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

« 02 » июня 20 23 г.

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ

Дисциплина: Информатика в приложении к отрасли
(наименование)

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

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

Общая трудоёмкость: 108 (3)
(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

Основными целями дисциплины являются расширение теоретической базы в предметной области и прививание студентам практических навыков по работе со специальными возможностями информационного обеспечения в области защиты информации.
Задачи дисциплины:
- изучение основных положений государственной политики в области обеспечения информационной безопасности Российской Федерации, основных понятий в области защиты информации и методологических принципов создания систем защиты информации;
- изучение угроз информационной безопасности, сущности и разновидностей информационного оружия, методов и средств ведения информационных войн;
- изучение методов и средств обеспечения информационной безопасности компьютерных систем;
- приобретение навыков анализа информационной инфраструктуры с точки зрения информационной безопасности, подбора способов и средств защиты информации.

1.2. Изучаемые объекты дисциплины

основные понятия, общеметодологические принципы теории информационной безопасности;
- основы государственной информационной политики по обеспечению безопасности информации;
- угрозы безопасности информации и уязвимости информационных систем;
- информационные войны и информационное оружие;
- методы нарушения конфиденциальности, целостности и доступности информации;
- причины, виды каналы утечки информации и несанкционированного доступа;
- уровни и сервисы защиты информации;
- способы и средства защиты информации;
- критерии оценки защищенности информационных систем;
- основы организации защиты информации на предприятии.

1.3. Входные требования

Информатика, теория проектирования 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
ОПК-4	ИД-1ОПК-4	Знает основополагающие принципы построения системы безопасности информационных систем в соответствии с требованиями регламентирующих документов в области информационной безопасности	Знает основополагающие принципы механики; основополагающие принципы термодинамики и молекулярной физики; основные положения электричества и магнетизма; основные положения колебаний и оптики; основополагающие принципы квантовой физики; основополагающие принципы работы элементов и функциональных узлов электронной аппаратуры; терминологию, основные руководящие и регламентирующие документы в области ЭВМ и вычислительных систем; дифференциальные уравнения простых электрических цепей; методы анализа электрических цепей в переходных и установившихся режимах в частотной и временной областях.	Отчёт по практическому занятию
ОПК-4	ИД-2ОПК-4	Умеет использовать ПО, позволяющее осуществлять сбор, обработку, анализ и систематизацию научно-технической информации в области информационной безопасности информационных систем	Умеет проводить физический эксперимент, обрабатывать его результаты и делать выводы о проделанной исследовательской работе; решать типовые прикладные физические задачи; работать с современной измерительной техникой; анализировать компонентную базу электронной аппаратуры; осуществлять сбор, обработку, анализ и систематизацию научно-технической информации в области ЭВМ и систем с применением	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
			современных информационных технологий	
ОПК-4	ИД-3ОПК-4	Владеет методами расчёта и построения безопасных сетей передачи информации. Владеет методами оценки возможных утечек по техническому электромагнитному каналу	Владеет методами расчета простых линейных и нелинейных электрических цепей	Отчёт по практическому занятию

3. Объем и виды учебной работы

Вид учебной работы	Всего часов	Распределение по семестрам в часах
		Номер семестра
		5
1. Проведение учебных занятий (включая проведение текущего контроля успеваемости) в форме: 1.1. Контактная аудиторная работа, из них:	45	45
- лекции (Л)	16	16
- лабораторные работы (ЛР)		
- практические занятия, семинары и (или) другие виды занятий семинарского типа (ПЗ)	27	27
- контроль самостоятельной работы (КСР)	2	2
- контрольная работа		
1.2. Самостоятельная работа студентов (СРС)	63	63
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	СРС
5-й семестр				
Безопасность передачи информации	6	0	11	21
1. Прикладные вопросы шифрования 2. Прикладные вопросы туннелирования трафика 3. ПО применяемое для контроля трафика				

Наименование разделов дисциплины с кратким содержанием	Объем аудиторных занятий по видам в часах			Объем внеаудиторных занятий по видам в часах
	Л	ЛР	ПЗ	СРС
Безопасность хранения информации	4	0	5	21
1. Прикладные вопросы обеспечения целостности и доступности 2. ПО применяемое для обеспечения целостности и доступности				
Автоматизированное проектирование систем безопасности	6	0	11	21
1. Вопросы проектирования безопасных сетей 2. Вопросы проектирования систем видео наблюдения 3. Прикладные вопросы проектирования систем противодействия злоумышленнику				
ИТОГО по 5-му семестру	16	0	27	63
ИТОГО по дисциплине	16	0	27	63

Тематика примерных практических занятий

№ п.п.	Наименование темы практического (семинарского) занятия
1	Шифрование с симметричным и ассимитричным ключом, теория оценки их криптостойкости
2	Создание безопасного соединения двух участков сети (VPN)
3	Создание RAID массивов
4	DLP системы, контроль информационных потоков
5	Автоматизированныесистемы проектирования систем видеонаблюдения

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.

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 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	Запечников С. В., Милославская Н. Г., Толстой А. И. Основы построения виртуальных частных сетей : учебное пособие для вузов. 2-е изд., стер Москва : Горячая линия-Телеком, 2011. 248 с. 15,5 усл. печ. л.	15
2	Левин М. PGP: Кодирование и шифрование информации с открытым ключом. Москва : Майор, 2001. 167 с.	1
3	Росляков А. В. Виртуальные частные сети. Основы построения и применения. Москва : Эко-Трендз, 2006. 301 с.	2
4	Столлингс В. Основы защиты сетей. Приложение с стандарты : пер. с англ. Москва [и др.] : Вильямс, 2002. 429 с.	7
5	Таненбаум Э. С. Компьютерные сети : пер. с англ. 3-е изд Санкт-Петербург [и др.] : Питер, 2002. 846 с.	5
6	Таненбаум Э. С. Современные операционные системы. 2-е изд Санкт-Петербург [и др.] : Питер, 2002. 1037 с.	7
7	Ярочкин В. И. Информационная безопасность : учебник для вузов. 2-е изд Москва : Акад. проект : Гаудеамус, 2004. 543 с.	18
2. Дополнительная литература		
2.1. Учебные и научные издания		
1	Данилов А. Н., Данилова С. А., Зорин А. А. Основы информационной безопасности : учебное пособие. Пермь : Изд-во ПГТУ, 2008. 555 с.	62
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		

1	Данилов А. Н., Кротова Е. Л., Липин Ю. Н. Практикум по курсам Математические основы криптологии и Криптографические методы и средства обеспечения информационной безопасности : учебное пособие. Пермь : Изд-во ПГТУ, 2008. 238 с.	59

6.2. Электронная учебно-методическая литература

Вид литературы	Наименование разработки	Ссылка на информационный ресурс	Доступность (сеть Интернет / локальная сеть; авторизованный / свободный доступ)
Дополнительная литература	Данилов А. Н., Данилова С. А., Зорин А. А. Основы информационной безопасности : учебное пособие. Пермь : Изд-во ПГТУ, 2008.	https://elib.pstu.ru/Record/RUPNRPUelib2829	сеть Интернет; авторизованный доступ
Дополнительная литература	Никифоров С. Н. Методы защиты информации. Пароли, скрытие, шифрование : учебное пособие. 2-е изд., стер. Санкт-Петербург : Лань, 2019.	https://elib.pstu.ru/Record/lanRU-LAN-BOOK-114698	сеть Интернет; авторизованный доступ

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

Вид ПО	Наименование ПО
Операционные системы	MS Windows XP (подп. Azure Dev Tools for Teaching до 27.03.2022)
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
Прикладное программное обеспечение общего назначения	VMware Workstation Player (VMware Academic)
Прикладное программное обеспечение общего назначения	WinRAR (лиц№ 879261.1493674)
Прикладное программное обеспечение общего назначения	Wireshark

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

Наименование	Ссылка на информационный ресурс

Наименование	Ссылка на информационный ресурс
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/
База данных компании EBSCO	https://www.ebsco.com/

7. Материально-техническое обеспечение образовательного процесса по дисциплине

Вид занятий	Наименование необходимого основного оборудования и технических средств обучения	Количество единиц
Лекция	Мультимедийный проектор	1
Практическое занятие	Персональный копьютер	10

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 «Информатика в приложении к отрасли»
Приложение к рабочей программе дисциплины

Направление подготовки:	10.03.01 Информационная безопасность
Направленность (профиль) образовательной программы:	Информационная безопасность (общий профиль, СУОС)
Квалификация выпускника:	Бакалавр
Выпускающая кафедра:	Автоматика и телемеханика
Форма обучения:	Очная

Курс: 3 **Семестр**: 5

Трудоёмкость:
Кредитов по рабочему учебному плану: 3 ЗЕ
Часов по рабочему учебному плану: 108 ч.

Форма промежуточной аттестации:
Зачёт: 5 семестр

Пермь 2021

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 (5-го семестра учебного плана). Предусмотрены аудиторные лекционные и практические занятия. В рамках освоения учебного материала дисциплины формируются 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 зачета. 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**		**Зачёт**
Усвоенные знания						
З.1 знать классификацию современных компьютерных систем, типовые структуры, архитектуру и принципы организации компьютерных сетей; назначение, функции и обобщённую структуру операционных систем; назначение и основные компоненты систем баз данных; состав, назначение функциональных компонентов и программного обеспечения персонального компьютера; структуру и принципы работы современных и перспективных микропроцессоров.		ТО		КР		ТВ
Освоенные умения						
У.1 уметь применять типовые программные средства сервисного назначения и пользоваться сетевыми средствами для обмена данными, в том числе с использованием глобальной информационной сети интернет; составлять SQL запросы и осуществлять удалённый доступ к базам данных; определять состав компьютера: тип процессора и его параметры, тип модулей памяти и их характеристики, тип видеокарты, состав и параметры периферийных устройств.				КР		ПЗ
Приобретенные владения						
В.1 владеть навыками подготовки документов в среде типовых офисных пакетов; навыками применения				КР		

технических и программных средств тестирования с целью определения исправности компьютера и оценки его производительности.						

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 дифференцированного зачета.

Итоговой оценкой достижения результатов обучения по дисциплине является промежуточная аттестация в виде зачета, проводимая с учётом 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 контрольных работ (после проведения практических занятий).

2.2.1. Рубежная контрольная работа

Всего запланировано 5 рубежные контрольные работы (КР) после освоения студентами учебных модулей дисциплины и проведения практических занятий.

Типовые задания КР1:

1. Применить шифрование с симметричным и ассимитричным ключом.
2. Провести оценку их соединения.

Типовые задания КР2:

Создать безопасное соединения двух участков сети (VPN).

Типовые задания КР3:

Создать массив RAID0 и RAID1.

Типовые задания КР4:

Применить DLP систему к существующей сети.

Типовые задания КР5:

Разработать с помощью автоматизированных систем проектирования план видеонаблюдения территории.

Типовые шкала и критерии оценки результатов рубежной контрольной работы 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.

2.3.1. Процедура промежуточной аттестации без дополнительного аттестационного испытания

Промежуточная аттестация проводится в форме зачета. Зачет по дисциплине основывается на результатах выполнения предыдущих индивидуальных заданий студента по данной дисциплине.

Критерии выведения итоговой оценки за компоненты компетенций при проведении промежуточной аттестации в виде зачета приведены в общей части ФОС образовательной программы.

2.3.2. Процедура промежуточной аттестации с проведением аттестационного испытания

В отдельных случаях (например, в случае переаттестации дисциплины) промежуточная аттестация в виде зачета по дисциплине может проводиться с проведением аттестационного испытания по билетам. Билет содержит теоретические вопросы (ТВ) для проверки усвоенных знаний, практические задания (ПЗ) для проверки освоенных умений.

Билет формируется таким образом, чтобы в него попали вопросы и практические задания, контролирующие уровень сформированности ***всех*** заявленных компетенций.

2.3.2.1. Типовые вопросы и задания для зачета по дисциплине

Типовые вопросы для контроля усвоенных знаний:

1. Шифрование с симметричным и ассимитричным ключом, теория оценки их криптостойкости.
2. Создание безопасного соединения двух участков сети (VPN).
3. Создание RAID массивов.
4. DLP системы, контроль информационных потоков.
5. Автоматизированные системы проектирования систем видеонаблюдения.

Типовые вопросы и практические задания для контроля освоенных умений:

1. Настроить VPN соединение 2 компьютеров.
2. Настроить RAID массив.
3. Обнаружить инцидент информационной безопасности с помощью DLP системы.

2.3.2.2. Шкалы оценивания результатов обучения на зачете

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

Типовые шкала и критерии оценки результатов обучения при сдаче зачета 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 зачете считается, что *полученная оценка за компонент проверяемой в билете компетенции обобщается на соответствующий компонент всех компетенций, формируемых в рамках данной учебной дисциплины*.

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 зачета используются типовые критерии, приведенные в общей части ФОС образовательной программы.

Примеры вопросов для проверки знаний:

1. Программное обеспечение, управляющее компьютерами (включая микроконтроллеры) и позволяющее запускать на них прикладные программы? (операционная система)
2. Специализированная программа для обнаружения компьютерных вирусов, а также нежелательных (считающихся вредоносными) программ и восстановления заражённых (модифицированных) такими программами файлов? (антивирус)
3. Программное обеспечение, анализирующее входящий и исходящий трафик компьютера? (анализатор трафика, сниффер)
4. Технология виртуализации данных для объединения нескольких физических дисковых устройств в логический модуль для повышения отказоустойчивости и (или) производительности? (RAID)
5. Технологии предотвращения утечек конфиденциальной информации из информационной системы вовне? (DLP)
6. Текстовый файл в MS-DOS, OS/2 или Windows, содержащий последовательность команд, предназначенных для исполнения командным интерпретатором? (пакетный файл, BAT-файл)
7. Способ передачи или хранения информации с учётом сохранения в тайне самого факта такой передачи? (стеганография)
8. Определённым образом оформленный блок данных, передаваемый по сети? (сетевой пакет)
9. Сетевая модель, включающая в себя семь уровней: физический, канальный, сетевой, транспортный, сеансовый, представления, прикладной? (Модель OSI)
10. Открытый стандарт, используемый для расчета количественных оценок уязвимости в безопасности компьютерной системы, обычно с целью понять приоритет её исправления? (CVSS)