

ФГБОУ ВО «БАШКИРСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ»
ФАКУЛЬТЕТ МАТЕМАТИКИ И ИНФОРМАЦИОННЫХ ТЕХНОЛОГИЙ

Утверждено:
на заседании кафедры
протокол № 9 от «28» февраля 2022 г.
Зав. кафедрой _____ /С.А. Мустафина

Согласовано:
Председатель УМК факультета
_____ /А.М. Ефимов

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ (МОДУЛЯ)

дисциплина Спецсеминар "Искусственный интеллект в кибербезопасности"

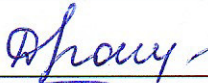
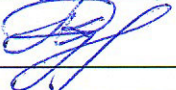
Факультативные дисциплины

программа магистратуры

Направление подготовки (специальность)
01.04.02 «Прикладная математика и информатика»

Направленность (профиль) подготовки
Искусственный интеллект в кибербезопасности

Квалификация
магистр

Разработчик (составитель) Доцент, к.ф.-м.н.	 /Юнусова Д.С.
Доцент, к.х.н.	 /Корнилова А.А.

Для приема: 2022

Уфа 2022 г.

Составители: Юнусова Дарья Сергеевна, к.ф.-м.н., доцент кафедры математического моделирования, Корнилова Алия Адиповна, к.х.н., доцент кафедры математического моделирования.

Программа утверждена ученым советом факультета математики и информационных технологий:
протокол № 7 от «1» марта 2022 г.

Дополнения и изменения, внесенные в программу практики, утверждены на заседании ученого совета факультета / института:

,

протокол № ____ от « ____ » _____ 201 _ г.

Декан/ Директор _____ / Ф.И.О./

Дополнения и изменения, внесенные в программу практики, утверждены на заседании ученого совета факультета / института:

,

протокол № ____ от « ____ » _____ 201 _ г.

Декан/ Директор _____ / Ф.И.О./

Дополнения и изменения, внесенные в программу практики, утверждены на заседании ученого совета факультета / института:

,

протокол № ____ от « ____ » _____ 201 _ г.

Декан/ Директор _____ / Ф.И.О./

Дополнения и изменения, внесенные в программу практики, утверждены на заседании ученого совета факультета / института:

,

протокол № ____ от « ____ » _____ 201 _ г.

Декан/ Директор _____ / Ф.И.О./

Список документов и материалов

1. Перечень планируемых результатов обучения по дисциплине, соотнесенных с установленными в образовательной программе индикаторами достижения компетенций
2. Цель и место дисциплины в структуре образовательной программы
3. Содержание рабочей программы (объем дисциплины, типы и виды учебных занятий, учебно-методическое обеспечение самостоятельной работы обучающихся)
4. Фонд оценочных средств по дисциплине
 - 4.1. Перечень компетенций и индикаторов достижения компетенций с указанием соотнесенных с ними запланированных результатов обучения по дисциплине. Описание критериев и шкал оценивания результатов обучения по дисциплине.
 - 4.2. Типовые контрольные задания или иные материалы, необходимые для оценивания результатов обучения по дисциплине, соотнесенных с установленными в образовательной программе индикаторами достижения компетенций. Методические материалы, определяющие процедуры оценивания результатов обучения по дисциплине.
5. Учебно-методическое и информационное обеспечение дисциплины
 - 5.1. Перечень основной и дополнительной учебной литературы, необходимой для освоения дисциплины
 - 5.2. Перечень ресурсов информационно-телекоммуникационной сети «Интернет» и программного обеспечения, необходимых для освоения дисциплины, включая профессиональные базы данных и информационные справочные системы
6. Материально-техническая база, необходимая для осуществления образовательного процесса по дисциплине

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

По итогам освоения дисциплины обучающийся должен достичь следующих результатов обучения:

Категория (группа) компетенций	Формируемая компетенция (с указанием кода)	Код и наименование индикатора достижения компетенции	Результаты обучения по дисциплине
	ОПК-4. Способен комбинировать и адаптировать существующие информационно-коммуникационные технологии для решения задач в области профессиональной деятельности с учетом требований информационной безопасности	ОПК-4.1. Адаптирует известные научные принципы и методы исследований с целью их практического применения	Адаптирует известные научные принципы и методы исследований с целью их практического применения
		ОПК-4.2. Решает профессиональные задачи на основе применения новых научных принципов и методов исследования	Решает профессиональные задачи на основе применения новых научных принципов и методов исследования
		ОПК-4.3. Использует современные подходы к верификации ПО в профессиональной деятельности с учетом требований информационной безопасности	Использует современные подходы к верификации ПО в профессиональной деятельности с учетом требований информационной безопасности
	ПК-6. Способен руководить проектами по созданию комплексных систем на основе аналитики больших данных в различных отраслях	ПК-6.1. Осуществляет руководство проектом по построению комплексных систем на основе аналитики больших данных в различных отраслях	ПК-6.1. 3-1. Знает методологию и принципы руководства проектом по созданию, поддержке и использованию комплексных систем на основе аналитики больших данных
			ПК-6.1. 3-2. Знает специфику сфер и отраслей, для которых реализуется проект по аналитике больших данных
			ПК-6.1. У-1. Умеет решать задачи по руководству коллективной проектной деятельностью для создания, поддержки и использования комплексных систем на основе аналитики больших данных
			ПК-6.1. У-2. Умеет сосредотачивать внимание на целях, достижение которых обеспечивает большую отдачу и сильное воздействие
			ПК-6.1. У-3. Умеет формировать матрицу приоритетов, включая критерии отбора проектов для реализации
			ПК-6.2. Применяет варианты использования больших данных, определений, словарей и эталонной архитектуры больших данных при руководстве проектами по построению комплексных систем на основе аналитики больших данных в различных отраслях
		ПК-6.2. У-1. Умеет определять риски, связанные с реализацией / развертыванием инициатив / проектов в области аналитики больших данных	
		ПК-6.2. У-2. Умеет описывать каждый риск на различных этапах развертывания аналитики больших данных, его воздействие, реализацию и серьезность	

			ПК-6.2. У-3. Умеет определять цели проектов в области аналитики больших данных в организации / подразделениях / службах
			ПК-6.2. У-4. Умеет разрабатывать стратегические планы на уровне организации для проектов аналитики больших данных
		ПК-6.3. Проводит планирование, управление, развертывание, аудит безопасности и защиты персональных данных при работе с большими данными и руководит операционной деятельностью, связанной с безопасностью и защитой персональных данных при работе с большими данными	ПК-6.3. З-1. Знает терминологию и последовательность мероприятий по безопасности и защите персональных данных при работе с большими данными
			ПК-6.3. У-1. Умеет проводить подготовку и планирование действий по верхнеуровневому управлению безопасностью и защитой персональных данных при работе с большими данными
			ПК-6.3. У-2. Умеет проводить мониторинг, оценку и контроль действий по верхнеуровневому управлению безопасностью и защитой персональных данных при работе с большими данными
			ПК-6.3. У-3. Умеет определять цели верхнеуровневого управления безопасностью и защитой персональных данных при работе с большими данными

2. Цель и место дисциплины в структуре образовательной программы

Дисциплина *Спецсеминар "Искусственный интеллект в кибербезопасности"* относится к блоку Факультативные дисциплины. Дисциплина изучается на 1 курсе в 1 и 2 семестрах.

Целью изучения дисциплины является научить студентов руководить проектами по созданию комплексных систем на основе аналитики больших данных в различных отраслях

Для освоения дисциплины необходимы компетенции, сформированные в рамках изучения следующих дисциплин: «Управление научными проектами», «Системный подход к решению проблем в профессиональной деятельности».

3. Содержание рабочей программы (объем дисциплины, типы и виды учебных занятий, учебно-методическое обеспечение самостоятельной работы обучающихся)

Содержание рабочей программы представлено в Приложении № 1.

4. Фонд оценочных средств по дисциплине

4.1. Перечень компетенций и индикаторов достижения компетенций с указанием соотнесенных с ними запланированных результатов обучения по дисциплине. Описание критериев и шкал оценивания результатов обучения по дисциплине.

Код и формулировка компетенции ПК-1 Способен демонстрировать базовые знания математических и естественных наук, программирования и информационных технологий

Код и наименование индикатора достижения компетенции	Результаты обучения по дисциплине	Критерии оценивания результатов обучения	
		Зачтено	Не зачтено
ОПК-4.1. Адаптирует известные научные принципы и методы исследований с целью их практического применения	ОПК-4.1. У-1. Умеет адаптировать известные научные принципы и методы исследований с целью их практического применения	В целом успешное, но содержащее отдельные пробелы умение адаптировать известные научные принципы и методы исследований с целью их практического применения	Фрагментарные умения адаптировать известные научные принципы и методы исследований с целью их практического применения
ОПК-4.2. Решает профессиональные задачи на основе применения новых научных принципов и методов исследования	ОПК-4.1. У-1. Умеет решать профессиональные задачи на основе применения новых научных принципов и методов исследования	В целом успешное, но содержащее отдельные пробелы умение решать профессиональные задачи на основе применения новых научных принципов и методов исследования	Фрагментарные умения решать профессиональные задачи на основе применения новых научных принципов и методов исследования
ОПК-4.3. Использует современные подходы к верификации ПО в профессиональной деятельности с учетом требований информационной безопасности	ОПК-4.1. У-1. Умеет использовать современные подходы к верификации ПО в профессиональной деятельности с учетом требований информационной безопасности	В целом успешное, но не систематическое владение навыками использования современных подходов к верификации ПО в профессиональной деятельности с учетом требований информационной безопасности	Фрагментарное владение навыками использования современных подходов к верификации ПО в профессиональной деятельности с учетом требований информационной безопасности
ПК-6.1. Осуществляет руководство проектом по построению комплексных систем на основе аналитики больших данных в различных отраслях.	ПК-6.1. З-1. Знает методологию и принципы руководства проектом по созданию, поддержке и использованию комплексных систем на основе аналитики больших данных.	Фрагментарные представления о методологии и принципах руководства проектом по созданию, поддержке и использованию комплексных систем на основе аналитики больших данных.	Сформированные систематические представления о методологию и принципы руководства проектом по созданию, поддержке и использованию комплексных систем на основе аналитики больших данных.
ПК-6.1. Осуществляет руководство проектом по построению комплексных систем на основе аналитики больших данных в различных отраслях	ПК-6.1. З-2. Знает специфику сфер и отраслей, для которых реализуется проект по аналитике больших данных	Фрагментарное знания о специфике сфер и отраслей, для которых реализуется проект по аналитике больших данных	В целом успешное, но не систематическое знания о специфике сфер и отраслей, для которых реализуется проект по аналитике больших данных
ПК-6.1. Осуществляет руководство проектом по построению комплексных систем на основе аналитики больших данных в различных отраслях	ПК-6.1. У-1. Умеет решать задачи по руководству коллективной проектной деятельностью для создания, поддержки и использования комплексных систем на основе аналитики	Фрагментарные умения решать задачи по руководству коллективной проектной деятельностью для создания, поддержки и использования комплексных систем на основе аналитики больших данных.	В целом успешное, но не систематическое умение решать задачи по руководству коллективной проектной деятельностью для создания, поддержки и использования комплексных систем на основе аналитики больших данных

	больших данных		
ПК-6.1. Осуществляет руководство проектом по построению комплексных систем на основе аналитики больших данных в различных отраслях	ПК-6.1. У-2. Умеет сосредотачивать внимание на целях, достижение которых обеспечивает большую отдачу и сильное воздействие	Фрагментарные умения сосредотачивать внимание на целях, достижение которых обеспечивает большую отдачу и сильное воздействие	В целом успешное, но не систематическое умение сосредотачивать внимание на целях, достижение которых обеспечивает большую отдачу и сильное воздействие
ПК-6.1. Осуществляет руководство проектом по построению комплексных систем на основе аналитики больших данных в различных отраслях	ПК-6.1. У-3. Умеет формировать матрицу приоритетов, включая критерии отбора проектов для реализации	Фрагментарные умения формировать матрицу приоритетов, включая критерии отбора проектов для реализации.	В целом успешное, но не систематическое умение формировать матрицу приоритетов, включая критерии отбора проектов для реализации.
ПК-6.2. Применяет варианты использования больших данных, определений, словарей и эталонной архитектуры больших данных при руководстве проектами по построению комплексных систем на основе аналитики больших данных в различных отраслях	ПК-6.2. У-1. Умеет определять риски, связанные с реализацией / развертыванием инициатив / проектов в области аналитики больших данных	Фрагментарные умения определять риски, связанные с реализацией / развертыванием инициатив / проектов в области аналитики больших данных.	В целом успешное, но не систематическое умение определять риски, связанные с реализацией / развертыванием инициатив / проектов в области аналитики больших данных.
ПК-6.2. Применяет варианты использования больших данных, определений, словарей и эталонной архитектуры больших данных при руководстве проектами по построению комплексных систем на основе аналитики больших данных в различных отраслях	ПК-6.2. У-2. Умеет описывать каждый риск на различных этапах развертывания аналитики больших данных, его воздействие, реализацию и серьезность	Фрагментарные умения описывать каждый риск на различных этапах развертывания аналитики больших данных, его воздействие, реализацию и серьезность.	В целом успешное, но не систематическое умение описывать каждый риск на различных этапах развертывания аналитики больших данных, его воздействие, реализацию и серьезность.
ПК-6.2. Применяет варианты использования больших данных, определений, словарей и эталонной архитектуры больших данных при руководстве проектами по построению комплексных систем на основе аналитики больших данных в различных отраслях	ПК-6.2. У-3. Умеет определять цели проектов в области аналитики больших данных в организации / подразделениях / службах	Фрагментарные умения определять цели проектов в области аналитики больших данных в организации / подразделениях / службах.	В целом успешное, но не систематическое умение определять цели проектов в области аналитики больших данных в организации / подразделениях / службах.
ПК-6.2. Применяет варианты использования больших данных, определений, словарей и	ПК-6.2. У-4. Умеет разрабатывать стратегические планы на уровне	Фрагментарные умения разрабатывать стратегические планы на уровне организации для проектов аналитики	В целом успешное, но не систематическое умение разрабатывать стратегические планы на уровне организации

эталонной архитектуры больших данных при руководстве проектами по построению комплексных систем на основе аналитики больших данных в различных отраслях	организации для проектов аналитики больших данных	больших данных.	для проектов аналитики больших данных.
ПК-6.3. Проводит планирование, управление, развертывание, аудит безопасности и защиты персональных данных при работе с большими данными и руководит операционной деятельностью, связанной с безопасностью и защитой персональных данных при работе с большими данными	ПК-6.3. З-1. Знает терминологию и последовательность мероприятий по безопасности и защите персональных данных при работе с большими данными	Фрагментарные знания о терминологии и последовательности мероприятий по безопасности и защите персональных данных при работе с большими данными.	В целом успешное, но не систематическое о знании терминологии и последовательности мероприятий по безопасности и защите персональных данных при работе с большими данными.
ПК-6.3. Проводит планирование, управление, развертывание, аудит безопасности и защиты персональных данных при работе с большими данными и руководит операционной деятельностью, связанной с безопасностью и защитой персональных данных при работе с большими данными	ПК-6.3. У-1. Умеет проводить подготовку и планирование действий по верхнеуровневому управлению безопасностью и защитой персональных данных при работе с большими данными	Фрагментарные умения проводить подготовку и планирование действий по верхнеуровневому управлению безопасностью и защитой персональных данных при работе с большими данными	В целом успешное, но не систематическое умение проводить подготовку и планирование действий по верхнеуровневому управлению безопасностью и защитой персональных данных при работе с большими данными
ПК-6.3. Проводит планирование, управление, развертывание, аудит безопасности и защиты персональных данных при работе с большими данными и руководит операционной деятельностью, связанной с безопасностью и защитой персональных данных при работе с большими данными	ПК-6.3. У-2. Умеет проводить мониторинг, оценку и контроль действий по верхнеуровневому управлению безопасностью и защитой персональных данных при работе с большими данными	Фрагментарные умения проводить мониторинг, оценку и контроль действий по верхнеуровневому управлению безопасностью и защитой персональных данных при работе с большими данными	В целом успешное, но не систематическое умение проводить мониторинг, оценку и контроль действий по верхнеуровневому управлению безопасностью и защитой персональных данных при работе с большими данными
ПК-6.3. Проводит планирование, управление, развертывание, аудит безопасности и защиты персональных данных при работе с большими данными и руководит операционной деятельностью, связанной с безопасностью и защитой персональных данных при работе с большими данными	ПК-6.3. У-3. Умеет определять цели верхнеуровневого управления безопасностью и защитой персональных данных при работе с большими данными	Фрагментарные умения определять цели верхнеуровневого управления безопасностью и защитой персональных данных при работе с большими данными.	В целом успешное, но не систематическое умение определять цели верхнеуровневого управления безопасностью и защитой персональных данных при работе с большими данными

безопасностью и защитой персональных данных при работе с большими данными			
---	--	--	--

4.2. Типовые контрольные задания или иные материалы, необходимые для оценивания результатов обучения по дисциплине, соотнесенных с установленными в образовательной программе индикаторами достижения компетенций. Методические материалы, определяющие процедуры оценивания результатов обучения по дисциплине.

Код и наименование индикатора достижения компетенции	Результаты обучения по дисциплине	Оценочные средства
ОПК-4. Способен комбинировать и адаптировать существующие информационно-коммуникационные технологии для решения задач в области профессиональной деятельности с учетом требований информационной безопасности	ОПК-4.1. Адаптирует известные научные принципы и методы исследований с целью их практического применения	Групповой и индивидуальный опрос Практические работы Зачет
	ОПК-4.2. Решает профессиональные задачи на основе применения новых научных принципов и методов исследования	Групповой и индивидуальный опрос Практические работы Зачет
	ОПК-4.3. Использует современные подходы к верификации ПО в профессиональной деятельности с учетом требований информационной безопасности	Групповой и индивидуальный опрос Практические работы Зачет
ПК-6. Способен руководить проектами по созданию комплексных систем на основе аналитики больших данных в различных отраслях.	ПК-6.1. Осуществляет руководство проектом по построению комплексных систем на основе аналитики больших данных в различных отраслях.	Групповой и индивидуальный опрос Практические работы Зачет
	ПК-6.2. Применяет варианты использования больших данных, определений, словарей и эталонной архитектуры больших данных при руководстве проектами по построению комплексных систем на основе аналитики больших данных в различных отраслях.	Групповой и индивидуальный опрос Практические работы Зачет
	ПК-6.3. Проводит планирование, управление, развертывание, аудит безопасности и защиты персональных данных при работе с большими данными и руководит операционной деятельностью, связанной с безопасностью и защитой персональных данных при работе с большими данными.	Групповой и индивидуальный опрос Практические работы Зачет

Критериями оценивания при *модульно-рейтинговой системе* являются баллы, которые выставляются преподавателем за виды деятельности (оценочные средства) по итогам изучения модулей (разделов дисциплины), перечисленных в рейтинг-плане дисциплины (для зачета: текущий контроль – максимум 50 баллов; рубежный контроль – максимум 50 баллов, поощрительные баллы – максимум 10).

Шкалы оценивания:

(для зачета:

зачтено – от 60 до 110 рейтинговых баллов (включая 10 поощрительных баллов),
не зачтено – от 0 до 59 рейтинговых баллов).

Типовые вопросы к зачету

1. Обнаружение и предотвращение вторжений.
2. Защита конечных устройств.
3. Поведенческий анализ действий пользователей.
4. Адаптивная аутентификация.
5. Регрессия (Regression) – задача прогнозирования следующего значения на основе предыдущих.
6. Классификация (Classification) – задача разделения объектов на разные категории.
7. Кластеризация (Clustering)– задача группировки объектов по сходству.
8. Визуализация метода иерархической кластеризации в виде графа.

Лабораторная работа

Цель проведения лабораторных работы – самостоятельная деятельность студента по освоению предметной части изучаемой дисциплины.

Примеры заданий

- Лабораторная работа №1. Выбор темы исследования.
Лабораторная работа №2. План реализации работы.
Лабораторная работа №3. Разработка проекта.
Лабораторная работа №4. Тест проекта и исправление ошибок.
Лабораторная работа №5. Защита проекта.

Типовые работы.

курс 1, семестр 1

1. Исследование и разработка детектора атак уклонением на искусственные нейронные сети.
2. Исследование и разработка анализатора данных на предмет содержания атакующих данных.
3. Исследование и разработка комплекса имитации атак на глубокие нейронные сети.

Типовые работы.

курс 1, семестр 2

4. Исследование и разработка критериев оценки устойчивости моделей машинного обучения к внешним воздействиям.
5. Исследование и разработка системы профилирования искусственной нейронной сети.
6. Исследование и разработка формальных методов верификации ИНС.
7. Исследование возможности применения существующих алгоритмов.

Рейтинг – план дисциплины

Спецсеминар "Искусственный интеллект в кибербезопасности"

(название дисциплины согласно рабочему учебному плану)

направление/специальность 01.04.02 Прикладная математика и информатика

курс 1, семестр 1

Виды учебной деятельности студентов	Балл за конкретное задание	Число заданий за семестр	Баллы	
			Минимальный	Максимальный
Модуль 1				
Текущий контроль				
Аудиторная работа	25	1	0	25
Рубежный контроль				
Лабораторная работа	5	5	0	25
Модуль 2				
Текущий контроль				
Аудиторная работа	25	1	0	25
Рубежный контроль				
Лабораторная работа	5	5	0	25
Поощрительные баллы				
1. Студенческая олимпиада	10	1	0	10
2. Публикация статей				
3. Творческие задания (выступление, презентация)				
Посещаемость (баллы вычитаются из общей суммы набранных баллов)				
1. Посещение лекционных занятий			0	-6
2. Посещение практических (семинарских, лабораторных занятий)			0	-10

Рейтинг – план дисциплины

Спецсеминар "Искусственный интеллект в кибербезопасности"

(название дисциплины согласно рабочему учебному плану)

направление/специальность 01.04.02 Прикладная математика и информатика

курс 1, семестр 2

Виды учебной деятельности студентов	Балл за конкретное задание	Число заданий за семестр	Баллы	
			Минимальный	Максимальный
Модуль 1				
Текущий контроль				
Аудиторная работа	25	1	0	25
Рубежный контроль				
Лабораторная работа	5	5	0	25
Модуль 2				
Текущий контроль				
Аудиторная работа	25	1	0	25
Рубежный контроль				
Лабораторная работа	5	5	0	25
Поощрительные баллы				
4. Студенческая олимпиада 5. Публикация статей 6. Творческие задания (выступление, презентация)	10	1	0	10
Посещаемость (баллы вычитаются из общей суммы набранных баллов)				
3. Посещение лекционных занятий			0	-6
4. Посещение практических (семинарских, лабораторных занятий)			0	-10

5. Учебно-методическое и информационное обеспечение дисциплины

5.1. Перечень основной и дополнительной учебной литературы, необходимой для освоения дисциплины

Основная литература:

1. Ясницкий, Л. Н. Интеллектуальные системы : учебник / Л. Н. Ясницкий. – 2-е изд., электрон. – Москва : Лаборатория знаний, 2020. – 224 с. : ил.,табл., схем. – (Учебник для высшей школы). – Режим доступа: по подписке. – URL: <https://biblioclub.ru/index.php?page=book&id=595480>
2. Боровская, Е. В. Основы искусственного интеллекта : учебное пособие : [16+] / Е. В. Боровская, Н. А. Давыдова. – 4-е изд., электрон. – Москва : Лаборатория знаний, 2020. – 130 с. : схем. – (Педагогическое образование). – Режим доступа: по подписке. – URL: <https://biblioclub.ru/index.php?page=book&id=595419>
3. Сурова, Н. Ю. Искусственный интеллект / Н. Ю. Сурова, М. Е. Косов. – Москва : Юнити-Дана, 2021. – 408 с. : ил., табл., схем. – Режим доступа: по подписке. – URL: <https://biblioclub.ru/index.php?page=book&id=690578>

Дополнительная литература:

4. Цилькер Б.Я., Орлов С.А. Организация ЭВМ и систем. СПб, «Питер», 2007
5. Степанов А.Н. Архитектура вычислительных систем и компьютерных сетей. СПб, «Питер», 2006
6. Крейгон Х. Архитектура компьютеров и ее реализация. М., «Мир», 2004

5.2. Перечень ресурсов информационно-телекоммуникационной сети «Интернет» и программного обеспечения, необходимых для освоения дисциплины, включая профессиональные базы данных и информационные справочные системы

1. <http://www.socionet.ru/> – Онлайн-овая научная инфраструктура, научно образовательная социальная сеть;
2. <http://www.msu.ru/> – МГУ им. М.В. Ломоносова;
3. <http://window.edu.ru/> – Наиболее обширная электронная база учебников и методических материалов на сайте информационной системы «Единое окно доступа к образовательным ресурсам»;
4. <http://www.rusneb.ru/> – Национальная электронная библиотека (НЭБ);
5. <http://enip.ras.ru/> – Единое научное информационное пространство РАН;
6. <http://univertv.ru/video/matematika/> – Открытый образовательный видеопортал Uni-verTV.ru. Образовательные фильмы на различные темы. Лекции в ведущих российских и зарубежных вузах. Научная конференция или научно-популярная лекция по

интересующему вопросу);

7. <http://eqworld.ipmnet.ru/ru/library.htm> – Учебно-образовательная физико-математическая библиотека;
8. www.lib.mexmat.ru/books/41 – Электронная библиотека МГУ;
9. www.newlibrary.ru – Новая электронная библиотека;
10. www.edu.ru – Федеральный портал российского образования;
11. www.mathnet.ru – Общероссийский математический портал;
12. www.elibrary.ru – Научная электронная библиотека;
13. www.mathburo.ru – Матбюро: решения задач по высшей математике;
14. www.nehudlit.ru – Электронная библиотека учебных материалов;
15. www.wolframcenter.ru/instructors – Wolfram Mathematica, Русскоязычная поддержка,

6. Материально-техническая база, необходимая для осуществления образовательного процесса по дисциплине

<i>Наименование специализированных аудиторий, кабинетов, лабораторий</i>	<i>Вид занятий</i>	<i>Наименование оборудования, программного обеспечения</i>
<i>1</i>	<i>2</i>	<i>3</i>
Аудитория № 528 (физико-математический корпус - учебное)	Лекции	Компьютер, мультимедийный проектор, экран, доска, учебная мебель, доска настенная меловая
Лаборатория аудитория № 520а (физико-математический корпус - учебное), № 521 (физико-математический корпус - учебное), аудитория № 522 (физико-математический корпус - учебное), аудитория № 524 (физико-математический корпус - учебное), аудитория № 525 (физико-математический корпус - учебное)	Практические работы	<p>Аудитория № 520а Учебная мебель, доска, монитор LG 19 L1942S SF 1280 x 1024,5ms,8000:1,black (3,4 кг,VGA,19"(48,3см)5мс, мониторы LG 19" L1942SBF 1280x1024,5ms,8000:1,black 10 шт., системный блок HPPavilionSlimlineS3500FAMDathlon64 X2 5400+/2.8GHz,4Gb,500Gb 12шт.,доска аудитор. ДА36.</p> <p>Аудитория № 521 Учебная мебель, доска, коммутатор HP V1905-24 Switch 24*10/100+2*10/100/1000, персональные компьютеры в комплекте DEPO Neos 460MDi5 2300/4GDDR1333/T500G/DVD W – 12 шт., проектор Optoma EX542i.DLP3D.XGA(1024*768).2700 ANSI Lm.3000 1.Lamp5000+/-40 ver, шкаф TLKTWP-065442-G-GY, экран на штативе DraperDiplomat (1:1) 84/84* 213*213 MW, доска аудитор. ДА36.</p> <p>Аудитория № 522 Учебная мебель, доска, персональный компьютер LenovoThinkCentre A70z IntelPentium E 5800, 320 Gb, 19" – 13 шт., кондиционер LessarLS/LUH24KB2.</p> <p>Аудитория № 524 Учебная мебель, доска настенная меловая, коммутатор HP V1905-24 Switch 24*10/100+2*10/100/1000, персональный компьютер в комплекте HP AiO 20"CQ 100 eu – 27 шт., экран ScreeMediaGolgviev 274*206 NW 4:3, универсальное потолочное крепление ScreeMedia для проектора, регулировка высоты , шкаф TLKTWP-065442-G-GY, патч-корд (1296), доска аудитор. ДА32.</p> <p>Аудитория № 525 Учебная мебель, доска, персональные компьютеры в комплекте DEPONeos 460MDi5 2300/4GDDR1333/T500G/DVDW/ - 13 шт., доска аудитор. ДА32</p> <p>1. Windows 8 Russian. Windows Professional 8 Russian Upgrade. Договор № 104 от 17.06.2013 г. Лицензии бессрочные. 2.</p>

<i>Наименование специализированных аудиторий, кабинетов, лабораторий</i>	<i>Вид занятий</i>	<i>Наименование оборудования, программного обеспечения</i>
<i>1</i>	<i>2</i>	<i>3</i>
		Microsoft Office Standard 2013 Russian. Договор № 114 от 12.11.2014 г. Лицензии бессрочные. 3. Среда разработки Microsoft Visual Studio Community 2017 (Условия лицензии на программное обеспечение Microsoft Visual Studio Community 2017, свободное программное обеспечение). 4. AcademicEdition Networked Volume Licenses RAD Studio XE3 Professional Concurrent AppWaveEnglish; договор №263 от 07.12.2012 г.

ФГБОУ ВО «БАШКИРСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ»
ФАКУЛЬТЕТ МАТЕМАТИКИ И ИНФОРМАЦИОННЫХ ТЕХНОЛОГИЙ

СОДЕРЖАНИЕ РАБОЧЕЙ ПРОГРАММЫ

дисциплины Спецсеминар "Искусственный интеллект в кибербезопасности" на 1 семестрочная форма обучения

Вид работы	Объем дисциплины
Общая трудоемкость дисциплины (з.е. / часов)	1/36
Учебных часов на контактную работу с преподавателем:	
лекций	
практических/ семинарских	
лабораторных	32
других (групповая, индивидуальная консультация и иные виды учебной деятельности, предусматривающие работу обучающихся с преподавателем) (ФКР)	0,2
Учебных часов на самостоятельную работу обучающихся (СР)	3,8
Учебных часов на подготовку к экзамену/зачету/дифференцированному зачету (Контроль)	

Форма(ы) контроля:

Зачет 1 семестр

СОДЕРЖАНИЕ РАБОЧЕЙ ПРОГРАММЫ

дисциплины Спецсеминар "Искусственный интеллект в кибербезопасности" на 2 семестр

очная форма обучения

Вид работы	Объем дисциплины
Общая трудоемкость дисциплины (з.е. / часов)	1/36
Учебных часов на контактную работу с преподавателем:	
лекций	
практических/ семинарских	
лабораторных	32
других (групповая, индивидуальная консультация и иные виды учебной деятельности, предусматривающие работу обучающихся с преподавателем) (ФКР)	0,2
Учебных часов на самостоятельную работу обучающихся (СР)	3,8
Учебных часов на подготовку к экзамену/зачету/дифференцированному зачету (Контроль)	

Форма(ы) контроля:

Зачет 2 семестр

№	Тема и содержание	Форма изучения материалов: лекции, практические занятия, семинарские занятия, лабораторные работы, самостоятельная работа и трудоемкость (в часах)				Задания по самостоятельной работе студентов	Форма текущего контроля успеваемости (коллоквиумы, контрольные работы, компьютерные тесты и т.п.)
		ЛК	ПР/СЕМ	ЛР	СР		
1	2	3	4	5	6	8	9
1.	Искусственный интеллект в кибербезопасности.			4		Проработка лекционного материала, литературных источников.	Групповой и индивидуальный опрос, лабораторные работы
2.	Основные методы использования ИИ для обеспечения надежности, устойчивости и реагирования системы.			4	0,2	Проработка лекционного материала, литературных источников.	Групповой и индивидуальный опрос, лабораторные работы
3.	Злоумышленное использование ИИ. Внедрение новых угроз.			4		Проработка лекционного материала, литературных источников.	Групповой и индивидуальный опрос, лабораторные работы
4.	Изменения типичного характера угроз и новые формы уязвимостей в системах ИИ			6		Проработка лекционного материала, литературных источников.	Групповой и индивидуальный опрос, лабораторные работы
5.	Этические нормы, связанные с ИИ в кибербезопасности			4		Проработка лекционного материала, литературных источников.	Групповой и индивидуальный опрос, лабораторные работы
6.	Асимметрия во взаимодействии ИИ и кибербезопасности. Асимметрия в разработке этических стандартов ИИ			4		Проработка лекционного материала, литературных источников.	Групповой и индивидуальный опрос, лабораторные работы
7.	Риски кибербезопасности, связанные с антропоморфным ИИ			6	0,2	Проработка лекционного материала, литературных источников.	Групповой и индивидуальный опрос, лабораторные работы
8.	Кибербезопасность для Искусственного Интеллекта			6		Проработка лекционного материала, литературных источников.	Групповой и индивидуальный опрос, лабораторные работы
9.	Системы машинного обучения			4		Проработка лекционного материала, литературных источников.	Групповой и индивидуальный опрос, лабораторные работы
10.	Роль операторов			4		Проработка лекционного материала, литературных источников.	Групповой и индивидуальный опрос, лабораторные работы

11.	Безопасность и защищенность открытой, автономной ИТ-инфраструктуры на основе ИИ и ее эволюция во время выполнения			4		Проработка лекционного материала, литературных источников.	Групповой и индивидуальный опрос, лабораторные работы
12.	Решение проблемы незащищенности сети в связи с ИИ			4		Проработка лекционного материала, литературных источников.	Групповой и индивидуальный опрос, лабораторные работы
13.	Пример безопасного жизненного цикла разработки систем ИИ			6		Проработка лекционного материала, литературных источников.	Групповой и индивидуальный опрос, лабораторные работы
14.	Существующие правовые рамки: кибербезопасность РФ и ЕС			4	0,2	Проработка лекционного материала, литературных источников.	Групповой и индивидуальный опрос, лабораторные работы
	ИТОГО			64	0,4		