

МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ РОССИЙСКОЙ ФЕДЕРАЦИИ  
Федеральное государственное автономное образовательное учреждение высшего образования  
"Казанский (Приволжский) федеральный университет"  
Институт вычислительной математики и информационных технологий



подписано электронно-цифровой подписью

## Программа дисциплины

### Машинное обучение

Направление подготовки: 10.04.01 - Информационная безопасность

Профиль подготовки: Математические методы и программные технологии защиты информации

Квалификация выпускника: магистр

Форма обучения: очное

Язык обучения: русский

Год начала обучения по образовательной программе: 2017

## **Содержание**

1. Перечень планируемых результатов обучения по дисциплине (модулю), соотнесенных с планируемыми результатами освоения ОПОП ВО
2. Место дисциплины (модуля) в структуре ОПОП ВО
3. Объем дисциплины (модуля) в зачетных единицах с указанием количества часов, выделенных на контактную работу обучающихся с преподавателем (по видам учебных занятий) и на самостоятельную работу обучающихся
4. Содержание дисциплины (модуля), структурированное по темам (разделам) с указанием отведенного на них количества академических часов и видов учебных занятий
  - 4.1. Структура и тематический план контактной и самостоятельной работы по дисциплине (модулю)
  - 4.2. Содержание дисциплины (модуля)
5. Перечень учебно-методического обеспечения для самостоятельной работы обучающихся по дисциплине (модулю)
6. Фонд оценочных средств по дисциплине (модулю)
7. Перечень литературы, необходимой для освоения дисциплины (модуля)
8. Перечень ресурсов информационно-телекоммуникационной сети "Интернет", необходимых для освоения дисциплины (модуля)
9. Методические указания для обучающихся по освоению дисциплины (модуля)
10. Перечень информационных технологий, используемых при осуществлении образовательного процесса по дисциплине (модулю), включая перечень программного обеспечения и информационных справочных систем (при необходимости)
11. Описание материально-технической базы, необходимой для осуществления образовательного процесса по дисциплине (модулю)
12. Средства адаптации преподавания дисциплины (модуля) к потребностям обучающихся инвалидов и лиц с ограниченными возможностями здоровья
13. Приложение №1. Фонд оценочных средств
14. Приложение №2. Перечень литературы, необходимой для освоения дисциплины (модуля)
15. Приложение №3. Перечень информационных технологий, используемых для освоения дисциплины (модуля), включая перечень программного обеспечения и информационных справочных систем

Программу дисциплины разработал(а)(и) заведующий кафедрой, к.н. (доцент) Вахитов Г.З. (кафедра технологий программирования, отделение фундаментальной информатики и информационных технологий), GZVahitov@kpfu.ru ; доцент, к.н. Еникеева З.А. (кафедра технологий программирования, отделение фундаментальной информатики и информационных технологий), ZAEニーkeeva@kpfu.ru

### **1. Перечень планируемых результатов обучения по дисциплине (модулю), соотнесенных с планируемыми результатами освоения ОПОП ВО**

Обучающийся, освоивший дисциплину (модуль), должен обладать следующими компетенциями:

Шифр компетенции	Расшифровка приобретаемой компетенции
ОК-1	способность к абстрактному мышлению, анализу, синтезу
ОК-2	способность самостоятельно приобретать с помощью информационных технологий и использовать в практической деятельности новые знания и умения
ПК-10	способность проводить аттестацию объектов информатизации по требованиям безопасности информации
ПК-11	способность проводить занятия по избранным дисциплинам предметной области данного направления и разрабатывать методические материалы, используемые в образовательной деятельности
ПК-14	способность организовать работу по созданию или модернизации систем, средств и технологий обеспечения информационной безопасности в соответствии с правовыми нормативными актами и нормативными методическими документами ФСБ России, ФСТЭК России
ПК-2	способность разрабатывать системы, комплексы, средства и технологии обеспечения информационной безопасности
ПК-3	способность проводить обоснование состава, характеристик и функциональных возможностей систем и средств обеспечения информационной безопасности объектов защиты на основе российских и международных стандартов
ПК-4	способность разрабатывать программы и методики испытаний средств и систем обеспечения информационной безопасности
ПК-6	способность осуществлять сбор, обработку, анализ и систематизацию научно-технической информации по теме исследования, выбор методов и средств решения задачи, разрабатывать планы и программы проведения научных исследований и технических разработок
ПК-8	способность обрабатывать результаты экспериментальных исследований, оформлять научно-технические отчеты, обзоры, готовить по результатам выполненных исследований научные доклады и статьи

Обучающийся, освоивший дисциплину (модуль):

Должен знать:

1. Математические основы машинного обучения: методы построения моделей множественной регрессия, задачи оптимизации.
2. Методологию построения нейронных сетей.
3. Метод группового учёта аргументов.

Должен уметь:

1. Программировать искусственные нейронные сети.
2. Программировать алгоритмы метода группового учёта аргументов.
3. Использовать стандартные библиотеки, применяемые в машинном обучении.

Должен владеть:

1. Приёмами оптимизации работы искусственной нейронной сети.

2. Приёмами отбора моделей в методе группового учёта аргументов.

Должен демонстрировать способность и готовность:

1. В применении машинного обучения в практически ценных задачах.

2. К модификации ныне существующих приёмов машинного обучения с целью улучшения практических результатов.

## **2. Место дисциплины (модуля) в структуре ОПОП ВО**

Данная дисциплина (модуль) включена в раздел "Б1.В.ДВ.4 Дисциплины (модули)" основной профессиональной образовательной программы 10.04.01 "Информационная безопасность (Математические методы и программные технологии защиты информации)" и относится к дисциплинам по выбору.

Осваивается на 1 курсе в 2 семестре.

## **3. Объем дисциплины (модуля) в зачетных единицах с указанием количества часов, выделенных на контактную работу обучающихся с преподавателем (по видам учебных занятий) и на самостоятельную работу обучающихся**

Общая трудоемкость дисциплины составляет 2 зачетных(ые) единиц(ы) на 72 часа(ов).

Контактная работа - 18 часа(ов), в том числе лекции - 0 часа(ов), практические занятия - 0 часа(ов), лабораторные работы - 18 часа(ов), контроль самостоятельной работы - 0 часа(ов).

Самостоятельная работа - 54 часа(ов).

Контроль (зачёт / экзамен) - 0 часа(ов).

Форма промежуточного контроля дисциплины: зачет во 2 семестре.

## **4. Содержание дисциплины (модуля), структурированное по темам (разделам) с указанием отведенного на них количества академических часов и видов учебных занятий**

### **4.1 Структура и тематический план контактной и самостоятельной работы по дисциплине (модулю)**

N	Разделы дисциплины / модуля	Семестр	Виды и часы контактной работы, их трудоемкость (в часах)			Самостоятельная работа
			Лекции	Практические занятия	Лабораторные работы	
1.	Тема 1. Общие понятия искусственных нейронных сетей.	2	0	0	2	6
2.	Тема 2. Алгоритм обратного распространения ошибки(backpropagation).	2	0	0	2	6
3.	Тема 3. Модели нейронных сетей для реализации отображений.	2	0	0	2	6
4.	Тема 4. Нейронные байесовские сети.	2	0	0	2	6
5.	Тема 5. Линейные модели классификации и регрессии.	2	0	0	2	6
6.	Тема 6. Введение в метод группового учёта аргументов (МГУА).	2	0	0	2	6
7.	Тема 7. О некоторых критериях селекции моделей в МГУА.	2	0	0	2	6
8.	Тема 8. Комбинаторный алгоритм МГУА (COMBI).	2	0	0	2	6
9.	Тема 9. Поиск объекта на изображении. Метод Виолы-Джонса	2	0	0	2	6
	Итого		0	0	18	54

### **4.2 Содержание дисциплины (модуля)**

#### **Тема 1. Общие понятия искусственных нейронных сетей.**

Историческая справка.

Аналогии с биологическим нейроном.

Однослойный персепtron.

Двухслойный персепtron.

Функции активации.

**Тема 2. Алгоритм обратного распространения ошибки(backpropagation).**

Функционирование сети.

Обучение сети.

Гетероассоциативная память.

Прогнозирование.

Автоассоциативная память.

Кластеризация

Число нейронов в скрытых слоях

Масштабирование данных

**Тема 3. Модели нейронных сетей для реализации отображений.**

Общая постановка задачи.

Теорема Колмогорова-Арнольда.

Работа Хект-Нильсена.

Следствия из теоремы Колмогорова-Арнольда-Хект-Нильсена. Использование других моделей нейронных сетей для представления отображений.

**Тема 4. Нейронные байесовские сети.**

Обучения байесовскими методами.

Байесовские методы обучения нейронных сетей.

Последовательное обучение нейронных сетей.

Выборка по значимости.

Приложение к распознаванию речи.

**Тема 5. Линейные модели классификации и регрессии.**

Метод наименьших квадратов.

Ковариационная матрица случайных отклонений.

Обобщённый метод наименьших квадратов.

**Тема 6. Введение в метод группового учёта аргументов (МГУА).**

Историческая справка.

Основные этапы реализации метода.

Использование полиномов Колмогорова-Габора

**Тема 7. О некоторых критериях селекции моделей в МГУА.**

Коэффициент детерминации.

Проверка модели на наличие автокорреляции.

Проверка модели на наличие гетероскедастичности.

Проверка модели на наличие мультиколлинеарности.

**Тема 8. Комбинаторный алгоритм МГУА (COMBI).**

Выборка данных.

Ряды усложнения частных описаний.

Формы частных описаний.

Выбор оптимальных моделей.

Дополнительное определение модели по дискриминационному критерию.

**Тема 9. Поиск объекта на изображении. Метод Виолы-Джонса**

Интегральное представление изображения.

Признаки Хаара.

Бустинг.

Обучение классификатора

Каскадная модель.

**5. Перечень учебно-методического обеспечения для самостоятельной работы обучающихся по дисциплине (модулю)**

Самостоятельная работа обучающихся выполняется по заданию и при методическом руководстве преподавателя, но без его непосредственного участия. Самостоятельная работа подразделяется на самостоятельную работу на аудиторных занятиях и на внеаудиторную самостоятельную работу. Самостоятельная работа обучающихся включает как полностью самостоятельное освоение отдельных тем (разделов) дисциплины, так и проработку тем (разделов), осваиваемых во время аудиторной работы. Во время самостоятельной работы обучающиеся читают и конспектируют учебную, научную и справочную литературу, выполняют задания, направленные на закрепление знаний и отработку умений и навыков, готовятся к текущему и промежуточному контролю по дисциплине.

Организация самостоятельной работы обучающихся регламентируется нормативными документами, учебно-методической литературой и электронными образовательными ресурсами, включая:

Порядок организации и осуществления образовательной деятельности по образовательным программам высшего образования - программам бакалавриата, программам специалитета, программам магистратуры (утвержден приказом Министерства образования и науки Российской Федерации от 5 апреля 2017 года №301)

Письмо Министерства образования Российской Федерации №14-55-996ин/15 от 27 ноября 2002 г. "Об активизации самостоятельной работы студентов высших учебных заведений"

Устав федерального государственного автономного образовательного учреждения "Казанский (Приволжский) федеральный университет"

Правила внутреннего распорядка федерального государственного автономного образовательного учреждения высшего профессионального образования "Казанский (Приволжский) федеральный университет"

Локальные нормативные акты Казанского (Приволжского) федерального университета

## **6. Фонд оценочных средств по дисциплине (модулю)**

Фонд оценочных средств по дисциплине (модулю) включает оценочные материалы, направленные на проверку освоения компетенций, в том числе знаний, умений и навыков. Фонд оценочных средств включает оценочные средства текущего контроля и оценочные средства промежуточной аттестации.

В фонде оценочных средств содержится следующая информация:

- соответствие компетенций планируемым результатам обучения по дисциплине (модулю);
- критерии оценивания сформированности компетенций;
- механизм формирования оценки по дисциплине (модулю);
- описание порядка применения и процедуры оценивания для каждого оценочного средства;
- критерии оценивания для каждого оценочного средства;
- содержание оценочных средств, включая требования, предъявляемые к действиям обучающихся, демонстрируемым результатам, задания различных типов.

Фонд оценочных средств по дисциплине находится в Приложении 1 к программе дисциплины (модулю).

## **7. Перечень литературы, необходимой для освоения дисциплины (модуля)**

Освоение дисциплины (модуля) предполагает изучение основной и дополнительной учебной литературы. Литература может быть доступна обучающимся в одном из двух вариантов (либо в обоих из них):

- в электронном виде - через электронные библиотечные системы на основании заключенных КФУ договоров с правообладателями;
- в печатном виде - в Научной библиотеке им. Н.И. Лобачевского. Обучающиеся получают учебную литературу на абонементе по читательским билетам в соответствии с правилами пользования Научной библиотекой.

Электронные издания доступны дистанционно из любой точки при введении обучающимся своего логина и пароля от личного кабинета в системе "Электронный университет". При использовании печатных изданий библиотечный фонд должен быть укомплектован ими из расчета не менее 0,5 экземпляра (для обучающихся по ФГОС З++ - не менее 0,25 экземпляра) каждого из изданий основной литературы и не менее 0,25 экземпляра дополнительной литературы на каждого обучающегося из числа лиц, одновременно осваивающих данную дисциплину.

Перечень основной и дополнительной учебной литературы, необходимой для освоения дисциплины (модуля), находится в Приложении 2 к рабочей программе дисциплины. Он подлежит обновлению при изменении условий договоров КФУ с правообладателями электронных изданий и при изменении комплектования фондов Научной библиотеки КФУ.

## **8. Перечень ресурсов информационно-телекоммуникационной сети "Интернет", необходимых для освоения дисциплины (модуля)**

Coursera - <https://coursera.org>

Stepik - <https://welcome.stepik.org>

Открытое образование - <https://openu.edu.ru>

## **9. Методические указания для обучающихся по освоению дисциплины (модуля)**

Курс 'Машинное обучение' нацелен на выполнение лабораторных работ (создания программного обеспечения). Студентам даны рекомендации к выполнению отдельных частей работы, а также приведены постановки экспериментов для исследования созданного программного обеспечения и примерные формы отчетности по лабораторной работе.

Общие цели работы: формирование и закрепление у студентов навыков выполнения научно-исследовательских задач; актуализация, углубление и закрепление знаний, полученных при изучении теоретического материала; ознакомление студентов с процессом обучения нейронных сетей при решении задачи распознавания образов.

Для написания реферата студенту необходимо освоить следующие темы: основы теории нейронных сетей, их архитектуру и типы; основные определения теории нейронных сетей; методы обучения нейронных сетей; основные проблемы и задачи, решаемые в области нейронных сетей. Далее необходимо использовать полученные знания в свое теме. Описать весь процесс создания нейронных сетей.

Рекомендации по подготовке к контрольной работе. Для подготовки используется теоретический материал, выданный преподавателем, а также материал из рекомендуемой и дополнительной литературы, интернет-источников. Для подготовки к контрольной работе преподавателем предоставляется перечень тем и подразделов, по которым будет проводится работа.

При подготовке к зачёты студент должен изучить предложенную литературу, просмотреть открытые источники, может пройти курсы по машинному обучению представленные на открытых интернет площадках. В результате студент должен уметь обрабатывать и анализировать данные, полученные в ходе проведения экспериментов; прослеживать причинно-следственные связи и устанавливать закономерности в результатах экспериментов в зависимости от входных параметров; давать характеристику и описание нейронным сетям без обратных связей; предлагать методы обучения в зависимости от типа решаемой задачи.

## **10. Перечень информационных технологий, используемых при осуществлении образовательного процесса по дисциплине (модулю), включая перечень программного обеспечения и информационных справочных систем (при необходимости)**

Перечень информационных технологий, используемых при осуществлении образовательного процесса по дисциплине (модулю), включая перечень программного обеспечения и информационных справочных систем, представлен в Приложении 3 к рабочей программе дисциплины (модуля).

## **11. Описание материально-технической базы, необходимой для осуществления образовательного процесса по дисциплине (модулю)**

Материально-техническое обеспечение образовательного процесса по дисциплине (модулю) включает в себя следующие компоненты:

Помещения для самостоятельной работы обучающихся, укомплектованные специализированной мебелью (столы и стулья) и оснащенные компьютерной техникой с возможностью подключения к сети "Интернет" и обеспечением доступа в электронную информационно-образовательную среду КФУ.

Учебные аудитории для контактной работы с преподавателем, укомплектованные специализированной мебелью (столы и стулья).

Компьютер и принтер для распечатки раздаточных материалов.

Мультимедийная аудитория.

Компьютерный класс.

## **12. Средства адаптации преподавания дисциплины к потребностям обучающихся инвалидов и лиц с ограниченными возможностями здоровья**

При необходимости в образовательном процессе применяются следующие методы и технологии, облегчающие восприятие информации обучающимися инвалидами и лицами с ограниченными возможностями здоровья:

- создание текстовой версии любого нетекстового контента для его возможного преобразования в альтернативные формы, удобные для различных пользователей;
- создание контента, который можно представить в различных видах без потери данных или структуры, предусмотреть возможность масштабирования текста и изображений без потери качества, предусмотреть доступность управления контентом с клавиатуры;
- создание возможностей для обучающихся воспринимать одну и ту же информацию из разных источников - например, так, чтобы лица с нарушениями слуха получали информацию визуально, с нарушениями зрения - аудиально;

- применение программных средств, обеспечивающих возможность освоения навыков и умений, формируемых дисциплиной, за счёт альтернативных способов, в том числе виртуальных лабораторий и симуляционных технологий;
- применение дистанционных образовательных технологий для передачи информации, организации различных форм интерактивной контактной работы обучающегося с преподавателем, в том числе вебинаров, которые могут быть использованы для проведения виртуальных лекций с возможностью взаимодействия всех участников дистанционного обучения, проведения семинаров, выступления с докладами и защиты выполненных работ, проведения тренингов, организации коллективной работы;
- применение дистанционных образовательных технологий для организации форм текущего и промежуточного контроля;
- увеличение продолжительности сдачи обучающимся инвалидом или лицом с ограниченными возможностями здоровья форм промежуточной аттестации по отношению к установленной продолжительности их сдачи;
- продолжительности сдачи зачёта или экзамена, проводимого в письменной форме, - не более чем на 90 минут;
- продолжительности подготовки обучающегося к ответу на зачёте или экзамене, проводимом в устной форме, - не более чем на 20 минут;
- продолжительности выступления обучающегося при защите курсовой работы - не более чем на 15 минут.

Программа составлена в соответствии с требованиями ФГОС ВО и учебным планом по направлению 10.04.01 "Информационная безопасность" и магистерской программе "Математические методы и программные технологии защиты информации".

**Приложение 2**  
к рабочей программе дисциплины (модуля)  
**Б1.В.ДВ.4 Машинное обучение**

**Перечень литературы, необходимой для освоения дисциплины (модуля)**

Направление подготовки: 10.04.01 - Информационная безопасность

Профиль подготовки: Математические методы и программные технологии защиты информации

Квалификация выпускника: магистр

Форма обучения: очное

Язык обучения: русский

Год начала обучения по образовательной программе: 2017

**Основная литература:**

1. Машинное обучение. Наука и искусство построения алгоритмов, которые извлекают знания из данных [Электронный ресурс] / Флах П. -

М. : ДМК Пресс, 2015. - <http://www.studentlibrary.ru/book/ISBN9785970602737.html>

2. Вьюгин, В.В. Математические основы машинного обучения и прогнозирования [Электронный ресурс] : учеб. пособие ? Электрон. дан. ?

Москва : МЦНМО, 2013. ? 304 с. ? Режим доступа: <https://e.lanbook.com/book/56397> ? Загл. с экрана.

3. Жданов, А.А. Автономный искусственный интеллект [Электронный ресурс] : учеб. пособие ? Электрон. дан. ?

Москва : Издательство 'Лаборатория знаний', 2015. ? 362 с. ? Режим доступа: <https://e.lanbook.com/book/70761> ? Загл. с экрана

**Дополнительная литература:**

1. Информационные аналитические системы [Электронный ресурс] : учебник / Т. В. Алексеева, Ю. В. Амириди, В. В. Дик и др.; под ред. В. В. Дика. -

М.: МФПУ Синергия, 2013. - 384 с. Режим доступа: <http://znanium.com/bookread2.php?book=451186>

2. Осипов Г. В. Методы искусственного интеллекта/Осипов Г. В. - М.: Физматлит, 2011. - 296 с.

<http://znanium.com/bookread2.php?book=544787>

3. Гаврилова И. В., Масленникова, О. Е. Основы искусственного интеллекта [Электронный ресурс]: учеб. пособие / О. Е. Масленникова, И. В. Гаврилова. -

2-е изд., стер. - М.: ФЛИНТА, 2013. - 282 с. - ISBN 978-5-9765-1602-1.

<http://znanium.com/catalog.php?bookinfo=465912>

Приложение 3  
к рабочей программе дисциплины (модуля)  
Б1.В.ДВ.4 Машинное обучение

**Перечень информационных технологий, используемых для освоения дисциплины (модуля), включая перечень программного обеспечения и информационных справочных систем**

Направление подготовки: 10.04.01 - Информационная безопасность

Профиль подготовки: Математические методы и программные технологии защиты информации

Квалификация выпускника: магистр

Форма обучения: очное

Язык обучения: русский

Год начала обучения по образовательной программе: 2017

Освоение дисциплины (модуля) предполагает использование следующего программного обеспечения и информационно-справочных систем:

Операционная система Microsoft Windows 7 Профессиональная или Windows XP (Volume License)

Пакет офисного программного обеспечения Microsoft Office 365 или Microsoft Office Professional plus 2010

Браузер Mozilla Firefox

Браузер Google Chrome

Adobe Reader XI или Adobe Acrobat Reader DC

Kaspersky Endpoint Security для Windows

Учебно-методическая литература для данной дисциплины имеется в наличии в электронно-библиотечной системе "ZNANIUM.COM", доступ к которой предоставлен обучающимся. ЭБС "ZNANIUM.COM" содержит произведения крупнейших российских учёных, руководителей государственных органов, преподавателей ведущих вузов страны, высококвалифицированных специалистов в различных сферах бизнеса. Фонд библиотеки сформирован с учетом всех изменений образовательных стандартов и включает учебники, учебные пособия, учебно-методические комплексы, монографии, авторефераты, диссертации, энциклопедии, словари и справочники, законодательно-нормативные документы, специальные периодические издания и издания, выпускаемые издательствами вузов. В настоящее время ЭБС ZNANIUM.COM соответствует всем требованиям федеральных государственных образовательных стандартов высшего образования (ФГОС ВО) нового поколения.