МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ РОССИЙСКОЙ ФЕДЕРАЦИИ
Федеральное государственное автономное образовательное учреждение высшего образования
«СЕВЕРО-КАВКАЗСКИЙ ФЕДЕРАЛЬНЫЙ УНИВЕРСИТЕТ»
Пятигорский институт (филиал) СКФУ

УТВЕРЖДАЮ
Зам. директора по учебной работе
Пятигорского института (филиал)
СКФУ
М.В. Мартыненко
«28» марта 2022 г.

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ
«РАЗРАБОТКА И ЭКСПЛУАТАЦИЯ ЗАЩИЩЕННЫХ АВТОМАТИЗИРОВАННЫХ ИНФОРМАЦИОННЫХ СИСТЕМ»

Направление подготовки/специальность **10.03.01 Информационная безопасность**
Направленность (профиль)/специализация **Безопасность компьютерных систем**
Форма обучения очная
Год начала обучения 2022
Реализуется в 7,8 семестрах

Разработано
Ст. преподавателем кафедры СУиИТ,
Калиберда И.В.

Пятигорск 2022 г.

1. Цель и задачи освоения дисциплины (модуля)

Дисциплина «Разработка и эксплуатация защищенных автоматизированных информационных систем» имеет целью изучение основных понятий, методологии и практических приемов проектирования, разработки и внедрения информационных систем с учетом требований по обеспечению информационной безопасности.

Задачами дисциплины являются:

1. Приобретение обучаемыми необходимого объема знаний и практических навыков в области стандартизациии нормотворчества в области защиты информационных систем.

2. Формирование у обучаемых целостного представления об организации и содержании процессов проектирования, разработки, внедрения и эксплуатации защищенных информационных систем.

2. Место дисциплины (модуля) в структуре образовательной программы

Дисциплина «Разработка и эксплуатация защищенных автоматизированных информационных систем» относится к Блок 1.Дисциплины (модули) «Часть, формируемая участниками образовательных отношений» образовательной программы. Ее освоение происходит в 7,8 семестрах.

3. Перечень планируемых результатов обучения по дисциплине (модулю), соотнесённых с планируемыми результатами освоения образовательной программы

Код, формулировка компетенции	Код, формулировка индикатора	Планируемые результаты обучения по дисциплине (модулю), характеризующие этапы формирования компетенций, индикаторов
ПК-7 Способность проводить анализ исходных данных для проектирования подсистем и средств обеспечения информационной безопасности и участвовать в проведении технико-экономического обоснования соответствующих проектных решений	ИД-1 ПК-7 Знает требования по защите информации, включая использование математического аппарата для решения прикладных задач. ИД-2 ПК-7 Умеет составлять планы этапов проведения научно-исследовательских и опытно-конструкторских работ. ИД-3 ПК-7 Владеет навыками разработки и анализа структурных и функциональных схем защищенных компьютерных систем в сфере профессиональной деятельности.	Разрабатывает защищенные автоматизированные информационные системы
ПК-8 Способность оформлять рабочую техническую документацию с учетом действующих нормативных и методических документов	ИД-1 ПК-8 Понимает действующие нормативные и методические документы. ИД-2 ПК-8 Способен анализировать, систематизировать, оформлять техническую документацию. ИД-3 ПК-8 Владеет навыками грамотного составления технической документации.	

4. Объем учебной дисциплины (модуля) и формы контроля

Объем занятий:	З.е.	Астр. ч.	Из них в форме практической подготовки
Всего:	5	135	
Из них аудиторных:		58,5	
Лекций		22,5	
Лабораторных работ		36	
Практических занятий			
Самостоятельной работы		49,5	
Формы контроля:			
Экзамен	8 семестр	27	
Зачет с оценкой			
Зачет	7 семестр		

5. Содержание дисциплины (модуля), структурированное по темам (разделам) с указанием количества часов и видов занятий

5.1.Тематический план дисциплины (модуля)

№	Раздел (тема) дисциплины	Реализуемые компетенции, индикаторы	Контактная работа обучающихся с преподавателем, часов				Самостоятельная работа, часов
			Лекции	Практические занятия	Лабораторные работы	Групповые консультации	
7 семестр							
1	Принципы системного подхода присоздании сложных систем	ИД-1$_{ПК-7}$ ИД-2$_{ПК-7}$ ИД-3$_{ПК-7}$ ИД-1$_{ПК-8}$ ИД-2$_{ПК-8}$ ИД-3$_{ПК-8}$	1,5		6		13,5
2	Нормативно-методическое обеспечениесоздания информационных систем	ИД-1$_{ПК-7}$ ИД-2$_{ПК-7}$ ИД-3$_{ПК-7}$ ИД-1$_{ПК-8}$ ИД-2$_{ПК-8}$ ИД-3$_{ПК-8}$	1,5				
3	Стандарт жизненного цикла информационных систем	ИД-1$_{ПК-7}$ ИД-2$_{ПК-7}$ ИД-3$_{ПК-7}$ ИД-1$_{ПК-8}$ ИД-2$_{ПК-8}$ ИД-3$_{ПК-8}$	1,5				
4	Модели жизненного цикла информационных систем	ИД-1$_{ПК-7}$ ИД-2$_{ПК-7}$ ИД-3$_{ПК-7}$ ИД-1$_{ПК-8}$ ИД-2$_{ПК-8}$ ИД-3$_{ПК-8}$	1,5		3		
5	Оценка процессов создания информационных систем	ИД-1$_{ПК-7}$ ИД-2$_{ПК-7}$	1,5		6		

		ИД-3$_{ПК-7}$ ИД-1$_{ПК-8}$ ИД-2$_{ПК-8}$ ИД-3$_{ПК-8}$					
6	Методология и обзор методов IDEF	ИД-1$_{ПК-7}$ ИД-2$_{ПК-7}$ ИД-3$_{ПК-7}$ ИД-1$_{ПК-8}$ ИД-2$_{ПК-8}$ ИД-3$_{ПК-8}$	1,5				
7	Методология и обзор методов eEPC	ИД-1$_{ПК-7}$ ИД-2$_{ПК-7}$ ИД-3$_{ПК-7}$ ИД-1$_{ПК-8}$ ИД-2$_{ПК-8}$ ИД-3$_{ПК-8}$	1,5				
8	Постановка проблемы комплексного обеспечения информационной безопасности информационных систем	ИД-1$_{ПК-7}$ ИД-2$_{ПК-7}$ ИД-3$_{ПК-7}$ ИД-1$_{ПК-8}$ ИД-2$_{ПК-8}$ ИД-3$_{ПК-8}$	1,5		6		
9	Особенности проектирования на современном уровне и синтез комплексной системы информационной безопасности	ИД-1$_{ПК-7}$ ИД-2$_{ПК-7}$ ИД-3$_{ПК-7}$ ИД-1$_{ПК-8}$ ИД-2$_{ПК-8}$ ИД-3$_{ПК-8}$	1,5		6		
	Итого за 7 семестр		**13,5**		**27**		**13,5**
10	Методы и методики проектирования комплексной системы информационной безопасности от несанкционированного доступа	ИД-1$_{ПК-7}$ ИД-2$_{ПК-7}$ ИД-3$_{ПК-7}$ ИД-1$_{ПК-8}$ ИД-2$_{ПК-8}$ ИД-3$_{ПК-8}$	1,5				36
11	Методы и методики оценки качества комплексной системы информационной безопасности	ИД-1$_{ПК-7}$ ИД-2$_{ПК-7}$ ИД-3$_{ПК-7}$ ИД-1$_{ПК-8}$ ИД-2$_{ПК-8}$ ИД-3$_{ПК-8}$	1,5				
12	Аттестация информационных систем по требованиям безопасности	ИД-1$_{ПК-7}$ ИД-2$_{ПК-7}$ ИД-3$_{ПК-7}$ ИД-1$_{ПК-8}$ ИД-2$_{ПК-8}$ ИД-3$_{ПК-8}$	1,5				
13	Особенности эксплуатации комплексной системы обеспечения безопасности на объекте защиты	ИД-1$_{ПК-7}$ ИД-2$_{ПК-7}$ ИД-3$_{ПК-7}$ ИД-1$_{ПК-8}$ ИД-2$_{ПК-8}$	1,5		9		

		ИД-3$_{ПК-8}$					
14	Модели защиты информации	ИД-1$_{ПК-7}$ ИД-2$_{ПК-7}$ ИД-3$_{ПК-7}$ ИД-1$_{ПК-8}$ ИД-2$_{ПК-8}$ ИД-3$_{ПК-8}$	1,5				
15	Реализация системы управления доступом	ИД-1$_{ПК-7}$ ИД-2$_{ПК-7}$ ИД-3$_{ПК-7}$ ИД-1$_{ПК-8}$ ИД-2$_{ПК-8}$ ИД-3$_{ПК-8}$	1,5				
	Итого за 8 семестр		**9**		**9**		**36**
	ИТОГО:		**9**		**9**		**36**

5.2 Наименование и содержание лекций

№ темы	Наименование тем дисциплины, их краткое содержание	Объем часов	Из них практическая подготовка, часов
	7 семестр		
1	Принципы системного подхода при создании сложных систем	1,5	
2	Нормативно-методическое обеспечение создания информационных систем	1,5	
3	Стандарт жизненного цикла информационных систем	1,5	
4	Модели жизненного циклаинформационных систем	1,5	
5	Оценка процессов созданияинформационных систем	1,5	
6	Методология и обзор методов IDEF	1,5	
7	Методология и обзор методов eEPC	1,5	
8	Постановка проблемы комплексного обеспечения информационной безопасности информационных систем	1,5	
9	Особенности проектирования на современном уровне и синтез комплексной системы информационной безопасности	1,5	
	Итого за 7 семестр	**13,5**	
	8 семестр		
10	Методы и методики проектирования комплексной системы информационной безопасности от несанкционированного доступа	1,5	
11	Методы и методики оценки качества комплексной системы информационной безопасности	1,5	
12	Аттестация информационных систем по требованиям безопасности	1,5	
13	Особенности эксплуатации комплексных систем	1,5	

	безопасности на объекте защиты		
14	Модели защиты информации	1,5	
15	Реализация системы управления доступом	1,5	
	Итого за 8 семестр	**9**	
	ИТОГО:	**9**	

5.3 Наименование лабораторных работ

№ Темы дисциплины	Наименование тем дисциплины, их краткое содержание	Объем часов	Из них практическая подготовка, часов
7 семестр			
Тема 1. Принципы системного подхода при создании сложных систем			
1	Изучение инструментального средства для моделирования на языке UML Visual Paradigm for UML	6	
Тема 4. Модели жизненного цикла информационных систем			
2	Моделирование компьютерных сетей на базе программного обеспечения CCNA Network Visualizer 6.0	3	
Тема 5. Оценка процессов создания информационных систем			
3	Введение в операционную систему IOS	3	
4	Введение в операционную систему Android	3	
Тема 8. Постановка проблемы комплексного обеспечения информационной безопасностиинформационных систем			
5	Обеспечение защиты маршрутизаторов и коммутаторов	6	
Тема 9. Особенности проектирования на современном уровне и синтез комплексной системыинформационной безопасности			
6	Средства шифрования	3	
7	Межсетевые экраны	3	
	Итого за 7 семестр:	**27**	
8 семестр			
Тема 13. Особенности эксплуатации комплексных систем безопасности на объекте защиты			
8	Программные продукты для анализов рисков информационной безопасности	4,5	
9	Эксплуатация уязвимостей для анализов рисков информационной безопасности	4,5	
	Итого за 8 семестр	**9**	
	Итого	**36**	

5.4 Перечень практических занятий

5.5 Технологическая карта самостоятельной работы обучающегося

Коды реализуемых компетенций	Вид деятельности студентов	Средства и технологии оценки	Объем часов, в том числе (астр.)		
			СРС	Контактная работа с преподавателем	Всего
ИД-1$_{ПК-7}$ ИД-2$_{ПК-7}$ ИД-3$_{ПК-7}$ ИД-1$_{ПК-8}$ ИД-2$_{ПК-8}$ ИД-3$_{ПК-8}$	Самостоятельное изучение литературы и источников	Собеседование	25,83	2,87	28,7
ИД-1$_{ПК-7}$ ИД-2$_{ПК-7}$ ИД-3$_{ПК-7}$ ИД-1$_{ПК-8}$ ИД-2$_{ПК-8}$ ИД-3$_{ПК-8}$	Подготовка к лабораторным занятиям	Защита ПР	9,72	1,08	10,8
ИД-1$_{ПК-7}$ ИД-2$_{ПК-7}$ ИД-3$_{ПК-7}$ ИД-1$_{ПК-8}$ ИД-2$_{ПК-8}$ ИД-3$_{ПК-8}$	Написание реферата/доклада	Защита доклада	9	1	10
		Итого	44,55	4,95	49,5

6. Фонд оценочных средств для проведения текущего контроля успеваемости и промежуточной аттестации обучающихся по дисциплине (модулю)

Фонд оценочных средств (ФОС) для проведения текущего контроля успеваемости и промежуточной аттестации обучающихся по дисциплине «Разработка и эксплуатация защищенных автоматизированных информационных систем» базируется на перечне осваиваемых компетенций с указанием этапов их формирования в процессе освоения дисциплины (модуля). ФОС обеспечивает объективный контроль достижения запланированных результатов обучения. ФОС включает в себя:

- описание показателей и критериев оценивания компетенций на различных этапах их формирования, описание шкал оценивания;
- методические материалы, определяющие процедуры оценивания знаний, умений, навыков и (или) опыта деятельности, характеризующих этапы формирования компетенций;
- типовые контрольные задания и иные материалы, необходимые для оценки знаний, умений и уровня овладения формируемыми компетенциями в процессе освоения дисциплины (модуля).

ФОС является приложением к данной программе дисциплины (модуля).

7. Методические указания для обучающихся по освоению дисциплины

При [illegible] каждый студент должен принимать во внимание следующие положения.

Дисциплина (модуль) построена по тематическому принципу, каждая тема представляет собой логически завершенный раздел.

Теоретический материал посвящен рассмотрению ключевых, базовых положений

курсов и разъяснению учебных заданий, выносимых на самостоятельную работу студентов.

Практические занятия направлены на приобретение опыта практической работы в соответствующей предметной области.

Самостоятельная работа студентов направлена на самостоятельное изучение дополнительного материала, подготовку к практическим занятиям, а также выполнения всех видов самостоятельной работы.

Для успешного освоения дисциплины, необходимо выполнить все виды самостоятельной работы, используя рекомендуемые источники информации.

8. Учебно-методическое и информационное обеспечение дисциплины

8.1. Перечень основной и дополнительной литературы, необходимой для освоения дисциплины (модуля)

8.1.1. Перечень основной литературы:

1.Аверченков, В. И.
    Служба защиты информации. Организация и управление Электронный ресурс : Учебное пособие для вузов / В. И. Аверченков, М. Ю. Рытов. - Брянск : Брянский государственный технический университет, 2012. - 186 с. - Книга находится в премиум-версии ЭБС IPR BOOKS. - ISBN 5-89838-138-4

2.Сердюк, В. А. Организация и технологии защиты информации : обнаружение и предотвращение информационных атак в автоматизированных системах предприятий / В.А. Сердюк. - Москва : Издательский дом Высшей школы экономики, 2015. - 574 с. - ISBN978-5-7598-0698-1

8.1.2. Перечень дополнительной литературы:

1.Костылева, Н.В.
    Информационное обеспечение управленческой деятельности Электронный ресурс : учебное пособие / Д.В. Шкурин / Ю.А. Мальцева / Н.В. Костылева ; ред. И.В. Котляревская. - Информационное обеспечение управленческой деятельности,2022-08-31. - Екатеринбург : Уральский федеральный университет, ЭБС АСВ, 2016. - 148 с. - Книга находится в базовой версии ЭБС IPRbooks. - ISBN 978-5-7996-1785-1

2.Петренко, С. А.
    Политики безопасности компании при работе в Интернет Электронный ресурс / С. А. Петренко, В. А. Курбатов. - Политики безопасности компании при работе в Интернет,2019-04-19. - Саратов : Профобразование, 2017. - 397 с. - Книга находится в премиум-версии ЭБС IPR BOOKS. - ISBN 978-5-4488-0082-5

3.Степанова, Е. Е. Информационное обеспечение управленческой деятельности : [учеб. пособие] / Е.Е. Степанова, Н.В. Хмелевская. - 2-е изд., испр. и доп. - М. : ФОРУМ, 2010. - 192 с. : ил. - (Профессиональное образование). - Библиогр.: с. 186-187. - ISBN 978-5-91134- 382-8

8.2. Перечень учебно-методического обеспечения самостоятельной работы обучающихся по дисциплине (модулю)

1. Методические рекомендации по выполнению практических работ по дисциплине "Разработка и эксплуатация защищенных автоматизированных информационных систем"

2. Методические рекомендации по организации самостоятельной работы студентов по дисциплине "Разработка и эксплуатация защищенных автоматизированных информационных систем"

8.3. Перечень ресурсов информационно-телекоммуникационной сети «Интернет», необходимых для освоения дисциплины (модуля)

1. Anti-Malware.ru – независимый информационно-аналитический центр: сайт. – URL: http://www.anti-malware.ru

2. BugTraq.Ru – информационная безопасность: сайт. – URL: http://bugtraq.ru

3. Ismmarket.ru – рынок информационной безопасности: сайт. – URL: http://ismmarket.ru

4. ISO27000.ru – Защита информации, управление информационной безопасностью и рисками: сайт. – URL: http:// iso27000.ru

5. WikiSec.ru – энциклопедия информационной безопасности: сайт. – URL: http:// wikisec.ru

6. Информационный портал по безопасности SecurityLab.ru, новости, статьи, обзор уязвимостей, вирусов и мнения аналитиков: сайт. – URL: http://securitylab.ru

9. Перечень информационных технологий, используемых при осуществлении образовательного процесса по дисциплине (модулю), включая перечень программного обеспечения и информационных справочных систем

При чтении лекций используется компьютерная техника, демонстрации презентационных мультимедийных материалов. На семинарских и практических занятиях студенты представляют презентации, подготовленные ими в часы самостоятельной работы.

Информационные справочные системы:

Информационно-справочные и информационно-правовые системы, используемые при изучении дисциплины:

1	КонсультантПлюс - http://www.consultant.ru/

Программное обеспечение:

1	Операционная система: Microsoft Windows 8: 2013-02(3000). Бессрочная лицензия. Договор № 01-эа/13 от 25.02.2013. Окончание бесплатной поддержки – 2023-01 ИЛИ Операционная система: Microsoft Windows 10: 2016-08(20), 2017-10(67), 2018-01(18), 2018-04(6), 2018-05(6), 2019-02(7). Бессрочная лицензия. Договоры № 27-эа/16 от 02.08.2016. и № 0321100021117000009_229123 от 10.10.2017. На текущий момент окончания поддержки не анонсировано.
2	Базовый пакет программ Microsoft Office (Word, Excel, PowerPoint). MicrosoftOfficeStandard 2013: договор № 01-эа/13 от 25.02.2013г., Лицензирование Microsoft Office https://support.microsoft.com/ru-ru/lifecycle/search/16674 Дата начала жизненного цикла 09.01.2013г.; набор обновлений Office 2013 Service Pack1 Дата начала жизненного цикла 25.02.2014г., Дата окончания основной фазы поддержки 10.04.2018; Дополнительная дата окончания поддержки 11.04.2023г.
3	Android SDK BestCrypt PGP UML Visual Paradigm for UML

10. Описание материально-технической базы, необходимой для осуществления образовательного процесса по дисциплине (модулю)

Лекционные занятия	Учебная аудитория с мультимедиа оборудованием; Мультимедийное оборудование: проектор, компьютер, экран настенный. Комплект учебной мебели.
Лабораторные занятия	Лаборатория технической защиты информации, аудита технических каналов утечки информации на объектах информатизации с интерактивным мультимедиа оборудованием; Персональные компьютеры. Мультимедийное оборудование: интерактивный проектор, компьютер, магнитно-маркерная доска.

	Генератор шума по сети электропитания и линиям заземления. Генератор шума. Устройство комбинированной защиты объектов информатизации от утечки информации. Электронно-оптическое устройство. Скоростной поисковый приемник. Генератор-излучатель виброакустического шума. Портативный металлодетектор. Имитатор закладных устройств. Стенды лабораторные. Автоматизированный комплекс «Сигурд-М19». Комплект дополнительного оборудования для системы Сигурд-М19. Стол поворотный диэлектрический управляемый. Комплекс оценки защищенности выделенных помещений по виброакустическому каналу. Цифровой осциллограф. Автоматизированный комплекс «Талис-НЧ-М1». Учебный лабораторный стенд «Основы цифровой электроники и микропроцессорной техники» с осциллографом. Комплект учебной мебели.
Самостоятельная работа	Помещения для самостоятельной работы; Персональные компьютеры с выходом в сеть Интернет. Комплект учебной мебели.

Учебные аудитории для проведения учебных занятий, оснащены оборудованием и техническими средствами обучения.

Помещения для самостоятельной работы обучающихся, оснащенные компьютерной техникой с возможностью подключения к сети "Интернет" и обеспечением доступа к электронной информационно-образовательной среде.

11. Особенности освоения дисциплины (модуля) лицами с ограниченными возможностями здоровья

Обучающимся с ограниченными возможностями здоровья предоставляются специальные учебники, учебные пособия и дидактические материалы, специальные технические средства обучения коллективного и индивидуального пользования, услуги ассистента (помощника), оказывающего обучающимся необходимую техническую помощь, а также услуги сурдопереводчиков и тифлосурдопереводчиков.

Освоение дисциплины (модуля) обучающимися с ограниченными возможностями здоровья может быть организовано совместно с другими обучающимися, а также в отдельных группах.

Освоение дисциплины (модуля) обучающимися с ограниченными возможностями здоровья осуществляется с учетом особенностей психофизического развития, индивидуальных возможностей и состояния здоровья.

В целях доступности получения высшего образования по образовательной программе лицами с ограниченными возможностями здоровья при освоении дисциплины (модуля) обеспечивается:

1) для лиц с ограниченными возможностями здоровья по зрению:

- присутствие ассистента, оказывающий студенту необходимую техническую помощь с учетом индивидуальных особенностей (помогает занять рабочее место, передвигаться, прочитать и оформить задание, в том числе, записывая под диктовку),
- письменные задания, а также инструкции о порядке их выполнения оформляются увеличенным шрифтом;

- специальные учебники, учебные пособия и дидактические материалы (имеющие крупный шрифт или аудиофайлы),

- индивидуальное равномерное освещение не менее 300 люкс,

- при необходимости студенту для выполнения задания предоставляется увеличивающее устройство;

2) для лиц с ограниченными возможностями здоровья по слуху:

- присутствие ассистента, оказывающий студенту необходимую техническую помощь с учетом индивидуальных особенностей (помогает занять рабочее место, передвигаться, прочитать и оформить задание, в том числе, записывая под диктовку),

- обеспечивается наличие звукоусиливающей аппаратуры коллективного пользования, при необходимости обучающемуся предоставляется звукоусиливающая аппаратура индивидуального пользования;

- обеспечивается надлежащими звуковыми средствами воспроизведения информации;

3) для лиц с ограниченными возможностями здоровья, имеющих нарушения опорно-двигательного аппарата (в том числе с тяжелыми нарушениями двигательных функций верхних конечностей или отсутствием верхних конечностей):

- письменные задания выполняются на компьютере со специализированным программным обеспечением или надиктовываются ассистенту;

- по желанию студента задания могут выполняться в устной форме.