки знаний, умений, навыков и уровня сформированности компетенции применяется балльно-рейтинговая система контроля и оценки успеваемости студентов в процессе текущего контроля.

Промежуточная аттестация проводится в форме зачета с учетом текущей успеваемости.

10.2 Методические указания для занятий лекционного типа

Лекционный курс предполагает систематизированное изложение основных вопросов тематического плана. В ходе лекционных занятий раскрываются базовые вопросы в рамках каждой темы дисциплины (Таблицы 4.4, 4.5, 4.6) . Обозначаются ключевые аспекты тем, а также делаются акценты на наиболее сложные и важные положения изучаемого материала. Материалы лекций являются опорной основой для подготовки обучающихся к лабораторным работам и выполнения заданий самостоятельной работы, а также к мероприятиям текущего контроля успеваемости и промежуточной аттестации по дисциплине.

10.3 Методические указания по освоению дисциплины на лабораторных работах

Подготовку к каждой лабораторной работе студент должен начать с ознакомления с планом занятия, который отражает содержание предложенной темы. Каждая выполненная работа с оформленным отчетом подлежит защите у преподавателя.

При оценивании лабораторных работ учитывается следующее:

- качество выполнения практической части работы и степень соответствия результатов работы заданным требованиям;
- качество оформления отчета по работе;
- качество устных ответов на контрольные вопросы при защите работы.

10.4 Методические указания по освоению дисциплины на занятиях семинарского типа

Практические (семинарские) занятия не предусмотрены учебным планом

10.5 Методические указания по освоению дисциплины на курсовой работе

Курсовая работа не предусмотрена учебным планом.

10.6 Методические указания по самостоятельной работе обучающихся

Самостоятельная работа обеспечивает подготовку обучающегося к аудиторным занятиям и мероприятиям текущего контроля и промежуточной аттестации по изучаемой дисциплине. Результаты этой подготовки проявляются в активности обучающегося на занятиях и в качестве выполненных практических заданий и других форм текущего контроля.

При выполнении заданий для самостоятельной работы рекомендуется проработка материалов лекций по каждой пройденной теме, а также изучение рекомендуемой литературы, представленной в Разделе 6.

В процессе самостоятельной работы при изучении дисциплины студенты могут работать на компьютере в специализированных аудиториях для самостоятельной работы, указанных в Разделе 9. В аудиториях имеется доступ через информационно-телекоммуникационную сеть «Интернет» к электронной информационно-образовательной среде университета (ЭИОС) и электронной библиотечной системе (ЭБС), где в электронном виде располагаются учебные и учебно-методические материалы, которые могут быть использованы для самостоятельной работы при изучении дисциплины.

11. ОЦЕНОЧНЫЕ СРЕДСТВА ДЛЯ КОНТРОЛЯ ОСВОЕНИЯ ДИСЦИПЛИНЫ

11.1 Типовые контрольные задания или иные +материалы, необходимые для оценки знаний, умений, навыков и (или) опыта в ходе текущего контроля успеваемости

Для текущего контроля знаний студентов по дисциплине проводится **комплексная оценка знаний,** включающая

- выполнение и защита лабораторных работ **для студентов всех форм обучения**;

Темы лабораторных работ:

1. Знакомство с eToken API
2. Работа с сертификатами X.509 на eToken
3. Объекты eToken
4. Шифрование данных с помощью eToken

11.2 Типовые контрольные задания или иные материалы, необходимые для оценки знаний, умений, навыков и (или) опыта в ходе промежуточной аттестации по дисциплине

Зачет для студентов очной формы обучения в 8 семестре.

Типовые вопросы для промежуточной аттестации в форме зачета для студентов очной формы обучения

Вопросы, направленные на проверку компетенции ОПК-5.2, ОПК-5.3, ОПК-15:

1. Понятие политики безопасности. Описание типовых политик безопасности.
2. Угрозы безопасности компьютерных систем.
3. Понятие монитора безопасности. Концепция диспетчера доступа.
4. Дискреционный доступ. Реализация разграничения доступа к внешним устройствам.
5. Мандатный доступ, его реализация для файлов, папок и процессов. Управление потоками информации.
6. Метод генерации изолированной программной среды.
7. Принципы создания программно-аппаратных средств обеспечения информационной безопасности.
8. Методы и средства ограничения доступа к компонентам вычислительных систем.
9. Методы и средства привязки программного обеспечения к аппаратному окружению и физическим носителям.
10. Управление ключами криптографическими ключами. Методы и средства хранения ключевой информации.
11. Защита программ от изучения. Способы встраивания средств защиты в программное обеспечение.
12. Защита от разрушающих программных воздействий и вредоносного программного обеспечения.
13. Защита программ от изменения и контроль целостности.
14. Средства контроля защищенности информации для различных подсистем защиты.
15. Стандарты информационной безопасности.
16. Сертификация программно-аппаратных средств.
17. Требования к программной и программно-аппаратной реализаций средств обеспечения информационной безопасности.
18. Показатели защищенности средств вычислительной техники от несанкционированного доступа.
19. Классы защищенности автоматизированных систем.
20. Требования к процессу сертификации продукта информационных технологий

Вопросы, направленные на проверку компетенции ОПК-10:

1. Принципы создания программно-аппаратных средств обеспечения информационной безопасности.
2. Методы и средства ограничения доступа к компонентам вычислительных систем.
3. Управление ключами криптографическими ключами. Методы и средства хранения ключевой информации.
4. Защита программ от изменения и контроль целостности.
5. Средства контроля защищенности информации для различных подсистем защиты.

В полном объеме оценочные средства имеются на кафедре «Информационная безопасность вычислительных систем и сетей». Оценочные средства могут быть получены по требованию.