

ФЕДЕРАЛЬНОЕ АГЕНТСТВО ЖЕЛЕЗНОДОРОЖНОГО ТРАНСПОРТА
Федеральное государственное бюджетное образовательное учреждение
высшего образования «Петербургский государственный университет путей сообщения
Императора Александра I»
(ФГБОУ ВО ПГУПС)

Кафедра «Информатика и информационная безопасность»

РАБОЧАЯ ПРОГРАММА

дисциплины

*Б1.О.40 «МАШИННОЕ ОБУЧЕНИЕ И НЕЙРОСЕТЕВОЕ УПРАВЛЕНИЕ
ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТЬЮ»*

для специальности

10.05.03 «Информационная безопасность автоматизированных систем»

по специализации

«Безопасность автоматизированных систем на железнодорожном транспорте»

Форма обучения – очная

Санкт-Петербург
2025

ЛИСТ СОГЛАСОВАНИЙ

Рабочая программа рассмотрена и утверждена на заседании кафедры «Информатика и информационная безопасность»
Протокол № 10 от 31 марта 2025 г.

И.о. заведующего кафедрой
«Информатика и информационная безопасность»
31 марта 2025 г.

К.З. Билятдинов

СОГЛАСОВАНО

Руководитель ОПОП
31 марта 2025 г.

М.Л. Глухарев

1. Цели и задачи дисциплины

Рабочая программа дисциплины «*Машинное обучение и нейросетевое управление информационной безопасностью*» (Б1.О.40) (далее – дисциплина) составлена в соответствии с требованиями федерального государственного образовательного стандарта высшего образования по специальности 10.05.03 «*Информационная безопасность автоматизированных систем*» (далее – ФГОС ВО), утвержденного 26 ноября 2020 г., приказ Министерства науки и высшего образования Российской Федерации № 1457, с учетом профессионального стандарта 06.033 «*Специалист по защите информации в автоматизированных системах*», утвержденного приказом Министерства труда и социальной защиты Российской Федерации от 15 сентября 2016 г. № 522н.

Целью изучения дисциплины является ознакомление обучающихся с основами функционирования нейронных сетей и их применения для реализации практических разработок в области защиты информации в автоматизированных системах

Для достижения цели дисциплины решаются следующие задачи:

- Формирование знаний о принципах устройства нейронных сетей, классах задач, решаемых нейронными сетями, алгоритмах машинного обучения.
- Формирование умений применять нейронные сети для решения задач обеспечения информационной безопасности, разрабатывать и обучать нейронные сети, применять их для решения задач обеспечения информационной безопасности.

2. Перечень планируемых результатов обучения по дисциплине, соотнесенных с установленными в образовательной программе индикаторами достижения компетенций

Планируемыми результатами обучения по дисциплине является формирование у обучающихся компетенций и/или части компетенций. Сформированность компетенций и/или части компетенций оценивается с помощью индикаторов достижения компетенций.

Индикаторы достижения компетенций	Результаты обучения по дисциплине (модулю)
ОПК-8. Способен применять методы научных исследований при проведении разработок в области защиты информации в автоматизированных системах	
ОПК-8.1.1. Знает основные перспективы развития науки и техники в области профессиональной деятельности, в том числе системы поддержки принятия решений, системы искусственного интеллекта	Обучающийся знает: <ul style="list-style-type: none">– Принципы устройства и обучения нейронных сетей;– Классы задач, решаемых нейронными сетями;– Алгоритмы обучения нейронных сетей с учителем и без учителя;– Способы применения нейронных сетей для решения задач обеспечения информационной безопасности
ОПК-8.2.1. Умеет применять методы и системы искусственного интеллекта при реализации практических разработок в области защиты информации в автоматизированных системах	Обучающийся умеет: <ul style="list-style-type: none">– Проектировать и создавать нейронные сети;– Обучать нейронные сети;– Применять нейронные сети для решения задач обеспечения информационной безопасности.

3. Место дисциплины в структуре основной профессиональной образовательной программы

Дисциплина относится к обязательной части блока 1 «Дисциплины (модули)».

4. Объем дисциплины и виды учебной работы

Вид учебной работы	Всего часов
Контактная работа (по видам учебных занятий) В том числе:	
– лекции (Л)	32
– практические занятия (ПЗ)	–
– лабораторные работы (ЛР)	32
Самостоятельная работа (СРС) (всего)	40
Контроль	4
Форма контроля (промежуточной аттестации)	3
Общая трудоемкость: час / з.е.	108 / 3

Примечание: «Форма контроля» – экзамен (Э), зачет (З), зачет с оценкой (З*), курсовой проект (КП), курсовая работа (КР)

5. Структура и содержание дисциплины

5.1. Разделы дисциплины и содержание рассматриваемых вопросов

№ п/п	Наименование раздела дисциплины	Содержание раздела	Индикаторы достижения компетенций
1	Основы нейронных сетей	<p>Лекция 1. Задачи распознавания и классификации.</p> <p>Лекция 2. Устройство нейронной сети. Модель нейрона. Персептрон</p> <p>Лекция 3. Топологии нейронных сетей.</p> <p>Лекция 4. Алгоритм работы нейронной сети</p> <p>Лекция 5. Проектирование нейронных сетей</p> <p>Лабораторная работа 1. Проектирование однослойной НС (4 часа)</p> <p>Лабораторная работа 2. Реализация однослойной НС средствами Excel (4 часа)</p> <p>Самостоятельная работа:</p> <ul style="list-style-type: none"> – Изучение пособий [1], [4], [5] из п. 8.5. – Подготовка к выполнению лабораторных работ. 	ОПК-8.1.1
2	Обучение нейронных сетей	<p>Лекция 6. Обучение нейронных сетей. Тестовые и обучающие выборки. Обучение с учителем и без учителя (6 часов).</p> <p>Лекция 7. Автоматизация обучения нейронных сетей и инструменты для создания НС (4 часа).</p> <p>Лабораторная работа 3. Обучение однослойной НС (4 часа)</p> <p>Лабораторная работа 4. Реализация и обучение НС средствами Matlab (8 часов)</p> <p>Самостоятельная работа:</p> <ul style="list-style-type: none"> – Изучение пособий [2–5] из п. 8.5. 	ОПК-8.1.1 ОПК-8.2.1

№ п/п	Наименование раздела дисциплины	Содержание раздела	Индикаторы достижения компетенций
		– Подготовка к выполнению лабораторных работ.	
3	Применение нейронных сетей в информационной безопасности	<p>Лекция 8. Типы задач обеспечения информационной безопасности</p> <p>Лекция 9. Применение нейронных сетей для решения задач идентификации угроз ИБ (4 часа)</p> <p>Лекция 10. Источники данных для обучения нейронных сетей, используемых для идентификации угроз ИБ</p> <p>Лекция 11. Глубинное обучение нейронных сетей, используемых для идентификации угроз ИБ</p> <p>Лабораторная работа 5. Разработка нейронной сети для идентификации инцидента информационной безопасности (12 часов)</p> <p>Самостоятельная работа:</p> <ul style="list-style-type: none"> – Подготовка к выполнению лабораторной работы. – Подготовка к сдаче зачета. 	ОПК-8.1.1 ОПК-8.2.1

5.2. Разделы дисциплины и виды занятий

№ п/п	Наименование раздела дисциплины	Л	ПЗ	ЛР	СРС	Всего
1	Основы нейронных сетей	10	0	8	10	28
2	Обучение нейронных сетей	12	0	12	15	39
3	Применение нейронных сетей в информационной безопасности	10	0	12	15	37
	Итого	32	0	32	40	104
Контроль						4
Всего (общая трудоемкость, час.)						108

6. Оценочные материалы для проведения текущего контроля успеваемости и промежуточной аттестации обучающихся по дисциплине

Оценочные материалы по дисциплине является неотъемлемой частью рабочей программы и представлены отдельным документом, рассмотренным на заседании кафедры и утвержденным заведующим кафедрой.

7. Методические указания для обучающихся по освоению дисциплины

Порядок изучения дисциплины следующий:

1. Освоение разделов дисциплины производится в порядке, приведенном в разделе 5 «Содержание и структура дисциплины». Обучающийся должен освоить все разделы дисциплины, используя методические материалы дисциплины, а также учебно-методическое обеспечение, приведенное в разделе 8 рабочей программы.

2. Для формирования компетенций обучающийся должен представить выполненные задания, необходимые для оценки знаний, умений, навыков и (или) опыта деятельности, предусмотренные текущим контролем успеваемости (см. оценочные материалы по дисциплине).

3. По итогам текущего контроля успеваемости по дисциплине, обучающийся должен пройти промежуточную аттестацию (см. оценочные материалы по дисциплине).

8. Описание материально-технического и учебно-методического обеспечения, необходимого для реализации образовательной программы по дисциплине

8.1. Помещения представляют собой учебные аудитории для проведения учебных занятий, предусмотренных программой специалитета, укомплектованные специализированной учебной мебелью и оснащенные оборудованием и техническими средствами обучения, служащими для представления учебной информации большой аудитории: настенным экраном (стационарным или переносным), маркерной доской и (или) меловой доской, мультимедийным проектором (стационарным или переносным).

Все помещения, используемые для проведения учебных занятий и самостоятельной работы, соответствуют действующим санитарным и противопожарным нормам и правилам.

Помещения для самостоятельной работы обучающихся оснащены компьютерной техникой с возможностью подключения к сети «Интернет» и обеспечением доступа в электронную информационно-образовательную среду университета.

8.2. Университет обеспечен необходимым комплектом лицензионного и свободно распространяемого программного обеспечения, в том числе отечественного производства:

- MS Office;
- Операционная система Windows;
- Антивирус Касперский;
- Matlab 6.
- Eclipse IDE (Python) (свободно распространяемое ПО)

8.3. Обучающимся обеспечен доступ (удаленный доступ) к современным профессиональным базам данных:

– Электронно-библиотечная система издательства «Лань». [Электронный ресурс]. – URL: <https://e.lanbook.com/> — Режим доступа: для авториз. пользователей;

– Электронно-библиотечная система ibooks.ru («Айбукс»). – URL: <https://ibooks.ru/> — Режим доступа: для авториз. пользователей;

– Электронная библиотека ЮРАЙТ. – URL: <https://biblio-online.ru/> — Режим доступа: для авториз. пользователей;

– Единое окно доступа к образовательным ресурсам - каталог образовательных интернет-ресурсов и полнотекстовой электронной учебно-методической библиотеке для общего и профессионального образования». – URL: <http://window.edu.ru/> — Режим доступа: свободный.

– Словари и энциклопедии. – URL: <http://academic.ru/> — Режим доступа: свободный.

– Научная электронная библиотека "КиберЛенинка" - это научная электронная библиотека, построенная на парадигме открытой науки (Open Science), основными задачами которой является популяризация науки и научной деятельности, общественный контроль качества научных публикаций, развитие междисциплинарных исследований, современного института научной рецензии и повышение цитируемости российской науки. – URL: <http://cyberleninka.ru/> — Режим доступа: свободный.

8.4. Обучающимся обеспечен доступ (удаленный доступ) к информационным справочным системам:

– Национальный Открытый Университет "ИНТУИТ". Бесплатное образование. [Электронный ресурс]. – URL: <https://intuit.ru/> — Режим доступа: свободный.

8.5. Перечень печатных и электронных изданий, используемых в образовательном процессе:

1. Бураков, Д. П. Логические основы интеллектуальных систем : учебное пособие, Ч. 2 – СПб : ФГБОУ ВО ПГУПС. – 2020. – 76 с.

2. Нейронные сети в Matlab : учебное пособие / перевод с английского А. А. Маслов. — Санкт-Петербург : БГТУ "Военмех" им. Д.Ф. Устинова, 2017. — 165 с. — ISBN 978-5-906920-72-0. — Текст : электронный // Лань : электронно-библиотечная система. —

URL: <https://e.lanbook.com/book/121856> (дата обращения: 16.05.2021). — Режим доступа: для авториз. пользователей.

3. Соробин, А. Б. Сверточные нейронные сети: примеры реализаций : учебно-методическое пособие / А. Б. Соробин. — Москва : РТУ МИРЭА, 2020. — 159 с. — Текст : электронный // Лань : электронно-библиотечная система. — URL: <https://e.lanbook.com/book/163853> (дата обращения: 16.05.2021). — Режим доступа: для авториз. пользователей.

4. Цуриков, А. Н. Моделирование и обучение искусственных нейронных сетей : учебное пособие / А. Н. Цуриков. — Ростов-на-Дону : РГУПС, 2019. — 112 с. — ISBN 978-5-88814-867-9. — Текст : электронный // Лань : электронно-библиотечная система. — URL: <https://e.lanbook.com/book/140610> (дата обращения: 16.05.2021). — Режим доступа: для авториз. пользователей.

5. Кузнецов, В. П. Нейронные сети: практический курс : учебное пособие / В. П. Кузнецов. — Рязань : РГРТУ, 2014. — 72 с. — Текст : электронный // Лань : электронно-библиотечная система. — URL: <https://e.lanbook.com/book/168060> (дата обращения: 16.05.2021). — Режим доступа: для авториз. пользователей.

8.6. Перечень ресурсов информационно-телекоммуникационной сети «Интернет», используемых в образовательном процессе:

– Личный кабинет обучающегося и электронная информационно-образовательная среда. [Электронный ресурс]. – URL: <https://my.pgups.ru> — Режим доступа: для авториз. пользователей;

– Электронная информационно-образовательная среда. [Электронный ресурс]. – URL: <https://sdo.pgups.ru> — Режим доступа: для авториз. пользователей.

Разработчик рабочей программы, доцент
14.03.2025 г.

Т.С. Карпова