

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

« 15 » мая 20 23 г.

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ

Дисциплина: Методы и средства обеспечения информационной безопасности
компьютерных и программных систем
_____ (наименование)

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

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

Общая трудоёмкость: _____ 108 (3)
(часы (ЗЕ))

Направление подготовки: _____ 09.03.01 Информатика и вычислительная техника
(код и наименование направления)

Направленность: Информатика и вычислительная техника (общий профиль,
СУОС)
_____ (наименование образовательной программы)

1. Общие положения

1.1. Цели и задачи дисциплины

Цель учебной дисциплины - получение знаний в области изучения и создания современных распределенных защищенных информационных систем различного применения и степени сложности.

Задачи учебной дисциплины:

- Изучение технологий проектирования и создания безопасных распределенных компьютерных и программных систем; классификации средств защиты информации в корпоративных вычислительных сетях и системах; инструментальных программных и аппаратных средств анализа их защищенности;
- Формирование умений в разработке проектов защищенных компьютерных и программных систем для типовых современных применений, отвечающих предъявляемым требованиям к уровню защищенности, выполняемых с использованием современных программных, программно-аппаратных и аппаратных средств защиты информации;
- Овладение навыками разработки и внедрения защищенной компьютерной и программной системы, включающих навыки базовой и расширенной настройки и использования современных программных и аппаратных средств защиты информации.

1.2. Изучаемые объекты дисциплины

Предметом освоения дисциплины являются следующие объекты:

- методы и средства защиты информации в компьютерных и программных системах;
- основные угрозы информации в современных сложных сетевых информационных системах;
- программные, программно-аппаратные и аппаратные средства защиты информации, применяемые при обеспечении информационной безопасности;
- программные средства анализа текущего уровня защищенности;
- современные технологии построения безопасных информационных систем.

1.3. Входные требования

Не предусмотрены

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-2.3	ИД-1ПК-2.3	<p>Знает:</p> <ul style="list-style-type: none"> - основные угрозы информации в информационных системах и сетях; современные программные и аппаратные средства крипто-графической защиты информации; - современную классификацию средств защиты информации от несанкционированного доступа операционных систем и систем управления базами данных; технологию проектирования и создания безопасных информационных систем; - современную нормативно-правовую базу создания защищенных распределенных информационных систем; - инструментальные программные и аппаратные средства анализа защищенности компьютерных и программных систем. 	Знает средства защиты от несанкционированного доступа операционных систем и систем управления базами данных.	Зачет
ПК-2.3	ИД-2ПК-2.3	<p>Умеет:</p> <ul style="list-style-type: none"> - применять современные программные средства защиты информации; конфигурировать и настраивать современные аппаратные средства защиты информационных процессов в компьютерных системах; - применять современные аппаратные средства защиты информационных процессов при аудите распределенных компьютерных и программных систем. 	Умеет конфигурировать сетевые устройства.	Защита лабораторной работы

Компетенция	Индекс индикатора	Планируемые результаты обучения по дисциплине (знать, уметь, владеть)	Индикатор достижения компетенции, с которым соотнесены планируемые результаты обучения	Средства оценки
ПК-2.3	ИД-3ПК-2.3	Владеет: - навыками разработки защищенной информационной системы; - навыками настройки и конфигурирования программных и аппаратных средств защиты информации.	Владеет навыками настройки параметров управления безопасностью операционных систем сетевых устройств.	Защита лабораторной работы

3. Объем и виды учебной работы

Вид учебной работы	Всего часов	Распределение по семестрам в часах	
		Номер семестра	
		7	
1. Проведение учебных занятий (включая проведение текущего контроля успеваемости) в форме:	44	44	
1.1. Контактная аудиторная работа, из них:			
- лекции (Л)	14	14	
- лабораторные работы (ЛР)	28	28	
- практические занятия, семинары и (или) другие виды занятий семинарского типа (ПЗ)			
- контроль самостоятельной работы (КСР)	2	2	
- контрольная работа			
1.2. Самостоятельная работа студентов (СРС)	64	64	
2. Промежуточная аттестация			
Экзамен			
Дифференцированный зачет			
Зачет	9	9	
Курсовой проект (КП)			
Курсовая работа (КР)			
Общая трудоемкость дисциплины	108	108	

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	
7-й семестр				

Наименование разделов дисциплины с кратким содержанием	Объем аудиторных занятий по видам в часах			Объем внеаудиторных занятий по видам в часах
	Л	ЛР	ПЗ	СРС
Принципы построения структуры и защиты информации в компьютерных и программных системах различного типа	6	6	0	18
Основные типы сетей (лабораторно-учебные, локальные, локально-виртуальные, частные, провайдерские, кампусные, городские, глобальные, корпоративно- распределенные) их структура, назначение. Основные угрозы информации в компьютерных и программных системах; современные программные и аппаратные средства защиты информации, классификация средств защиты информации в корпоративных вычислительных сетях и системах.				
Программные и аппаратные средства анализа защищенности информационных систем и обеспечения информационной безопасности	2	6	0	16
Администрирование сетей, парольная защита, антивирусная защита, межсетевые экраны, брандмауэры, фаерволы. Виртуальные сети. Виртуальные частные сети. Установление TCP-соединения. Пакетные фильтры. Пограничные роутеры.				
Методы обеспечения защиты компьютерных и программных систем	6	16	0	30
Криптографическое обеспечение защиты информации. Система IPSEC, SSL, TLS. Администрирование web- сервера. Создание логов. Процедуры создания backup web-сервера. Конфигурирование и настройка брандмауэров и фаерволов. Использование методов идентификации и аутентификации. Аутентификация, основанная на IP-адресе. Контроль целостности данных.				
ИТОГО по 7-му семестру	14	28	0	64
ИТОГО по дисциплине	14	28	0	64

Тематика примерных лабораторных работ

№ п.п.	Наименование темы лабораторной работы
1	Создание сети из двух компьютеров
2	Создание коммутируемой компьютерной сети
3	Подключение и основные настройки межсетевого экрана, управление через консоль, Web-интерфейс, SSH
4	Настройка доступа в Интернет и маршрутизации. Способы подключения к Интернет-провайдеру с использованием межсетевого экрана

№ п.п.	Наименование темы лабораторной работы
5	Аутентификация пользователей. Встроенная база данных, внешние базы данных – RADIUS, LDAP, Active Directory
6	Виртуальные частные сети IPsec/PPTP/L2TP/SSL VPN
7	Защита почтового сервера и почтовых клиентов с помощью SMTP, POP3. Антиспам-фильтр
8	Настройка VLAN
9	Защита от сетевых атак. Защита от атак типа «отказ в обслуживании» DoS, встроенные механизмы защиты
10	Организация антивирусной защиты. Обновление, использование.

5. Организационно-педагогические условия

5.1. Образовательные технологии, используемые для формирования компетенций

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

5.2. Методические указания для обучающихся по изучению дисциплины

<p>При изучении дисциплины обучающимся целесообразно выполнять следующие рекомендации:</p> <ol style="list-style-type: none"> 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 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

№ п/п	Библиографическое описание (автор, заглавие, вид издания, место, издательство, год издания, количество страниц)	Количество экземпляров в библиотеке
1. Основная литература		
1	Мельников Д. А. Информационная безопасность открытых систем : учебник / Д. А. Мельников. - Москва: Флинта, Наука, 2013.	11
2	Основы управления информационной безопасностью : учебное пособие для вузов / А. П. Курило [и др.]. - Москва: Горячая линия-Телеком, 2014.	15
2. Дополнительная литература		
2.1. Учебные и научные издания		
1	Галатенко В. А. Стандарты информационной безопасности : курс лекций : учебное пособие для вузов / В. А. Галатенко. - Москва: ИНТУИТ, 2006.	19
2	Информационная безопасность : учебное пособие / С. В. Петров [и др.]. - Новосибирск Москва: АРТА, 2012.	1
3	Мельников В. П. Информационная безопасность : учебник для вузов / В. П. Мельников, А. И. Куприянов, Т. Ю. Васильева. - Москва: Русайнс, 2017.	2
4	Теоретические основы компьютерной безопасности : учебное пособие для вузов / П. Н. Девянин [и др.]. - Москва: Радио и связь, 2000.	30
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)
Дополнительная литература	Информационная безопасность и защита информации	https://znanium.com/catalog/document?id=364911	сеть Интернет; свободный доступ
Дополнительная литература	Информационная безопасность конструкций ЭВМ и систем	https://znanium.com/catalog/document?id=362430	сеть Интернет; свободный 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	MS Windows 8.1 (подп. Azure Dev Tools for Teaching)
Операционные системы	Windows 10 (подп. Azure Dev Tools for Teaching)
Офисные приложения.	LibreOffice 6.2.4. OpenSource, бесплатен.
Офисные приложения.	Microsoft Office Professional 2007. лиц. 42661567
Прикладное программное обеспечение общего назначения	Dr.Web Enterprise Security Suite, 3000 лиц, ПНИПУ ОЦНИТ 2017

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

Наименование	Ссылка на информационный ресурс
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-библиотечная система Лань	https://e.lanbook.com/
Электронно-библиотечная система IPRbooks	http://www.iprbookshop.ru/
Информационные ресурсы Сети КонсультантПлюс	http://www.consultant.ru/

7. Материально-техническое обеспечение образовательного процесса по дисциплине

Вид занятий	Наименование необходимого основного оборудования и технических средств обучения	Количество единиц
Лабораторная работа	персональный компьютер	30
Лекция	персональный компьютер (ноутбук), мультимедийный проектор, экран	1

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 и средства обеспечения информационной безопасности
компьютерных и программных систем»**

Приложение к рабочей программе дисциплины

Направление подготовки:	09.03.01 Информатика и вычислительная техника
Направленность (профиль) образовательной программы:	Информатика и вычислительная техника (общий профиль, СУОС)
Квалификация выпускника:	«Бакалавр»
Выпускающая кафедра:	Информационных технологий и автоматизированных систем (ИТАС)
Форма обучения:	Очная

Курс: 4 Семестр: 7

Трудоёмкость:

Кредитов по рабочему учебному плану: 3 ЗЕ

Часов по рабочему учебному плану: 108 ч.

Форма промежуточной аттестации:

Зачёт: 7 семестр

Пермь 2023 г.

Фонд оценочных средств 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 (7-го семестра учебного плана). Согласно РПД предусмотрены аудиторские лекционные и лабораторные занятия, а также самостоятельная работа студентов. В рамках освоения учебного материала дисциплины формируются компоненты компетенций *знать, уметь, владеть*, указанные в РПД, которые выступают в качестве контролируемых результатов обучения по дисциплине (таблица 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 зачёта. 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		Промежуточный /рубежный		Итоговый	
	С	ТО	ОЛР	Т/КР		Зачёт
Усвоенные знания						
3.1 знать средства защиты от несанкционированного доступа операционных систем и систем управления базами данных		ТО1				ТВ
Освоенные умения						
У.1 уметь конфигурировать сетевые устройства			ОЛР1			ПЗ
Приобретенные владения						
В.1 владеть навыками настройки параметров управления безопасностью операционных систем сетевых устройств			ОЛР2			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); ТВ – теоретический вопрос; ПЗ – практическое задание; КЗ – комплексное задание зачёта.

Итоговой оценкой достижения результатов обучения по дисциплине является промежуточная аттестация в виде зачёта, 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 бланчного 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 (промежуточный) контроль

Рубежный (промежуточный) контроль для комплексного оценивания усвоенных знаний, освоенных умений и приобретенных владений (таблица 1.1) проводится в форме защиты лабораторных работ.

2.2.1. Защита лабораторных работ

Всего запланировано 10 лабораторных работ. Типовые темы лабораторных работ приведены в РПД.

Защита лабораторной работы проводится индивидуально каждым студентом или группой студентов. 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 зачёта по дисциплине устно по билетам. Билет содержит теоретические вопросы (ТВ) для проверки усвоенных знаний, практические задания (ПЗ) для проверки освоенных умений и комплексные задания (КЗ) для контроля уровня приобретенных владений 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. Защита человека от опасной информации и от неинформированности в области информационной безопасности.
2. Информация, сообщения, информационные процессы как объекты информационной безопасности.
3. Классификация информации по видам тайны и степеням конфиденциальности.
4. Использование динамически изменяющегося пароля. Методы модификации схемы простых паролей.
5. Жизненные циклы конфиденциальной информации в процессе ее создания, обработки, передачи.
6. Модель интеграции информационной безопасности в основную деятельность организации.

Типовые вопросы и практические задания для контроля освоенных умений:

1. Определение объектов защиты на типовом объекте информатизации (по вариантам).
2. Классификация защищаемой информации по видам тайны и степеням конфиденциальности (по вариантам).
3. Понятие и подходы к построению модели угроз.
4. Виды и каналы утечки информации (по вариантам).
5. Основные методы реализации угроз информационной безопасности (по вариантам).
6. На основе ГОСТ Р ИСО/МЭК 17799-2005, и с точки зрения начальника отдела по вопросам информационной безопасности в небольшой организации разработать перечень мероприятий при привлечении сторонних организаций к обработке информации.

Типовые комплексные задания для контроля приобретенных владений:

1. Разрабатывается информационная система, которая, в том числе, должна обеспечить работу с информацией ограниченного доступа (коммерческой тайной). Составьте список действий, которые необходимо выполнить на этапе проектирования системы, ее ввода в действие и при эксплуатации.

2. Разрабатывается информационная система, которая, в том числе, должна обеспечить работу с персональными данными. Составьте список действий, которые необходимо выполнить на этапе проектирования системы, ее ввода в действие и при эксплуатации.

3. Пользователь получил сообщение от партнеров, зашифрованное. как сообщалось в письме, алгоритмом BlowFish, хэш Naval. Ранее пользователю был сообщен ключ. Как расшифровать сообщение и послать ответное сообщение, зашифрованное таким же образом и с тем же ключом? Проиллюстрируйте действия на примере с ключом QWERTY.

Полный перечень теоретических вопросов и практических заданий в форме утвержденного комплекта билетов для проведения зачёта хранится на выпускающей кафедре.

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.