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

« 10 » октября 20 23 г.

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ

Дисциплина: Интеллектуальные средства обнаружения и блокировки
(наименование)

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

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

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

Направление подготовки: 09.04.01 Информатика и вычислительная техника
(код и наименование направления)

Направленность: Компьютерные системы и сети
(наименование образовательной программы)

Пермь 2023

1. Общие положения

1.1. Цели и задачи дисциплины

Знакомство студентов с современными средствами обнаружения и блокировки компьютерных атак. Разработка средств противодействия.

1.2. Изучаемые объекты дисциплины

Архитектура системы обнаружения атак.
Базы знаний, база методов и сигнатур.
Блоки построения дерева принятия решений.
Методы понижения вероятности ошибки.
Классификация и виды атак.
Способы выявления атак (сигнатурный, на основе аномалий, глубокий анализ траффика).
Ситуации нарушения доступности, конфиденциальности и целостности.
Обучение нейросети и наборы данных
Система обнаружения атак / обнаружения вторжений.

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
ПК-2.2	ИД-1ПК-2.2	Знает порядок работы и особенности компьютерных программ и баз данных, используемых для мониторинга функционирования инфокоммуникационных систем и сервисов	Знает порядок работы и особенности компьютерных программ и баз данных, используемых для мониторинга функционирования инфокоммуникационных систем и сервисов	Индивидуальное задание
ПК-2.2	ИД-2ПК-2.2	Умеет разрабатывать целевую архитектуру систем автоматизированного мониторинга и контроля функционирования инфокоммуникационных систем и сервисов и стратегию ее реализации	Умеет разрабатывать целевую архитектуру систем автоматизированного мониторинга и контроля функционирования инфокоммуникационных систем и сервисов и стратегию ее реализации	Индивидуальное задание

Компетенция	Индекс индикатора	Планируемые результаты обучения по дисциплине (знать, уметь, владеть)	Индикатор достижения компетенции, с которым соотнесены планируемые результаты обучения	Средства оценки
ПК-2.2	ИД-3ПК-2.2	Владеет навыками поиска информации по инновационным и конкурентным системам автоматизированного мониторинга и контроля функционирования инфокоммуникационных систем и сервисов	Владеет навыками поиска информации по инновационным и конкурентным системам автоматизированного мониторинга и контроля функционирования инфокоммуникационных систем и сервисов	Индивидуальное задание

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:	72	72
- лекции (Л)	18	18
- лабораторные работы (ЛР)	24	24
- практические занятия, семинары и (или) другие виды занятий семинарского типа (ПЗ)	26	26
- контроль самостоятельной работы (КСР)	4	4
- контрольная работа		
1.2. Самостоятельная работа студентов (СРС)	72	72
2. Промежуточная аттестация		
Экзамен		
Дифференцированный зачет	9	9
Зачет		
Курсовой проект (КП)		
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				
Системы обнаружения вторжений на основе нейросетей	3	4	4	12
Системы обнаружения вторжений на основе нейросетей Обзор и классификация СОВ. Исследование работы типовой СОВ				

Наименование разделов дисциплины с кратким содержанием	Объем аудиторных занятий по видам в часах			Объем внеаудиторных занятий по видам в часах
	Л	ЛР	ПЗ	СРС
Подготовка данных для использования в обучении и тестировании нейросетей при обнаружении сетевых атак	3	4	4	12
Способы захвата траффика. Способы противодействия захвату. Исследование ПО для захвата и классифицирования траффика.				
Особенности использования искусственных нейронных сетей в сфере информационной безопасности	3	4	4	12
Стадии атаки. Выявление признаков атаки. Подготовка обучающих данных. Эксперименты по обнаружению типовых атак.				
Использование схемы совпадений в системах обнаружения вторжений на основе нейронных сетей	3	4	4	12
Обучение и сравнение результатов различных классификаторов. Получение общего предсказания типа атаки. Оценка эффективности в сравнении с другими методами.				
Возможные варианты построения интеллектуальной системы обнаружения несанкционированной работы программного обеспечения	3	4	6	12
Сигнатурный метод анализа Контроль работы программ по профилям Использование прогнозируемых шаблонов Метод обнаружения опасных комбинаций безопасных событий Анализ переходов системы из состояния в состояние Контроль превышения пороговой величины частоты событий Статистический анализ последовательности системных вызовов Продукционные и экспертные системы				
Анализ зашифрованного сетевого трафика на основе вычисления энтропии и применения нейросетевых классификаторов	3	4	4	12
Методы получения признаков траффика Вычисление энтропии сигнала Нейросетевые методы классификации траффика Оценка пригодности метода				
ИТОГО по 4-му семестру	18	24	26	72
ИТОГО по дисциплине	18	24	26	72

Тематика примерных практических занятий

№ п.п.	Наименование темы практического (семинарского) занятия
1	Обучение и сравнение результатов различных классификаторов.
2	Разработка продукционной системы классификации траффика
3	Разработка нейросетевой системы классификации траффика

Тематика примерных лабораторных работ

№ п.п.	Наименование темы лабораторной работы
1	Исследование работы типовой СОВ
2	Исследование ПО для захвата и классифицирования траффика.
3	Выявление признаков атаки с помощью tcpdump, nmap и snort

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	Кирх О. Linux: Руководство администратора сети. Санкт-Петербург : Питер, 2000. 362 с	1
2	Ручкин В. Н., Костров Б. В., Свирина А. Г. Системы искусственного интеллекта. Нейросети и нейрокомпьютеры : учебник для вузов. Москва : КУРС, 2021. 283 с. 18,0 усл. печ. л.	2
3	Сидоркина И. Г. Системы искусственного интеллекта : учебное пособие для вузов. Москва : КНОРУС, 2011. 245 с. 15,5 усл. печ. л.	2
2. Дополнительная литература		
2.1. Учебные и научные издания		
1	Нусс С. В. Идентификация технического состояния технологического оборудования на основе нейросетевой модели : автореф. дис. .. канд. техн. наук 05.13.06. Пермь : Изд-во ПГТУ, 2009. 17 с.	1
2	Рейчард К., Фостер-Джонсон Э. Unix. Санкт-Петербург : Питер, 1999. 374 с.	1
3	Системы искусственного интеллекта : практический курс учебное пособие для вузов / Чулюков В.А., Астахова И.Ф., Потапов А.С., Каширина И.Л. Москва : БИНОМ. Лаб. знаний : Физматлит, 2008. 292 с.	4
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	Анализ зашифрованного сетевого трафика на основе вычисления энтропии и применения нейросетевых классификаторов // cyberleninka.ru URL: https://cyberleninka.ru/article/n/analiz-zashifrovannogo-setevogo-trafika-na-osnove-vychisleniya-entropii-i-primeneniya-	https://cyberleninka.ru/article/n/analiz-zashifrovannogo-setevogo-trafika-na-osnove-vychisleniya-entropii-i-primeneniya-neyrosetevyh-klassifikatorov	сеть Интернет; свободный доступ
Дополнительная литература	Подготовка данных для использования в обучении и тестировании нейросетей при обнаружении сетевых атак // cyberleninka.ru URL: https://cyberleninka.ru/article/n/podgotovka-dannyh-dlya-ispolzovaniya-v-obuchenii-i-testirovanii-neyrosetey-pri-obnaruzhenii-set	https://cyberleninka.ru/article/n/podgotovka-dannyh-dlya-ispolzovaniya-v-obuchenii-i-testirovanii-neyrosetey-pri-obnaruzhenii-setevyh-atak	сеть Интернет; свободный доступ
Дополнительная литература	Подготовка данных для использования в обучении и тестировании нейросетей при обнаружении сетевых атак // cyberleninka.ru URL: https://cyberleninka.ru/article/n/podgotovka-dannyh-dlya-ispolzovaniya-v-obuchenii-i-testirovanii-neyrosetey-pri-obnaruzhenii-set	https://cyberleninka.ru/article/n/podgotovka-dannyh-dlya-ispolzovaniya-v-obuchenii-i-testirovanii-neyrosetey-pri-obnaruzhenii-setevyh-atak	сеть Интернет; свободный доступ
Дополнительная литература	Системы обнаружения вторжений на основе нейросетей // cyberleninka.ru URL: https://cyberleninka.ru/article/n/sistemy-obnaruzheniya-vtorzheniy-na-osnove-neyrosetey (дата обращения: 09.09.2021)	https://cyberleninka.ru/article/n/sistemy-obnaruzheniya-vtorzheniy-na-osnove-neyrosetey	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)

Вид ПО	Наименование ПО
Среды разработки, тестирования и отладки	NetBeans (SUN PUBLIC LICENSE)
Среды разработки, тестирования и отладки	PIP (The Python Package Installer) Free

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/
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/

7. Материально-техническое обеспечение образовательного процесса по дисциплине

Вид занятий	Наименование необходимого основного оборудования и технических средств обучения	Количество единиц
Лабораторная работа	Дисплейный класс, 15 раб. мест.	1
Лекция	Ноутбук, проектор, экран	1
Практическое занятие	Ноутбук, 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 «Интеллектуальные средства обнаружения и блокировки» ***Приложение к рабочей программе дисциплины***

Направление подготовки:	**Информатика и вычислительная техника (09.04.01)**
Направленность (профиль) образовательной программы:	**Компьютерные системы и сети**
Квалификация выпускника:	**магистратура**
Выпускающая кафедра:	Информационных технологий и автоматизированных систем
Форма обучения:	очная

Курс: 2 **Семестр**: 3

Трудоёмкость:

Кредитов по рабочему учебному плану: 4
Часов по рабочему учебному плану:140

Форма промежуточной аттестации:

зачет

Пермь 2022 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 (3-го семестра учебного плана) и разбито на 4 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 (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. 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**
	ТО	**ОЛР**	**Зачет**
Усвоенные знания			
З.1 Знает порядок работы и особенности компьютерных программ и баз данных, используемых для мониторинга функционирования инфокоммуникационных систем и сервисов	ТО1	ОЛР1-ОЛР7	по результатам текущего и рубежного контроля
Освоенные умения			
У.1 Умеет разрабатывать целевую архитектуру систем автоматизированного мониторинга и контроля функционирования инфокоммуникационных систем и сервисов и стратегию ее реализации		ОЛР1- ОЛР7	по результатам текущего и рубежного контроля
Приобретенные владения			
В.1 Владеет навыками поиска информации по инновационным и конкурентным системам автоматизированного мониторинга и контроля		ОЛР8	по результатам текущего и рубежного контроля

функционирования инфокоммуникационных систем и сервисов			

ТО – коллоквиум (теоретический опрос); ОЛР – отчет по лабораторной работе.

Итоговой оценкой достижения результатов обучения по дисциплине является промежуточная аттестация в виде зачета, 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;

- 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 8 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 зачета по результатам текущего и рубежного контроля.

3. . 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.

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

4. Критерии оценивания уровня сформированности компонентов и компетенций

4.1. 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.

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