Министерство науки и высшего образования РФ
Федеральное государственное автономное образовательное учреждение высшего образования
«СИБИРСКИЙ ФЕДЕРАЛЬНЫЙ УНИВЕРСИТЕТ»

СОГЛАСОВАНО	**УТВЕРЖДАЮ**
Заведующий кафедрой	**Заведующий кафедрой**
Кафедра прикладной математики и компьютерной безопасности (ПМКБ_ИКИТ)	**Кафедра прикладной математики и компьютерной безопасности (ПМКБ_ИКИТ)**
наименование кафедры	наименование кафедры
	А.А. Кытманов
подпись, инициалы, фамилия	подпись, инициалы, фамилия
«____» _____ 20__г.	«____» _____ 20__г.
институт, реализующий ОП ВО	институт, реализующий дисциплину

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ МАШИННОЕ ОБУЧЕНИЕ И КРИПТОГРАФИЯ (APPLICATIONS OF MACHINE LEARNING IN CRYPTOGRAPHY)

Дисциплина Б1.В.ДВ.02.02 Машинное обучение и криптография (Applications of Machine Learning in Cryptography)

Направление подготовки / специальность 01.04.02 Прикладная математика и информатика, программа 01.04.02.09 Data Science and Mathematical Modeling 2020г

Направленность (профиль)

Форма обучения очная

Год набора 2020

Красноярск 2021

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ

составлена в соответствии с Федеральным государственным образовательным стандартом высшего образования с учетом профессиональных стандартов по укрупненной группе

010000 «МАТЕМАТИКА И МЕХАНИКА»

Направление подготовки /специальность (профиль/специализация)

Направление 01.04.02 Прикладная математика и информатика,
программа 01.04.02.09 Data Science and Mathematical Modeling 2020г.

Программу составили

1 Цели и задачи изучения дисциплины

1.1 Цель преподавания дисциплины

Ознакомление студентов с новым подходом к решению проблем криптографии с помощью искусственных нейронных сетей

1.2 Задачи изучения дисциплины

- Изучение нейросетевых криптосетей, принципов шифрования с помощью нейросетей
- Формирование навыков реализация алгоритмов шифрования на основе нейронных сетей.

1.3 Перечень планируемых результатов обучения по дисциплине (модулю), соотнесенных с планируемыми результатами освоения образовательной программы

УК-1:Способен осуществлять критический анализ проблемных ситуаций на основе системного подхода, вырабатывать стратегию действий.
УК-1.2:Определяет пробелы в информации, необходимой для решения проблемной ситуации, и проектирует процессы по их устранению.
УК-1.3:Критически оценивает надежность источников информации, работает с противоречивой информацией из разных источников.
УК-1.4:Разрабатывает и содержательно аргументирует стратегию решения проблемной ситуации на основе системного и междисциплинарных подходов.
ПК-3:Способен управлять разработкой продуктов, услуг и решений на основе данных.
ПК-3.1:Знает: состояние и перспективы развития информационных технологий, технологий данных в России и в мире; современные и перспективные методы сбора, хранения и передачи данных; источники данных, интенсивность генерации данных источниками; технические средства и среды сбора, хранения и обработки данных; современные и перспективные средства визуализации и интерпретации данных; исследование операций; машинное обучение; математическое моделирование; методы сравнительного анализа.
ПК-3.2:Способен проводить аналитические и поисковые исследования по тематике информационных технологий, технологий данных.
ПК-4:Способен разрабатывать и внедрять новые методы и технологии исследования данных.
ПК-4.1:Знает: состояние и перспективы развития информационных технологий, технологий данных в России и в мире; современные и перспективные методы сбора, хранения и передачи данных; источники данных, интенсивность генерации данных источниками; технические средства и среды сбора, хранения и обработки данных; современные и перспективные средства визуализации и интерпретации данных; исследование операций; машинное обучение; математическое моделирование; методы сравнительного анализа.
ПК-4.2:Способен проводить аналитические и поисковые исследования по тематике информационных технологий, технологий данных.

1.4 Место дисциплины (модуля) в структуре образовательной программы

Основы криптографии
Базовые модели и методы машинного обучения
Основы криптографии (The Basics of Cryptography)
Базовые модели и методы машинного обучения (The Basics of Machine Learning)

Прикладные задачи анализа данных
выполнение и защита выпускной квалификационной работы
Прикладные задачи анализа данных (Applied Data Analysis)
Выполнение и защита выпускной квалификационной работы (Final certification)

1.5 Особенности реализации дисциплины
Язык реализации дисциплины Английский.

Дисциплина (модуль) реализуется без применения ЭО и ДОТ.

2. Объем дисциплины (модуля)

Вид учебной работы	Всего, зачетных единиц (акад.час)	Семестр
		3
Общая трудоемкость дисциплины	**3 (108)**	**3 (108)**
Контактная работа с преподавателем:	**1 (36)**	**1 (36)**
занятия лекционного типа	0,5 (18)	0,5 (18)
занятия семинарского типа		
в том числе: семинары		
практические занятия	0,5 (18)	0,5 (18)
практикумы		
лабораторные работы		
другие виды контактной работы		
в том числе: групповые консультации		
индивидуальные консультации		
иная внеаудиторная контактная работа:		
групповые занятия		
индивидуальные занятия		
Самостоятельная работа обучающихся:	**2 (72)**	**2 (72)**
изучение теоретического курса (ТО)		
расчетно-графические задания, задачи (РГЗ)		
реферат, эссе (Р)		
курсовое проектирование (КП)	Нет	Нет
курсовая работа (КР)	Нет	Нет
Промежуточная аттестация (Зачёт)		

3 Содержание дисциплины (модуля)

3.1 Разделы дисциплины и виды занятий (тематический план занятий)

№ п/п	Модули, темы (разделы) дисциплины	Занятия лекционного типа (акад.час)	Занятия семинарского типа		Самостоятельная работа, (акад.час)	Формируемые компетенции
			Семинары и/или Практические занятия (акад.час)	Лабораторные работы и/или Практикумы (акад.час)		
1	2	3	4	5	6	7
1	Neural network technologies in cryptography	18	18	0	72	
Всего		18	18	0	72	

3.2 Занятия лекционного типа

№ п/п	№ раздела дисциплины	Наименование занятий	Объем в акад.часах		
			Всего	в том числе, в инновационной форме	в том числе, в электронной форме
1	1	Neural Cryptosystem	2	0	0
2	1	Extended Security Neural Networks	2	0	0
3	1	The perceptron problem and its cryptographic applications	2	0	0
4	1	Neural-like secret calculation structure for dynamic threshold schemes	2	0	0
5	1	Neural network for localization of erroneous private secrets of the threshold circuit	2	0	0
6	1	Finite ring neural networks for implementing threshold secretion separation schemes	2	0	0

7	1	Modifikatsii struktur neyronnykh sistem v kriptografii 52/5000 Modifications of the structures of neural systems in cryptography	2	0	0
8	1	Interactive Neural Networks in Cryptography	2	0	0
9	1	Neural network technologies in public key cryptographic systems	2	0	0
Всего			18	0	0

3.3 Занятия семинарского типа

№ п/п	№ раздела дисциплины	Наименование занятий	Объем в акад.часах		
			Всего	в том числе, в инновационной форме	в том числе, в электронной форме
1	1	Neural Cryptosystem	2	0	0
2	1	Extended Security Neural Networks	2	0	0
3	1	The perceptron problem and its cryptographic applications	2	0	0
4	1	Neural-like secret calculation structure for dynamic threshold schemes	2	0	0
5	1	Neural network for localization of erroneous private secrets of the threshold circuit	2	0	0
6	1	Finite ring neural networks for implementing threshold secretion separation schemes	2	0	0
7	1	Modifications of the structures of neural systems in cryptography	2	0	0
8	1	Interactive Neural Networks in Cryptography	2	0	0
9	1	Neural network technologies in public key cryptographic systems	2	0	0
Всего			18	0	0

3.4 Лабораторные занятия

№ п/п	№ раздела дисциплины	Наименование занятий	Объем в акад.часах		
			Всего	в том числе, в инновационной форме	в том числе, в электронной форме
Всего					

5 Фонд оценочных средств для проведения промежуточной аттестации

Оценочные средства находятся в приложении к рабочим программам дисциплин.

6 Перечень основной и дополнительной учебной литературы, необходимой для освоения дисциплины (модуля)

6.1. Основная литература			
	Авторы, составители	Заглавие	Издательство, год
Л1.1	Zeidler E.	Quantum Field Theory II: Quantum Electrodynamics. A Bridge between Mathematicians and Physicists: монография	New York: Springer-Verlag, 2009
Л1.2	Begg R., Palaniswami M.	Computational Intelligence for Movement Sciences: Neural Networks and Other Emerging Techniques	Hershey: Idea Group Publishing, 2006
6.2. Дополнительная литература			
	Авторы, составители	Заглавие	Издательство, год
Л2.1	Galushkin A. I.	Neural Networks Theory: with 176 figures	New York: Springer-Verlag, 2007

8 Методические указания для обучающихся по освоению дисциплины (модуля)

Для получения допуска к зачету по дисциплине необходимо выполнить преложенные лабораторные работы, защитить их в ходе собеседования с преподавателем.

Зачет проходит в устной форме по вопросам к зачету из предложенного перечня.

9 Перечень информационных технологий, используемых при осуществлении образовательного процесса по дисциплине (модулю) (при необходимости)

9.1 Перечень необходимого программного обеспечения

9.1.1	Язык программирования Python

9.2 Перечень необходимых информационных справочных систем

9.2.1	электронные информационно-справочные ресурсы научной библиотеки СФУ (http://bik.sfu-kras.ru)

10 Материально-техническая база, необходимая для осуществления образовательного процесса по дисциплине (модулю)

Учебные лаборатории и классы, оснащенные современными компьютерами, объединенными в локальные вычислительные сети с выходом в Интернет, а также периферийным и проекционным оборудованием.