Министерство науки и высшего образования Российской Федерации
Федеральное государственное автономное образовательное учреждение высшего образования

Пермский национальный исследовательский политехнический университет

УТВЕРЖДАЮ
Проректор по образовательной деятельности

_____ А.Б. Петроченков

« 06 » апреля 20 23 г.

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ

Дисциплина: Методы проектирования открытых информационных систем
(наименование)

Форма обучения: очная
(очная/очно-заочная/заочная)

Уровень высшего образования: специалитет
(бакалавриат/специалитет/магистратура)

Общая трудоёмкость: 288 (8)
(часы (ЗЕ))

Направление подготовки: 10.05.03 Информационная безопасность автоматизированных систем
(код и наименование направления)

Направленность: Безопасность открытых информационных систем (СУОС)
(наименование образовательной программы)

Пермь 2023

1. Общие положения

1.1. Цели и задачи дисциплины

Формирование комплекса знаний, умений и навыков в области проектирования систем защиты информации в распределенных информационных системах

1.2. Изучаемые объекты дисциплины

методы и средства защиты информации в корпоративных вычислительных сетях и системах; основные угрозы информации в современных сложных сетевых инфор-мационных системах; программные, программно-аппаратные и аппаратные сред-ства защиты информации, применяемые при обеспечении комплексной информа-ционной безопасности; программные средства анализа текущего уровня защищен-ности; современные технологии построения безопасных информационных систем и сетей.

1.3. Входные требования

Безопасность ОС, безопасность БД, безопасность компьютерных сетей

2. Планируемые результаты обучения по дисциплине

Компетенция	Индекс индикатора	Планируемые результаты обучения по дисциплине (знать, уметь, владеть)	Индикатор достижения компетенции, с которым соотнесены планируемые результаты обучения	Средства оценки

Компетенция	Индекс индикатора	Планируемые результаты обучения по дисциплине (знать, уметь, владеть)	Индикатор достижения компетенции, с которым соотнесены планируемые результаты обучения	Средства оценки
ПК-1.3	ИД-1ПК-1.3	основные угрозы информации в информационных системах и сетях; современные программные и аппаратные средства криптографической защиты информации; современную классификацию средств защиты информации в корпоративных вычислительных сетях и системах; этапы и технологию проектирования и создания безопасных информационных систем; современную нормативно-правовую базу создания защищенных распределенных информационных систем; инструментальные программные и аппаратные средства анализа защищенности информационных систем и сетей.	Знает эталонную модель взаимодействия открытых систем; основные угрозы безопасности информации и модели нарушителя в автоматизированных системах; основные меры по защите информации в автоматизированных системах	Тест
ПК-1.3	ИД-2ПК-1.3	проектировать комплексную защищенную инфраструктуру для типовых современных применений, отвечающую предъявляемым требованиям к уровню защищенности; разрабатывать модели информационно-технологических ресурсов, модели угроз и модели нарушителя информационной безопасности в распределенных информационных	Умеет анализировать основные узлы и устройства современных автоматизированных систем	Отчёт по практическому занятию

Компетенция	Индекс индикатора	Планируемые результаты обучения по дисциплине (знать, уметь, владеть)	Индикатор достижения компетенции, с которым соотнесены планируемые результаты обучения	Средства оценки
		системах; применять современные программные средства криптографической защиты информации; применять современные аппаратные средства защиты информационных процессов в компьютерных системах; применять современные аппаратные средства защиты информационных процессов при аудите распределенных компьютерных систем.		
ПК-1.3	ИД-3ПК-1.3	навыки разработки комплексной инфраструктуры защищенной информационной системы; навыки работы с программными и аппаратными средствами защиты информации.	Владеет навыками применения действующей нормативной базы в области обеспечения безопасности информации	Защита лабораторной работы

3. Объем и виды учебной работы

Вид учебной работы	Всего часов	Распределение по семестрам в часах	
		Номер семестра	
		9	10
1. Проведение учебных занятий (включая проведение текущего контроля успеваемости) в форме: 1.1. Контактная аудиторная работа, из них:	108	72	36
- лекции (Л)	24	16	8
- лабораторные работы (ЛР)	48	32	16
- практические занятия, семинары и (или) другие виды занятий семинарского типа (ПЗ)	30	20	10
- контроль самостоятельной работы (КСР)	6	4	2
- контрольная работа			
1.2. Самостоятельная работа студентов (СРС)	144	72	72
2. Промежуточная аттестация			
Экзамен	36		36
Дифференцированный зачет	9	9	
Зачет			
Курсовой проект (КП)	36		36
Курсовая работа (КР)			
Общая трудоемкость дисциплины	288	144	144

4. Содержание дисциплины

Наименование разделов дисциплины с кратким содержанием	Объем аудиторных занятий по видам в часах			Объем внеаудиторных занятий по видам в часах
	Л	ЛР	ПЗ	СРС
9-й семестр				
Проектирование защищенных распределенных информационных систем	16	32	20	72
Введение. Модели распределенных информационных систем (РИС). Модель РИС как объекта атаки-защиты Архитектуры, защищенных РИС Особенности разработки политики безопасности РИС				
ИТОГО по 9-му семестру	16	32	20	72
10-й семестр				
Технические механизмы и средства обеспечения информационной безопасности защищенных распределенных информационных систем.	8	16	10	72
Криптографические средства защиты Межсетевое экранирование Системы обнаружения и предотвращения вторжений Инструментальные средства аудита безопасности РИС				

Наименование разделов дисциплины с кратким содержанием	Объем аудиторных занятий по видам в часах			Объем внеаудиторных занятий по видам в часах
	Л	ЛР	ПЗ	СРС
ИТОГО по 10-му семестру	8	16	10	72
ИТОГО по дисциплине	24	48	30	144

Тематика примерных практических занятий

№ п.п.	Наименование темы практического (семинарского) занятия
1	Классификация нарушителей, модель нарушителя в РИУС
2	Модель угроз распределенной информационно-управляющей системы
3	Модель РИУС как объекта атаки-защиты
4	Особенности политики аутентификации пользователей распределенной информационно-управляющей системы
5	Механизмы и технологии аутентификации распределенной информационно-управляющей системы
6	Особенности реализации семейств безопасности в политике безопасности распределенной информационно-управляющей системы
7	Не технические меры обеспечения безопасности распределенной информационно-управляющей системы
8	Аудит, технический аудит и оценка безопасности распределенной информационно-управляющей системы
9	Технологии и средства анализа уязвимостей распределенной информационно-управляющей системы

Тематика примерных лабораторных работ

№ п.п.	Наименование темы лабораторной работы
1	Защита компьютерных сетей от атак на конфиденциальность и целостность
2	Защита серверов приложений и данных
3	Аудит и мониторинг инцидентов информационной безопасности

Тематика примерных курсовых проектов/работ

№ п.п.	Наименование темы курсовых проектов/работ
1	Модели распределенных информационно-управляющих систем
2	Архитектуры и моделирование защищенных распределенных информационно-управляющих систем
3	Аудит информационной безопасности в РИУС
4	Проектирование защищенных распределенных информационно-управляющих систем

№ п.п.	Наименование темы курсовых проектов/работ
5	Ключевые инструменты защиты информации в распределенных информационных системах

5. Организационно-педагогические условия

5.1. Образовательные технологии, используемые для формирования компетенций

Проведение лекционных занятий по дисциплине основывается на активном методе обучения, при котором учащиеся не пассивные слушатели, а активные участники занятия, отвечающие на вопросы преподавателя. Вопросы преподавателя нацелены на активизацию процессов усвоения материала, а также на развитие логического мышления. Преподаватель заранее намечает список вопросов, стимулирующих ассоциативное мышление и установление связей с ранее освоенным материалом.

Практические занятия проводятся на основе реализации метода обучения действием: определяются проблемные области, формируются группы. При проведении практических занятий преследуются следующие цели: применение знаний отдельных дисциплин и креативных методов для решения проблем и приятия решений; отработка у обучающихся навыков командной работы, межличностных коммуникаций и развитие лидерских качеств; закрепление основ теоретических знаний.

Проведение лабораторных занятий основывается на интерактивном методе обучения, при котором обучающиеся взаимодействуют не только с преподавателем, но и друг с другом. При этом доминирует активность учащихся в процессе обучения. Место преподавателя в интерактивных занятиях сводится к направлению деятельности обучающихся на достижение целей занятия.

При проведении учебных занятий используются интерактивные лекции, групповые дискуссии, ролевые игры, тренинги и анализ ситуаций и имитационных моделей.

5.2. Методические указания для обучающихся по изучению дисциплины

При изучении дисциплины обучающимся целесообразно выполнять следующие рекомендации:

1. Изучение учебной дисциплины должно вестись систематически.
2. После изучения какого-либо раздела по учебнику или конспектным материалам рекомендуется по памяти воспроизвести основные термины, определения, понятия раздела.
3. Особое внимание следует уделить выполнению отчетов по практическим занятиям, лабораторным работам и индивидуальным комплексным заданиям на самостоятельную работу.
4. Вся тематика вопросов, изучаемых самостоятельно, задается на лекциях преподавателем. Им же даются источники (в первую очередь вновь изданные в периодической научной литературе) для более детального понимания вопросов, озвученных на лекции.

6. Перечень учебно-методического и информационного обеспечения для самостоятельной работы обучающихся по дисциплине

6.1. Печатная учебно-методическая литература

№ п/п	Библиографическое описание (автор, заглавие, вид издания, место, издательство, год издания, количество страниц)	Количество экземпляров в библиотеке
1. Основная литература		

1	Гольдштейн Б. С. Сети связи : учебник для вузов / Б. С. Гольдштейн, Н. А. Соколов, Г. Г. Яновский. - Санкт-Петербург: БХВ-Петербург, 2011.	2
2	Мельников Д. А. Информационная безопасность открытых систем : учебник / Д. А. Мельников. - Москва: Флинта, Наука, 2013.	11
2. Дополнительная литература		
2.1. Учебные и научные издания		
1	Основы управления информационной безопасностью : учебное пособие для вузов / А. П. Курило [и др.] .— 2-е изд., испр .— Москва : Горячая линия-Телеком, 2014 .— 243 с.	15
2.2. Периодические издания		
	Не используется	
2.3. Нормативно-технические издания		
	Не используется	
3. Методические указания для студентов по освоению дисциплины		
	Не используется	
4. Учебно-методическое обеспечение самостоятельной работы студента		
	Не используется	

6.2. Электронная учебно-методическая литература

Вид литературы	Наименование разработки	Ссылка на информационный ресурс	Доступность (сеть Интернет / локальная сеть; авторизованный / свободный доступ)
Методические указания для студентов по освоению дисциплины	Практикум «Методы проектирования защищенных распределенных информационных систем»	online.at.pstu.ru	локальная сеть; авторизованный доступ
Основная литература	«Методы проектирования защищенных распределенных информационных систем» Учебно-методическое пособие	online.at.pstu.ru	локальная сеть; авторизованный доступ

6.3. Лицензионное и свободно распространяемое программное обеспечение, используемое при осуществлении образовательного процесса по дисциплине

Вид ПО	Наименование ПО
Операционные системы	Debian (GNU GPL)
Операционные системы	Windows 10 (подп. Azure Dev Tools for Teaching)
Прикладное программное обеспечение общего назначения	Dr.Web Enterprise Security Suite, 3000 лиц, ПНИПУ ОЦНИТ 2017
Прикладное программное обеспечение общего назначения	VMware Workstation Player (VMware Academic)

Вид ПО	Наименование ПО
Прикладное программное обеспечение общего назначения	Wireshark
Системы управления проектами, исследованиями, разработкой, проектированием, моделированием и внедрением	EVE NG Community Edition (Free Edition)
Среды разработки, тестирования и отладки	Microsoft Visual Studio (подп. Azure Dev Tools for Teaching)

6.4. Современные профессиональные базы данных и информационные справочные системы, используемые при осуществлении образовательного процесса по дисциплине

Наименование	Ссылка на информационный ресурс
База данных Scopus	https://www.scopus.com/
База данных научной электронной библиотеки (eLIBRARY.RU)	https://elibrary.ru/
База данных уязвимостей CVE Mitre	https://cve.mitre.org/
Банк данных угроз безопасности информации Федеральной службы по техническому и экспортному контролю	https://bdu.fstec.ru/
Научная библиотека Пермского национального исследовательского политехнического университета	http://lib.pstu.ru/
Электронно-библиотечеая система Лань	https://e.lanbook.com/
Электронно-библиотечная система IPRbooks	http://www.iprbookshop.ru/
Информационные ресурсы Сети КонсультантПлюс	http://www.consultant.ru/
Электронная библиотека диссертаций Российской государственной бибилиотеки	http://www.diss.rsl.ru/
База данных компании EBSCO	https://www.ebsco.com/
Информационно-справочная система нормативно-технической документации "Техэксперт: нормы, правила, стандарты и законодательства России"	https://техэксперт.сайт/

7. Материально-техническое обеспечение образовательного процесса по дисциплине

Вид занятий	Наименование необходимого основного оборудования и технических средств обучения	Количество единиц
Курсовой проект	Все компьютеры с возможностью подключения к сети Интернет и обеспечением доступа в электрон-ную образовательную среду	20
Лабораторная работа	Все компьютеры с возможностью подключения к сети Интернет и обеспечением доступа в электрон-ную образовательную среду	20
Лекция	ПК преподавателя, проектор Mitsubishi SL4SU – 1шт., экран – 1 шт., доска	1
Практическое занятие	Все компьютеры с возможностью подключения к сети Интернет и обеспечением доступа в электрон-ную образовательную среду	20

8. Фонд оценочных средств дисциплины

Описан в отдельном документе

Министерство науки и высшего образования Российской Федерации
Федеральное государственное автономное образовательное учреждение высшего образования
«Пермский национальный исследовательский политехнический университет»

ФОНД ОЦЕНОЧНЫХ СРЕДСТВ
для проведения промежуточной аттестации обучающихся по дисциплине «Методы проектирования открытых информационных систем»
Приложение к рабочей программе дисциплины

Направление подготовки: 10.05.03 Информационная безопасность открытых систем

Направленность (профиль) образовательной программы: Безопасность открытых информационных систем

Квалификация выпускника: Специалист

Выпускающая кафедра: Автоматика и телемеханика

Форма обучения: Очная

Курс: 5 **Семестр**: 9, 10

Трудоёмкость:
Кредитов по рабочему учебному плану: 8 ЗЕ
Часов по рабочему учебному плану: 288 ч.

Форма промежуточной аттестации:
Экзамен: 10 семестр
Курсовой проект: 10 семестр
Зачет с оценкой: 9 семестр

Пермь 2021

Фонд оценочных средств для проведения промежуточной аттестации обучающихся для проведения промежуточной аттестации обучающихся по дисциплине является частью (приложением) к рабочей программе дисциплины. Фонд оценочных средств для проведения промежуточной аттестации обучающихся по дисциплине разработан в соответствии с общей частью фонда оценочных средств для проведения промежуточной аттестации основной образовательной программы, которая устанавливает систему оценивания результатов промежуточной аттестации и критерии выставления оценок**.** Фонд оценочных средств для проведения промежуточной аттестации обучающихся по дисциплине устанавливает формы и процедуры текущего контроля успеваемости и промежуточной аттестации обучающихся по дисциплине.

1. Перечень контролируемых результатов обучения по дисциплине, объекты оценивания и виды контроля

Согласно РПД, освоение учебного материала дисциплины запланировано в течение одного семестра (9-го и 10-го семестра учебного плана) и разбито на 3 учебных модуля. В каждом модуле предусмотрены аудиторные лекционные и лабораторные занятия, а также самостоятельная работа студентов. В рамках освоения учебного материала дисциплины формируется компоненты компетенций *знать, уметь, владеть*, указанные в РПД, которые выступают в качестве контролируемых результатов обучения по дисциплине (табл. 1.1).

Контроль уровня усвоенных знаний, освоенных умений и приобретенных владений осуществляется в рамках текущего, рубежного и промежуточного контроля при изучении теоретического материала, сдаче отчетов по лабораторным работам и экзамена. Виды контроля сведены в таблицу 1.1.

Таблица 1.1. Перечень контролируемых результатов обучения по дисциплине

Контролируемые результаты обучения по дисциплине (ЗУВы)	**Вид контроля**					
	Текущий		**Рубежный**		**Итоговый**	
	С	**ТО**	**ОЛР**	**Т/КР**		**Экзамен**
Усвоенные знания						
З.1 Знает основные угрозы информации в информационных системах и сетях; современные программные и аппаратные средства криптографической защиты информации; современную классификацию средств защиты информации в корпоративных вычислительных сетях и системах; этапы и технологию проектирования и создания безопасных информационных систем; современную нормативно-правовую базу создания защищенных распределенных информационных систем; инструментальные программные и аппаратные средства анализа защищенности информационных систем и сетей		ТО1 ТО2 ТО3	ОЛР1 ОЛР2 ОЛР3	КР1		КЗ
Освоенные умения						
У.1 Умеет использовать современные программные и аппаратные средства криптографической защиты информации; современную классификацию средств защиты информации в корпоративных вычислительных сетях и системах; этапы и			ОЛР1 ОЛР2 ОЛР3	КР1		КЗ

технологию проектирования и создания безопасных информационных систем; современную нормативно-правовую базу создания защищенных распределенных информационных систем; инструментальные программные и аппаратные средства анализа защищенности информационных систем и сетей основные угрозы информации в информационных системах и сетях; современные программные и аппаратные средства криптографической защиты информации; современную классификацию средств защиты информации в корпоративных вычислительных сетях и системах; этапы и технологию проектирования и создания безопасных информационных систем; современную нормативно-правовую базу создания защищенных распределенных информационных систем; инструментальные программные и аппаратные средства анализа защищенности информационных систем и сетей						
Приобретенные владения						
В.1. Владеет навыками разработки комплексной инфраструктуры защищенной информационной системы; навыки работы с программными и аппаратными средствами защиты информации.			ОЛР1 ОЛР2 ОЛР3	КР1		КЗ

С – собеседование по теме; ТО – коллоквиум (теоретический опрос); КЗ – кейс-задача (индивидуальное задание); ОЛР – отчет по лабораторной работе; Т/КР – рубежное тестирование (контрольная работа, курсовая работа); ТВ – теоретический вопрос; ПЗ – практическое задание; КЗ – комплексное задание экзамена.

Итоговой оценкой достижения результатов обучения по дисциплине является промежуточная аттестация в виде экзамена, проводимая с учетом результатов текущего и рубежного контроля.

2. Виды контроля, типовые контрольные задания и шкалы оценивания результатов обучения

Текущий контроль успеваемости имеет целью обеспечение максимальной эффективности учебного процесса, управление процессом формирования заданных компетенций обучаемых, повышение мотивации к учебе и предусматривает оценивание хода освоения дисциплины. В соответствии с Положением о проведении текущего контроля успеваемости и промежуточной аттестации обучающихся по образовательным программам высшего образования – программам бакалавриата, специалитета и магистратуры в ПНИПУ предусмотрены следующие виды и периодичность текущего контроля успеваемости обучающихся:

- входной контроль, проверка исходного уровня подготовленности обучаемого и его соответствия предъявляемым требованиям для изучения данной дисциплины;

- текущий контроль усвоения материала (уровня освоения компонента «знать» заданных компетенций) на каждом групповом занятии и контроль посещаемости лекционных занятий;

- промежуточный и рубежный контроль освоения обучаемыми отдельных компонентов «знать», «уметь» заданных компетенций путем компьютерного или бланочного тестирования, контрольных опросов, контрольных работ (индивидуальных домашних заданий), защиты отчетов по лабораторным работам, рефератов, эссе и т.д.

Рубежный контроль по дисциплине проводится на следующей неделе после прохождения модуля дисциплины, а промежуточный – во время каждого контрольного мероприятия внутри модулей дисциплины;

- межсессионная аттестация, единовременное подведение итогов текущей успеваемости не менее одного раза в семестр по всем дисциплинам для каждого направления подготовки (специальности), курса, группы;

- контроль остаточных знаний.

2.1. Текущий контроль усвоения материала

Текущий контроль усвоения материала в форме собеседования или выборочного теоретического опроса студентов проводится по каждой теме. Результаты по 4-балльной шкале оценивания заносятся в книжку преподавателя и учитываются в виде интегральной оценки при проведении промежуточной аттестации.

2.2. Рубежный контроль

Рубежный контроль для комплексного оценивания усвоенных знаний, освоенных умений и приобретенных владений (табл. 1.1) проводится в форме защиты лабораторных работ (после изучения каждого модуля учебной дисциплины) и курсовой работы (после изучения всех модулей учебной дисциплины).

Всего запланировано 3 лабораторных работ. Типовые темы лабораторных работ приведены в РПД.

Защита лабораторной работы проводится индивидуально каждым студентом. Типовые шкала и критерии оценки приведены в общей части ФОС образовательной программы.

Тема курсового проекта приведена в РПД. Курсовой проект содержит расчетную часть и практическое задание.

Защита курсового проекта проводится индивидуально каждым студентом путем собеседования по расчетной части и демонстрации результатов разработки программной модели. Типовые шкала и критерии оценки приведены в общей части ФОС образовательной программы.

2.3. Промежуточная аттестация (итоговый контроль)

Допуск к промежуточной аттестации осуществляется по результатам текущего и рубежного контроля. Условиями допуска являются успешная сдача всех лабораторных работ и положительная интегральная оценка по результатам текущего и рубежного контроля.

Промежуточная аттестация, согласно РПД, проводится в виде экзамена по дисциплине устно по билетам. Билет содержит теоретические вопросы (ТВ) для проверки усвоенных знаний и практические задания (ПЗ) для проверки освоенных умений всех заявленных компетенций.

Билет формируется таким образом, чтобы в него попали вопросы и практические задания, контролирующие уровень сформированности ***всех*** заявленных компетенций. Форма билета представлена в общей части ФОС образовательной программы.

2.3.1. Типовые вопросы и задания для экзамена по дисциплине

Типовые вопросы для контроля усвоенных знаний:

1. Классификация нарушителей, модель нарушителя в РИУС
2. Модель угроз распределенной информационно-управляющей системы
3. Модель угроз распределенной информационно-управляющей системы
4. Особенности политики аутентификации пользователей распределенной информационно-управляющей системы
5. Механизмы и технологии аутентификации распределенной информационно-управляющей системы
6. Особенности реализации семейств безопасности в политике безопасности распределенной информационно-управляющей системы
7. Не технические меры обеспечения безопасности распределенной информационно-управляющей системы
8. Аудит, технический аудит и оценка безопасности распределенной информационно-управляющей системы
9. Технологии и средства анализа уязвимостей распределенной информационно-управляющей системы

Типовые вопросы и практические задания для контроля освоенных умений:

1. Защита компьютерных сетей от атак на конфиденциальность и целостность
2. Защита серверов приложений и данных
3. Аудит и мониторинг инцидентов информационной безопасности

2.3.2. Шкалы оценивания результатов обучения на экзамене

Оценка результатов обучения по дисциплине в форме уровня сформированности компонентов *знать, уметь, владеть* заявленных компетенций проводится по 4-х балльной шкале оценивания путем выборочного контроля во время экзамена.

Типовые шкала и критерии оценки результатов обучения при сдаче экзамена для компонентов *знать, уметь и владеть* приведены в общей части ФОС образовательной программы.

3. Критерии оценивания уровня сформированности компонентов и компетенций

3.1. Оценка уровня сформированности компонентов компетенций

При оценке уровня сформированности компетенций в рамках выборочного контроля при экзамене считается, что *полученная оценка за компонент проверяемой в билете компетенции обобщается на соответствующий компонент всех компетенций, формируемых в рамках данной учебной дисциплины*.

Типовые критерии и шкалы оценивания уровня сформированности компонентов компетенций приведены в общей части ФОС образовательной программы.

3.2. Оценка уровня сформированности компетенций

Общая оценка уровня сформированности всех компетенций проводится путем агрегирования оценок, полученных студентом за каждый компонент формируемых компетенций, с учетом результатов текущего и рубежного контроля в виде

интегральной оценки по 4-х балльной шкале. Все результаты контроля заносятся в оценочный лист и заполняются преподавателем по итогам промежуточной аттестации.

Форма оценочного листа и требования к его заполнению приведены в общей части ФОС образовательной программы.

При формировании итоговой оценки промежуточной аттестации в виде экзамена используются типовые критерии, приведенные в общей части ФОС образовательной программы.