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: Технологии обеспечения информационной безопасности автономных сервисных роботов
(наименование)

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

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

Общая трудоёмкость: 144 (4)
(часы (ЗЕ))

Направление подготовки: 15.04.06 Мехатроника и робототехника
(код и наименование направления)

Направленность: Автономные сервисные роботы
(наименование образовательной программы)

Пермь 2023

1. Общие положения

1.1. Цели и задачи дисциплины

Цель - формирование комплекса знаний, умений и навыков в области применения методов защиты информации при проектировании и исследовании робототехнических систем.
Задачи:
- сформировать знания основных угрозы информации в информационных системах и сетях;
- сформировать умения и навыки проектирования комплексной защищенной инфраструктуры для автономных сервисных роботов.

1.2. Изучаемые объекты дисциплины

методы и средства защиты информации в автономных сервисных роботах; основные угрозы информации в современных автономных сервисных роботах; программные, программно-аппаратные и аппаратные средства защиты информации, применяемые при обеспечении комплексной информационной безопасности; программные средства анализа текущего уровня защищенности; современные технологии построения безопасных информационных систем и сетей.

1.3. Входные требования

Сетевые системы управления, системное программное обеспечение

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-1.1	ИД-1пк-1.1	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;	Знает основные положения аппарата и методологии нечеткой логики, нейронных сетей, навигации и защиты информации, применяемые в робототехнике.	Зачет
ПК-1.1	ИД-2пк-1.1	Умеет проектировать комплексную защищенную инфраструктуру для автономных сервисных роботов, отвечающую предъявляемым требованиям к уровню защищенности; разрабатывать модели информационно-технологических ресурсов, модели угроз и модели нарушителя информационной безопасности; применять современные программные средства криптографической защиты информации; применять современные аппаратные средства защиты информационных процессов в автономных сервисных роботах; применять	Умеет применять для проектирования и исследования робототехнических устройств и систем методы и средства нечеткой логики, нейронных сетей, навигации и защиты информации.	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
		современные аппаратные средства при аудите информационной безопасности автономных сервисных роботов.		
ПК-1.1	ИД-3пк-1.1	Владеет навыками разработки комплексной инфраструктуры защищенной информационной системы; навыками работы с программными и аппаратными комплексными средствами защиты информации в автономных сервисных роботах.	Владеет навыками практического применения алгоритмов нечеткой логики, навигации и защиты информации при разработке и реализации робототехнических устройств, систем и комплексов.	Защита лабораторной работы

3. Объем и виды учебной работы

Вид учебной работы	Всего часов	Распределение по семестрам в часах
		Номер семестра
		4
1. Проведение учебных занятий (включая проведение текущего контроля успеваемости) в форме: 1.1. Контактная аудиторная работа, из них:	54	54
- лекции (Л)	12	12
- лабораторные работы (ЛР)	12	12
- практические занятия, семинары и (или) другие виды занятий семинарского типа (ПЗ)	28	28
- контроль самостоятельной работы (КСР)	2	2
- контрольная работа		
1.2. Самостоятельная работа студентов (СРС)	90	90
2. Промежуточная аттестация		
Экзамен		
Дифференцированный зачет	9	9
Зачет		
Курсовой проект (КП)	36	36
Курсовая работа (КР)		
Общая трудоемкость дисциплины	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
4-й семестр				
Технологии защиты информации	4	4	10	30
Анализ угроз безопасности. Методы оценки рисков. Моделирование угроз безопасности. Архитектура защищенной информационной системы и криптографические методы обеспечения безопасности в каналах связи. Защита конечных узлов распределенной информационной системы				
Технологии обнаружения вторжений и аудита безопасности	6	4	10	30
Интеграция системы обнаружения вторжений Мониторинг распределенной инфраструктуры Аудит безопасности распределенной инфраструктуры				
Технологии управления инцидентами информационной безопасности	2	4	8	30
Основы расследования инцидентов. Планы аварийного восстановления. Сбор цифровых отпечатков. Системы управления инцидентами информационной безопасности				
ИТОГО по 4-му семестру	12	12	28	90
ИТОГО по дисциплине	12	12	28	90

Тематика примерных практических занятий

№ п.п.	Наименование темы практического (семинарского) занятия
1	Семинар "Нужно ли обучать навыкам атак на компьютерные системы?"
2	Разработка архитектуры защищенной информационной системы
3	Разработка комплексной системы информационной безопасности
4	Разработка модели тестирования автономного сервисного робота

Тематика примерных лабораторных работ

№ п.п.	Наименование темы лабораторной работы
1	Криптографическая защита каналов связи
2	Сегментирование и изоляция информационной системы

№ п.п.	Наименование темы лабораторной работы
3	Внедрение системы мониторинга инфраструктуры
4	Усиление периметра за счет интеграции СОВ

Тематика примерных курсовых проектов/работ

№ п.п.	Наименование темы курсовых проектов/работ
1	Разработка системы защиты АСР

5. Организационно-педагогические условия

5.1. Образовательные технологии, используемые для формирования компетенций

Материалы лекционных занятий по дисциплине представлены в виде видеолекций, в которых подача материала основывается на активном методе обучения, при которой 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. Материалы видеолекций дублируются в конспекте лекций доступном для самостоятельного изучения.
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; отработка у обучающихся навыков взаимодействия в составе коллектива; 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. Лабораторные работы выполняются в режиме онлайн с использованием виртуальных машин и онлайн-лаборатории на основе АСР Promobot.

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	Основы управления информационной безопасностью : учебное пособие для вузов / А. П. Курило [и др.]. - Москва: Горячая линия-Телеком, 2014.	15
2	Программно-аппаратные средства защиты информации : учебное пособие для вузов / Л. Х. Мифтахова [и др.]. - Санкт-Петербург: ИЦ Интермедия, 2018.	2
2. Дополнительная литература		
2.1. Учебные и научные издания		
1	Мельников Д. А. Информационная безопасность открытых систем : учебник / Д. А. Мельников. - Москва: Флинта, Наука, 2013.	11
2	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)
Методические указания для студентов по освоению дисциплины	Конспект лекций ТОИБ-АСР	online.at.pstu.ru	сеть Интернет; авторизованный доступ
Методические указания для студентов по освоению дисциплины	Практикум ТОИБ-АСР	online.at.pstu.ru	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	Windows 10 (подп. Azure Dev Tools for Teaching)
Офисные приложения.	Adobe Acrobat Reader DC. бесплатное ПО просмотра PDF
Прикладное программное обеспечение общего назначения	Dr.Web Enterprise Security Suite, 3000 лиц, ПНИПУ ОЦНИТ 2017
Прикладное программное обеспечение общего назначения	Oracle VM VirtualBox (GNU GPL 2)

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

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/
Виртуальный читальный зал Российской государственной библиотеки	https;//dvs.rsl.ru/
Информационные ресурсы Сети КонсультантПлюс	http://www.consultant.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	Виртуальное рабочее место обучающегося: ОС Windows, не менее 2 ядер CPU 3ГГц, не менее 4 ГБ оперативной памяти, не менее 80ГБ HDD	10
Лабораторная работа	Виртуальное рабочее место обучающегося: ОС Windows, не менее 2 ядер CPU 3ГГц, не менее 4 ГБ оперативной памяти, не менее 80ГБ HDD	10
Лабораторная работа	Лабораторный стенд «Promobot» с онлайн доступом	5
Лекция	Система LMS OpenEdX	1

Вид занятий	Наименование необходимого основного оборудования и технических средств обучения	Количество единиц
Лекция	Системы видео-конференц связи	1
Практическое занятие	Виртуальное рабочее место обучающегося: ОС Windows, не менее 2 ядер CPU 3ГГц, не менее 4 ГБ оперативной памяти, не менее 80ГБ HDD	10

8. Фонд оценочных средств дисциплины

Описан в отдельном файле

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 «Технологии обеспечения информационной безопасности автономных сервисных роботов»
Приложение к рабочей программе дисциплины

Направление подготовки: 15.04.06 Мехатроника и робототехника

Направленность (профиль) образовательной программы: Автономные сервисные роботы

Квалификация выпускника: Магистр

Выпускающая кафедра: Автоматика и телемеханика

Форма обучения: Очная

Курс: 2 **Семестр**: 4

Трудоёмкость:
Кредитов по рабочему учебному плану: 4 ЗЕ
Часов по рабочему учебному плану: 144 ч.

Форма промежуточной аттестации:
Зачёт с оценкой: 4 семестр
Курсовой проект: 4 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 (4-го семестра учебного плана) и разбито на 3 учебных модуля. В каждом модуле предусмотрены аудиторные лекционные, практические 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 (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 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;		ТО1 ТО2	ОЛР1 ОЛР2 ОЛР3 ОЛР4			КЗ
Освоенные умения						
У.1 Умеет проектировать комплексную защищенную инфраструктуру для автономных сервисных роботов, отвечающую предъявляемым требованиям к уровню защищенности; разрабатывать модели информационно□технологических ресурсов, модели угроз и модели нарушителя информационной безопасности; применять современные программные средства криптографической защиты информации; применять современные аппаратные средства защиты информационных процессов в автономных сервисных			ОЛР1 ОЛР2 ОЛР3 ОЛР4			КЗ

роботах; применять современные аппаратные средства при аудите информационной безопасности автономных сервисных роботов.						
Приобретенные владения						
В.1 Владеет навыками разработки комплексной инфраструктуры защищенной информационной системы; навыками работы с программными и аппаратными комплексными средствами защиты информации в автономных сервисных роботах			ОЛР1 ОЛР2 ОЛР3 ОЛР4			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 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 лабораторных работ и рубежных контрольных работ (после проведения практических занятий).

2.2.1. Защита лабораторных работ

Всего запланировано 4 лабораторные работы. 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.

2.3. Выполнение комплексного индивидуального задания на самостоятельную работу

Для оценивания навыков и опыта деятельности (владения), как результата обучения по дисциплине, не имеющей курсового проекта или работы, может быть использовано индивидуальное комплексное задание студенту.

Типовые шкала и критерии оценки результатов защиты индивидуального комплексного задания приведены в общей части ФОС образовательной программы.

2.4. 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.

2.4.1. 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.

2.4.2. 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 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.

2.4.2.1. Типовые вопросы и задания для зачета по дисциплине

Типовые вопросы для контроля усвоенных знаний:

1. Анализ угроз безопасности.
2. Методы оценки рисков.
3. Моделирование угроз безопасности.
4. Архитектура защищенной информационной системы и криптографические методы обеспечения безопасности в каналах связи.
5. Защита конечных узлов распределенной информационной системы
6. Интеграция системы обнаружения вторжений
7. Мониторинг распределенной инфраструктуры
8. Аудит безопасности распределенной инфраструктуры

Типовые вопросы и практические задания для контроля освоенных умений:

1. Криптографическая защита каналов связи
2. Сегментирование и изоляция информационной системы
3. Внедрение системы мониторинга инфраструктуры
4. Разработка системы защиты АСР

2.4.2.2. 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.