



МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ РОССИЙСКОЙ ФЕДЕРАЦИИ
Федеральное государственное бюджетное образовательное
учреждение высшего образования
«КАЗАНСКИЙ ГОСУДАРСТВЕННЫЙ ЭНЕРГЕТИЧЕСКИЙ УНИВЕРСИТЕТ»
(ФГБОУ ВО «КГЭУ»)



УТВЕРЖДАЮ

Директор института цифровых
технологий и экономики

Ю.В. Торкунова

«24» ноября 2021 г.

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ

ИСКУССТВЕННЫЙ ИНТЕЛЛЕКТ ДЛЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

Направление подготовки	09.04.01 Информатика и вычислительная техника
Направленность (профиль)	Инженерия искусственного интеллекта
Квалификация	Магистр
Форма обучения	Очная

Перечень сведений о рабочей программе	Учетные данные
Образовательная программа Инженерия искусственного интеллекта	Код ОП 09.04.01
Направление подготовки Информатика и вычислительная техника	Код направления и уровня подготовки 09.04.01

Программа составлена автором:

Программа модуля составлена авторами:

№ п/п	Фамилия Имя Отчество	Ученая степень, ученое звание	Должность	Подразделение
	Созыкин Андрей Владимиро вич	Кандидат технических наук	Доцент	Кафедра информационных технологий и систем управления, ИРИТ-РТФ, УрФУ

Программа оформлена в соответствии с ПОЛОЖЕНИЕМ О ПОРЯДКЕ РАЗРАБОТКИ И УТВЕРЖДЕНИЯ ОБРАЗОВАТЕЛЬНЫХ ПРОГРАММ – ПРОГРАММ БАКАЛАВРИАТА, ПРОГРАММ СПЕЦИАЛИТЕТА И ПРОГРАММ МАГИСТРАТУРЫ В КГЭУ

Рекомендовано учебно-методическим советом Института цифровых технологий и экономики ФГБОУ ВО «КГЭУ»

Протокол № 4 от 24.11.2021 г.

1. Цель, задачи и планируемые результаты обучения по дисциплине

Целью освоения дисциплины является изучение способов использования искусственного интеллекта в области обеспечения информационной безопасности. В рамках курса студенты сделают выводы о потенциале использования технологий искусственного интеллекта для предотвращения несанкционированного доступа к информации, а также уменьшения последствий при нарушении информационной безопасности.

Задачами освоения дисциплины являются:

- ознакомление студентов с основами компьютерной безопасности;
- освоение способов применения машинного обучения для задач информационной безопасности;
- формирование умений по созданию приложений искусственного интеллекта для информационной безопасности.

Компетенции, формируемые у обучающихся, запланированные результаты обучения по дисциплине, соотнесенные с индикаторами достижения компетенций:

Код и наименование компетенции	Индикаторы достижения компетенции	Планируемые результаты обучения
Профессиональные компетенции (ПК)		
ПК-8. Способен разрабатывать и модернизировать программное и аппаратное обеспечение технологий и систем искусственного интеллекта с учетом требований информационной безопасности в различных предметных областях	ПК-8.1. Разрабатывает программное и аппаратное обеспечение технологий и систем искусственного интеллекта для решения профессиональных задач с учетом требований информационной безопасности в различных предметных областях	ПК-8.1. 3-1. Знает новые научные принципы и методы разработки программного и аппаратного обеспечения технологий и систем искусственного интеллекта для решения профессиональных задач в различных предметных областях ПК-8.1. У-1. Умеет разрабатывать программное аппаратное обеспечение технологий и систем искусственного интеллекта с учетом требований информационной безопасности для решения профессиональных задач в различных предметных областях
	ПК-8.2 Модернизирует программное и аппаратное обеспечение технологий и систем искусственного интеллекта для решения профессиональных задач с учетом требований информационной безопасности в различных предметных областях	ПК-8.2. 3-1. Знает особенности модернизации программного технологий и систем искусственного интеллекта для решения профессиональных задач в различных предметных областях ПК-8.2. У-1. Умеет модернизировать программное и аппаратное обеспечение технологий и систем искусственного интеллекта с учетом требований информационной безопасности для решения профессиональных задач в различных предметных областях

2. Место дисциплины в структуре ОПОП

Дисциплина Искусственный интеллект для информационной безопасности относится к части учебного плана по направлению подготовки 09.04.03 Прикладная информатика, формируемой участниками образовательных отношений

Код компетенции	Предшествующие дисциплины (модули), практики, НИР, др.	Последующие дисциплины (модули), практики, НИР, др.
УК-7	Операционная система Linux Программирование на Python Математические основы искусственного интеллекта	Выполнение и защита выпускной квалификационной работы

Для освоения дисциплины обучающийся должен:

Знать:

1. основы математики, физики, вычислительной техники и программирования
2. современные информационные технологии и программные средства, в том числе отечественного производства при решении задач профессиональной деятельности
3. алгоритмические языки программирования, операционные системы и оболочки, современные среды разработки программного обеспечения

Уметь:

1. решать стандартные профессиональные задачи с применением естественнонаучных и инженерных знаний, методов математического анализа и моделирования
2. выбирать современные информационные технологии и программные средства, в том числе отечественного производства при решении задач профессиональной деятельности
3. составлять алгоритмы, писать и отлаживать коды на языке программирования, тестировать работоспособность программы, интегрировать программные модули

Владеть:

1. навыками применения современных информационных технологий и программных средств при решении задач профессиональной деятельности

3. Структура и содержание дисциплины

3.1. Структура дисциплины

Общая трудоемкость дисциплины составляет 3 зачетных(ые) единиц(ы) (ЗЕ), всего 108 часов, из которых 26 часов составляет контактная работа обучающегося с преподавателем (занятия лекционного типа 8 час., занятия семинарского типа (практические, семинарские занятия, лабораторные работы и т.п.) 16 час., самостоятельная работа обучающегося 82 час.

Вид учебной работы	Всего часов	Семестр
		3
ОБЩАЯ ТРУДОЕМКОСТЬ ДИСЦИПЛИНЫ	108	108
КОНТАКТНАЯ РАБОТА ОБУЧАЮЩЕГОСЯ С ПРЕПОДАВАТЕЛЕМ, в том числе:	26	26
Лекционные занятия (Лек)	8	8
Практические занятия (Пр)	16	16
Контроль самостоятельной работы и иная контактная работа (КСР)*	2	2
САМОСТОЯТЕЛЬНАЯ РАБОТА ОБУЧАЮЩЕГОСЯ	82	82
ФОРМА ПРОМЕЖУТОЧНОЙ АТТЕСТАЦИИ (3 – зачет)	3	3

3.2. Содержание дисциплины, структурированное по разделам и видам занятий

Разделы дисциплины	Семестр	Распределение трудоемкости (в часах) по видам учебной работы, включая СРС									Формируемые результаты обучения (знания, умения, навыки)	Литература	Формы текущего контроля успеваемости	Формы промежуточной аттестации	Максимальное количество баллов по балльно - рейтинговой системе								
		Занятия лекционного типа	Занятия практического / семинарского типа	Лабораторные работы	Групповые консультации	Самостоятельная работа студента, в т.ч.	Контроль самостоятельной работы (КСР)	Контактные часы во время аттестации (КПА)	подготовка к промежуточной аттестации	Сдача зачета / экзамена						Итого							
		Раздел 1. Основы компьютерной безопасности																					
		1. Типы атак в информационной безопасности. Криптография. Хэш-функции.	3	2				6										8	ПК-8.1.3-1	4	ДР	3	3

2. Безопасность компьютерных сетей и сетевых протоколов. Безопасность в ОС Linux. Инъекции. Бинарные уязвимости	3					6					6	ПК-8.1.3-1	4	ДР	3	3
Раздел 2. Применение машинного обучения для задач информационной безопасности																
Определение спама. Классификация сетевых атак. Определение распределенной сетевой атаки “отказ в обслуживании”.	3	2	2			8					12	ПК-8.1.3-1, ПК-8.1.У-1	1,2,3,4	ДР	3	6
Определение злонамеренных (malicious) сайтов.	3		2			6					8	ПК-8.1.3-1, ПК-8.1.У-1	1,2,3,4	ДР	3	6
Определение инъекций.	3		2			6					8	ПК-8.1.3-1, ПК-8.1.У-1	1,2,3,4	КР	3	8
Поиск злонамеренного программного обеспечения (malware).	3		2			6					8	ПК-8.1.3-1, ПК-8.1.У-1	1,2,3,4	КР	3	8
Анализ аномалий в активности пользователей.	3	2	2			10					14	ПК-8.1.3-1, ПК-8.1.У-1	1,2,3,4	КР	3	8
Раздел 3. Проекты искусственного интеллекта в области информационной безопасности																
Жизненный цикл проекта создания приложений искусственного интеллекта для информационной безопасности.	3					6					6	ПК-8.1.3-1, ПК-8.1.У-1	1,2,3,4	ДР	3	2

Подготовка набора данных в информационной безопасности	3	2	2			8					12	ПК-8.1.3-1, ПК-8.1.У-1	1,2,3,4	ДР	3	4
Выбор модели и ее обучение. Оценка качества модели	3		2			8					10	ПК-8.1.3-1, ПК-8.1.У-1	1,2,3,4	КР	3	4
Разработка приложения, использующего модель. Внедрение приложения в практическое	3		2			12					14	ПК-8.1.3-1, ПК-8.1.У-1	1,2,3,4	КР	3	8
Промежуточная аттестация																
Зачет	3														3	
ИТОГО		8	16			82	2				108					

3.3. Тематический план лекционных занятий

Номер раздела дисциплины	Темы лекционных занятий	Трудоемкость, час.
1	Типы атак в информационной безопасности Криптография. Хэш-функции.	2
1	Безопасность компьютерных сетей и сетевых протоколов. Безопасность в ОС Linux. Инъекции. Бинарные уязвимости	2
2	Определение спама. Классификация сетевых атак. Определение распределенной сетевой атаки “отказ в обслуживании”.	2
2	Виды аномалий в активности пользователей	2
3	Подготовка набора данных, связанных с нарушением безопасности информации	2
Всего		8

3.4. Тематический план практических занятий

Номер раздела дисциплины	Темы практических занятий	Трудоемкость, час.
2	Определение распределенной сетевой атаки “отказ в обслуживании”.	2
2	Определение злонамеренных (malicious) сайтов	2
2	Определение инъекций	2
2	Поиск злонамеренного программного обеспечения (malware).	2
2	Анализ аномалий в активности пользователей	2
3	Подготовка набора данных в информационной безопасности	2
3	Выбор модели и ее обучение. Оценка качества модели	2
3	Разработка приложения, использующего модель. Внедрение приложения в практическое использование.	2
Всего		16

3.5. Тематический план лабораторных работ

Лабораторные работы не предусмотрены

3.6. Самостоятельная работа студента

Номер раздела дисциплины	Вид СРС	Содержание СРС	Трудоемкость, час.
1	Закрепление лекционного материала	Типы атак в информационной безопасности Криптография. Хэш-функции.	6

1	Закрепление лекционного материала	Безопасность компьютерных сетей и сетевых протоколов. Безопасность в ОС Linux. Инъекции. Бинарные уязвимости	6
2	Закрепление лекционного материала, подготовка к практическому занятию	Классификация сетевых атак.	8
2	Закрепление лекционного материала, подготовка к практическому занятию	Особенности злонамеренных (malicious) сайтов.	6
2	Закрепление лекционного материала, подготовка к практическому занятию	SQL-инъекции	6
2	Закрепление лекционного материала, подготовка к практическому занятию	Классификация злонамеренного программного обеспечения (malware).	6
2	Закрепление лекционного материала, подготовка к практическому занятию	Виды аномалий в активности пользователей	10
3	Закрепление лекционного материала	Жизненный цикл проекта создания приложений искусственного интеллекта для информационной безопасности.	6
3	Подготовка к практическому занятию	Подготовка набора данных, связанных с нарушением безопасности информации	8
3	Подготовка к практическому занятию	Выбор модели и ее обучение. Оценка качества модели	8
3	Подготовка к практическому занятию	Разработка приложения, использующего модель. Внедрение приложения в практическое использование.	12
Всего			82

4. Образовательные технологии

При проведении учебных занятий используются традиционные образовательные технологии (лекции в сочетании с практическими занятиями и лабораторными работами, самостоятельное изучение определённых разделов) и современные образовательные технологии, направленные на обеспечение развития у обучающихся навыков командной работы, межличностной коммуникации, принятия решений, лидерских качеств интерактивные лекции, работа в команде, индивидуальное обучение, междисциплинарное обучение.

5. Оценивание результатов обучения

Оценивание результатов обучения по дисциплине осуществляется в рамках текущего контроля успеваемости, проводимого по балльно-рейтинговой системе (БРС), и промежуточной аттестации.

Обобщенные критерии и шкала оценивания уровня сформированности компетенции (индикатора достижения компетенции) по итогам освоения дисциплины:

Планируемые результаты обучения	Обобщенные критерии и шкала оценивания результатов обучения			
	неудовлетворительно	удовлетворительно	хорошо	отлично
	не зачтено	зачтено		
Полнота знаний	Уровень знаний ниже минимальных требований, имеют место грубые ошибки	Минимально допустимый уровень знаний, имеет место много негрубых ошибок	Уровень знаний в объеме, соответствующем программе, имеет место несколько негрубых ошибок	Уровень знаний в объеме, соответствующем программе подготовки, без ошибок
Наличие умений	При решении стандартных задач не продемонстрированы основные умения, имеют место грубые ошибки	Продemonстрированы основные умения, решены типовые задачи с негрубыми ошибками, выполнены все задания, но не в полном объеме	Продemonстрированы все основные умения, решены все основные задачи с негрубыми ошибками, выполнены все задания в полном объеме, но некоторые с недочетами	Продemonстрированы все основные умения, решены все основные задачи с отдельными незначительными недочетами, выполнены все задания в полном объеме
Наличие навыков (владение)	При решении стандартных задач не продемонстрированы	Имеется минимальный набор навыков для решения	Продemonстрированы базовые навыки при решении стандартных задач с	Продemonстрированы навыки при решении нестандартных задач

опытом)	базовые навыки, имеют место грубые ошибки	стандартных задач с некоторыми недочетами	некоторыми недочетами	без ошибок и недочетов
Характеристика сформированности компетенции (индикатора достижения компетенции)	Компетенция в полной мере не сформирована. Имеющихся знаний, умений, навыков недостаточно для решения практических (профессиональных) задач	Сформированность компетенции соответствует минимальным требованиям. Имеющихся знаний, умений, навыков в целом достаточно для решения практических (профессиональных) задач, но требуется дополнительная практика по большинству практических задач	Сформированность компетенции в целом соответствует требованиям. Имеющихся знаний, умений, навыков и мотивации в целом достаточно для решения стандартных практических (профессиональных) задач	Сформированность компетенции полностью соответствует требованиям. Имеющихся знаний, умений, навыков и мотивации в полной мере достаточно для решения сложных практических (профессиональных) задач
Уровень сформированности компетенции (индикатора достижения компетенции)	Низкий	Ниже среднего	Средний	Высокий

Шкала оценки результатов обучения по дисциплине:

Код компетенции	Код индикатора достижения компетенции	Запланированные результаты обучения по дисциплине	Уровень сформированности компетенции (индикатора достижения компетенции)			
			Высокий	Средний	Ниже среднего	Низкий
			Шкала оценивания			
			отлично	хорошо	удовлетворительно	неудовлетворительно
			зачтено			не зачтено
		Знать				

		новые научные принципы и методы разработки программного и аппаратного обеспечения технологий и систем искусственного интеллекта для решения профессиональных задач в различных предметных областях	Уровень знаний в объеме, соответствующем программе подготовки, без ошибок	Уровень знаний в объеме, соответствующем программе, имеет место несколько негрубых ошибок	Минимально допустимый уровень знаний, имеет место много негрубых ошибок	Уровень знаний ниже минимальных требований, имеют место грубые ошибки
ПК-11	ПК-11.1	Уметь				
		разрабатывать программное аппаратное обеспечение технологий и систем искусственного интеллекта с учетом требований информационной безопасности для решения профессиональных задач в различных предметных областях	Продемонстрированы все основные умения, решены все основные задачи с отдельными несущественными недочетами, выполнены все задания в полном объеме	Продемонстрированы все основные умения, решены все основные задачи с негрубыми ошибками, выполнены все задания в полном объеме, но некоторые с недочетами	Продемонстрированы основные умения, решены типовые задачи с негрубыми ошибками, выполнены все задания, но не в полном объеме	При решении стандартных задач не продемонстрированы основные умения, имеют место грубые ошибки

Оценочные материалы для проведения текущего контроля успеваемости и промежуточной аттестации приведены в Приложении к рабочей программе дисциплины. Полный комплект заданий и материалов, необходимых для оценивания результатов обучения по дисциплине, хранится на кафедре-разработчике в бумажном и электронном

6. Учебно-методическое и информационное обеспечение дисциплины

6.1. Учебно-методическое обеспечение

Основная литература

№ п/п	Автор(ы)	Наименование	Вид издания (учебник, учебное пособие,	Место издания, издательство	Год издания	Адрес электронного ресурса	Кол-во экземпляров в библиотеке КГЭУ
1	Чесалин А. Н.	Основы искусственного интеллекта с приложениями в информационной безопасности	учебное пособие	Москва: РТУ МИРЭА	2021	URL: https://e.lanbook.com/book/182429 (дата обращения: 21.12.2021). — Режим доступа: для авториз. пользователей	Текст: электронный
2	Чесалин А. Н.	Основы искусственного интеллекта с приложениями в информационной безопасности. Практикум	учебное пособие	Москва: РТУ МИРЭА	2020	URL: https://e.lanbook.com/book/163838 (дата обращения: 21.12.2021) — Режим доступа: для авториз. пользователей	Текст: электронный

Дополнительная литература

№ п/п	Автор(ы)	Наименование	Вид издания (учебник, учебное пособие,	Место издания, издательство	Год издания	Адрес электронного ресурса	Кол-во экземпляров в библиотеке КГЭУ
3	Остроух А. В.	Системы искусственного интеллекта	монография	Санкт-Петербург : Лань, 2021	2021	URL: https://e.lanbook.com/book/176662 (дата обращения: 21.12.2021). — Режим доступа: для авториз. пользователей	Текст: электронный
4	Н. А. Руденков, А. В. Пролетарский, Е. В. Смирнова, А. М. Суровов	Технологии защиты информации в компьютерных сетях	учебное пособие	Москва : ИНТУИТ	2016	URL: https://e.lanbook.com/book/100522 (дата обращения: 21.12.2021). — Режим доступа: для авториз. пользователей.	Текст: электронный

6.2. Информационное обеспечение

6.2.1. Электронные и интернет-ресурсы

№ п/п	Наименование электронных и интернет-ресурсов	Ссылка
	Онлайн-курс “Основы компьютерной безопасности”. URL: https://ulearn.me/Course/Hackerdom/ (дата обращения: 05.10.2021).	https://ulearn.me/Course/Hackerdom/ (дата обращения: 05.10.2021)
	Cyber Data Science	https://cyberdatascientist.com/ (дата обращения: 05.10.2021)
	Sarker, I.H., Kayes, A.S.M., Badsha, S. et al. Cybersecurity data science: an overview from machine learning perspective. J Big Data 7, 41 (2020).	https://doi.org/10.1186/s40537-020-00318-5 (дата обращения: 05.10.2021).
	A summary of cybersecurity datasets highlighting diverse attack-types and machine learning-based usage in different cyber applications.	https://journalofbigdata.springeropen.com/articles/10.1186/s40537-020-00318-5/tables/2 (дата обращения: 05.10.2021).
	CS 259D Data Mining for Cyber Security	https://web.stanford.edu/class/cs259d/ (дата обращения: 05.10.2021)
	Awesome Machine Learning for Cyber Security	https://github.com/jivoi/awesome-ml-for-cybersecurity (дата обращения: 05.10.2021)
	Machine Learning for Security	https://security.kiwi/docs/introduction/ (дата обращения: 05.10.2021)
	Clarence Chio, David Freeman. Machine Learning and Security: Protecting Systems with Data and Algorithms book repository	https://github.com/oreilly-mlsec/book-resources (дата обращения: 05.10.2021)
1	Научная электронная библиотека	https://elibrary.ru
4	Международная реферативная база данных научных изданий Springerlink	http:// link.springer.com

6.2.2. Профессиональные базы данных

№ п/п	Наименование профессиональных баз данных	Адрес	Режим доступа
	Applied Science & Technology Source. EBSCO publishing	http://search.ebscohost.com	http://search.ebscohost.com
	Wiley Online Library	http://onlinelibrary.wiley.com/	http://onlinelibrary.wiley.com/
	Гугл Академия	https://scholar.google.ru	https://scholar.google.ru

6.2.3. Информационно-справочные системы

№ п/п	Наименование информационно-справочных систем	Адрес	Режим доступа
1	Applied Science & Technology Source. EBSCO publishing	http://search.ebscohost.com	http://search.ebscohost.com
2	Wiley Online Library	http://onlinelibrary.wiley.com/	http://onlinelibrary.wiley.com/
3	Гугл Академия	https://scholar.google.ru/	https://scholar.google.ru/

6.2.4. Лицензионное и свободно распространяемое программное обеспечение дисциплины

№ п/п	Наименование программного обеспечения	Описание	Реквизиты подтверждающих документов
1	Браузер Chrome	Система поиска информации в сети интернет (включая русскоязычный интернет).	https://www.google.com/intl/ru/chrome/
2	Office Standard 2007 Russian OLP NL AcademicEdition+:	Офисные приложения	договор №21/2010 от 04.05.2010, лицензиар - ЗАО «Софт Лайн Трейд»,
3	LMS Moodle	Это современное программное обеспечение	https://download.moodle.org/releases/latest/
4	Windows Профессиональная (Pro)	Пользовательская операционная система	№2011.25486 от 28.11.2011
	Python	Бесплатно-распространяемое программное обеспечение	https://www.python.org/
	TensorFlow	Бесплатно-распространяемое программное обеспечение	https://www.tensorflow.org/
	Веб-среда разработки для языка программирования Python: google colab	Бесплатно-распространяемое программное обеспечение	https://colab.research.google.com/
	WireShark –	Бесплатно-распространяемое программное обеспечение	https://www.wireshark.org/
	Suricata	Бесплатно-распространяемое программное обеспечение	https://suricata.io/

7. Материально-техническое обеспечение дисциплины

№ п/п	Вид учебной работы	Наименование специальных помещений и помещений для СРС	Оснащенность специальных помещений и помещений для СРС

1	Лекционные занятия	Учебная аудитория для проведения занятий лекционного типа	Помещение В-608 для проведения занятий лекционного, семинарского типа, групповых и индивидуальных консультаций, текущего контроля и промежуточной аттестации Оснащение: персональный компьютер (26 шт.), интерактивная доска, мультимедийный проектор. Программное обеспечение: 1. Windows 7 Профессиональная (Pro): договор №2011.25486 от 28.11.2011, лицензиар – ЗАО «Софт Лайн Трейд», тип (вид) лицензии – неискл. право, срок действия лицензии - бессрочно. 2. Office Standard 2007 Russian OLP NL AcademicEdition+: договор №21/2010 от 04.05.2010, лицензиар - ЗАО «Софт Лайн Трейд», тип (вид) лицензии - неискл. право, срок действия лицензии - бессрочно 3. Браузер Chrome. свободная лицензия, тип (вид) лицензии – неискл. право, срок действия лицензии – бессрочно 4.LMS Moodle. Свободная лицензия, тип (вид) лицензии - неискл. право, срок действия лицензии - бессрочно. ПО в свободном доступе: Visual Studio 2019 Community Свободная лицензия, тип (вид) лицензии - неискл. право,
2	Самостоятельная работа обучающегося	Компьютерный класс для самостоятельной работы В-600а	Оснащение: моноблок (30 шт.), проектор, экран Программное обеспечение: Windows 10: договор № Tr096148 от 29.09.2020, лицензиар - ООО "Софтлайн трейд", тип (вид) лицензии - неискл. право, срок действия лицензии - до 14.09.2021. Office Standard 2007 Russian OLP NL AcademicEdition+: договор №21/2010 от 04.05.2010, лицензиар - ЗАО «Софт Лайн Трейд», тип (вид) лицензии - неискл. право, срок действия лицензии – бессрочно; Браузер Chrome, свободная лицензия, тип (вид) лицензии – неискл.право, срок действия лицензии – бессрочно; LMS Moodle, свободная лицензия, тип (вид) лицензии – неискл.право, срок действия лицензии - бессрочно.

3	Практические занятия	Компьютерный класс с выходом в Интернет	Помещение В-621 для проведения занятий семинарского типа, групповых и индивидуальных консультаций, текущего контроля и промежуточной аттестации Оснащение: Персональный компьютер (15 шт.), доска ученическая. Программное обеспечение: 1. Windows 7 Профессиональная (Pro): договор №2011.25486 от 28.11.2011, лицензиар – ЗАО «Софт Лайн Трейд», тип (вид) лицензии – неискл. право, срок действия лицензии - бессрочно. 2. Office Standard 2007 Russian OLP NL AcademicEdition+: договор №21/2010 от 04.05.2010, лицензиар - ЗАО «Софт Лайн Трейд», тип (вид) лицензии - неискл. право, срок действия лицензии - бессрочно 3. Браузер Chrome . свободная лицензия, тип (вид) лицензии – неискл. право, срок действия лицензии - бессрочно LMS Moodle. Свободная лицензия, тип (вид) лицензии - неискл. право, срок действия лицензии - бессрочно. ПО в свободном доступе: Visual Studio 2019 Community, IntelliJ IDEA Community Edition 2019, Python 3.7, PyCharm Community, Sublime Text 3, Denwer, Microsoft SQL Server Tools 18, MySQL WorkBench 8.0 CE, Android Studio, 1C:Предприятие Учебная версия, Arduino, Cisco Packet Tracer, Aris Express, ГИС Zulu 8.0 Инженерные расчеты, Oracle VM Virtual Box. Свободная лицензия, тип (вид) лицензии - неискл. право, срок действия лицензии - бессрочно.
4	Лабораторные работы	Компьютерный класс с выходом в Интернет	Помещение В-621 для проведения занятий семинарского типа, групповых и индивидуальных консультаций, текущего контроля и промежуточной аттестации Оснащение: Персональный компьютер (15 шт.),доска ученическая. Программное обеспечение: 1. Windows 7 Профессиональная (Pro): договор №2011.25486 от 28.11.2011, лицензиар – ЗАО «Софт Лайн Трейд», тип (вид) лицензии – неискл. право, срок действия лицензии - бессрочно. 2. Office Standard 2007 Russian OLP NL AcademicEdition+: договор №21/2010 от 04.05.2010, лицензиар - ЗАО «Софт Лайн Трейд», тип (вид) лицензии - неискл. право, срок действия лицензии - бессрочно 3. Браузер Chrome . свободная лицензия, тип (вид) лицензии – неискл. право, срок действия лицензии - бессрочно LMS Moodle. Свободная лицензия, тип (вид) лицензии - неискл. право, срок действия лицензии - бессрочно. ПО в свободном доступе: Visual Studio 2019 Community, IntelliJ IDEA Community Edition 2019, Python 3.7, PyCharm Community, Sublime Text 3, Denwer, Microsoft SQL Server Tools 18, MySQL WorkBench 8.0 CE, Android Studio, 1C:Предприятие Учебная версия, Arduino, Cisco Packet Tracer, Aris Express, ГИС Zulu 8.0 Инженерные расчеты, Oracle VM Virtual Box. Свободная лицензия, тип (вид) лицензии - неискл. право, срок действия лицензии - бессрочно.

5	Промежуточная аттестация	Учебная аудитория для проведения промежуточной аттестации	Оснащение: Персональный компьютер (15 шт.), доска ученическая. Программное обеспечение: 1. Windows 7 Профессиональная (Pro): договор №2011.25486 от 28.11.2011 , лицензиар – ЗАО «Софт Лайн Трейд», тип (вид) лицензии – неискл. право, срок действия лицензии - бессрочно. 2. Office Standard 2007 Russian OLP NL AcademicEdition+: договор №21/2010 от 04.05.2010, лицензиар - ЗАО «Софт Лайн Трейд», тип (вид) лицензии - неискл. право, срок действия лицензии - бессрочно 3. Браузер Chrome . свободная лицензия, тип (вид) лицензии – неискл. право, срок действия лицензии - бессрочно LMS Moodle. Свободная лицензия, тип (вид) лицензии - неискл. право, срок действия лицензии - бессрочно. ПО в свободном доступе: Visual Studio 2019 Community
---	--------------------------	---	--

8. Особенности организации образовательной деятельности для лиц с ограниченными возможностями здоровья и инвалидов

Лица с ограниченными возможностями здоровья (ОВЗ) и инвалиды имеют возможность беспрепятственно перемещаться из одного учебно-лабораторного корпуса в другой, подняться на все этажи учебно-лабораторных корпусов, заниматься в учебных и иных помещениях с учетом особенностей психофизического развития и состояния здоровья.

Для обучения лиц с ОВЗ и инвалидов, имеющих нарушения опорно-двигательного аппарата, обеспечены условия беспрепятственного доступа во все учебные помещения. Информация о специальных условиях, созданных для обучающихся с ОВЗ и инвалидов, размещена на сайте университета [www//kgeu.ru](http://kgeu.ru). Имеется возможность оказания технической помощи ассистентом, а также услуг сурдопереводчиков и тифлосурдопереводчиков.

Для адаптации к восприятию лицами с ОВЗ и инвалидами с нарушенным слухом справочного, учебного материала по дисциплине обеспечиваются следующие условия:

- для лучшей ориентации в аудитории, применяются сигналы оповещения о начале и конце занятия (слово «звонок» пишется на доске);
- внимание слабослышащего обучающегося привлекается педагогом жестом (на плечо кладется рука, осуществляется нерезкое похлопывание);
- разговаривая с обучающимся, педагогический работник смотрит на него, говорит ясно, короткими предложениями, обеспечивая возможность чтения по губам.

Компенсация затруднений речевого и интеллектуального развития слабослышащих обучающихся проводится путем:

- использования схем, диаграмм, рисунков, компьютерных презентаций с гиперссылками, комментирующими отдельные компоненты изображения;
- регулярного применения упражнений на графическое выделение существенных признаков предметов и явлений;
- обеспечения возможности для обучающегося получить адресную консультацию по электронной почте по мере необходимости.

Для адаптации к восприятию лицами с ОВЗ и инвалидами с нарушениями зрения справочного, учебного, просветительского материала, предусмотренного образовательной программой по выбранному направлению подготовки, обеспечиваются следующие условия:

- ведется адаптация официального сайта в сети Интернет с учетом особых потребностей инвалидов по зрению, обеспечивается наличие крупношрифтовой справочной информации о расписании учебных занятий;
- педагогический работник, его собеседник (при необходимости), присутствующие на занятии, представляются обучающимся, при этом каждый раз называется тот, к кому педагогический работник обращается;
- действия, жесты, перемещения педагогического работника коротко и ясно комментируются;
- печатная информация предоставляется крупным шрифтом (от 18 пунктов), тотально озвучивается;
- обеспечивается необходимый уровень освещенности помещений;
- предоставляется возможность использовать компьютеры во время занятий и право записи объяснений на диктофон (по желанию обучающихся).

Форма проведения текущей и промежуточной аттестации для обучающихся с ОВЗ и инвалидов определяется педагогическим работником в соответствии с учебным планом. При необходимости обучающемуся с ОВЗ, инвалиду с учетом их индивидуальных психофизических особенностей дается возможность пройти промежуточную аттестацию устно, письменно на бумаге, письменно на компьютере, в форме тестирования и т.п., либо предоставляется дополнительное время для подготовки ответа.



КГУУ

МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ РОССИЙСКОЙ ФЕДЕРАЦИИ
Федеральное государственное бюджетное образовательное учреждение
высшего образования
«КАЗАНСКИЙ ГОСУДАРСТВЕННЫЙ ЭНЕРГЕТИЧЕСКИЙ УНИВЕРСИТЕТ»
(ФГБОУ ВО «КГУУ»)

ОЦЕНОЧНЫЕ МАТЕРИАЛЫ

**для проведения текущего контроля успеваемости и промежуточной аттестации
студентов по итогам освоения дисциплины**

Искусственный интеллект для информационной безопасности

Направление подготовки 09.04.01 Информатика и вычислительная техника

Направленность (профиль) Инженерия искусственного интеллекта

Квалификация Магистр

Форма обучения Очная

№ п/п	Фамилия Имя Отчество	Ученая степень, ученое звание	Должность	Подразделение
1	Созыкин Андрей Влаимирович	кандидат технических наук	доцент	Кафедра информационных технологий и систем управления, ИРИТ-РТФ, УрФУ

Оценочные материалы оформлены в соответствии с ПОЛОЖЕНИЕМ О ПОРЯДКЕ РАЗРАБОТКИ И УТВЕРЖДЕНИЯ ОБРАЗОВАТЕЛЬНЫХ ПРОГРАММ – ПРОГРАММ БАКАЛАВРИАТА, ПРОГРАММ СПЕЦИАЛИТЕТА И ПРОГРАММ МАГИСТРАТУРЫ В КГУУ

Оценочные материалы по дисциплине «Искусственный интеллект для информационной безопасности» - комплект контрольно-измерительных материалов, предназначенных для оценивания результатов обучения на соответствие индикаторам достижения компетенции(й):

ПК-8.1. Разрабатывает программное и аппаратное обеспечение технологий и систем искусственного интеллекта для решения профессиональных задач с учетом требований информационной безопасности в различных предметных областях

ПК-8.2 Модернизирует программное и аппаратное обеспечение технологий и систем искусственного интеллекта для решения профессиональных задач с учетом требований информационной безопасности в различных предметных областях

Оценивание результатов обучения по дисциплине осуществляется в рамках текущего контроля успеваемости, проводимого по балльно-рейтинговой системе (БРС), и промежуточной аттестации.

Текущий контроль успеваемости обеспечивает оценивание процесса обучения по дисциплине. При текущем контроле успеваемости используются следующие оценочные средства: подготовка доклада с презентацией, отчет по практической работе, тест, зачет.

Промежуточная аттестация имеет целью определить уровень достижения запланированных результатов обучения по дисциплине за 3 семестр. Форма промежуточной аттестации зачёт.

Оценочные материалы включают задания для проведения текущего контроля успеваемости и промежуточной аттестации обучающихся, разработанные в соответствии с рабочей программой дисциплины.

1.Технологическая карта

Семестр 3

Номер раздела/ темы дис- циплины	Вид СРС	Наимено- вание оценочного средства	Код индикатора достижения компетенций	Уровень освоения дисциплины, баллы			
				неудов-но	удов-но	хорошо	отлично
				не зачтено	зачтено		
				низкий	ниже среднего	средний	высокий
Текущий контроль успеваемости							
2	Выполнение контрольной работы	КР	ПК-8	менее 3	3 - 5	5 - 8	8 - 10
2	Выполнение контрольной работы	КР	ПК-8	менее 3	3 - 5	5 - 8	8 - 10
2	Выполнение практической работы	ПР	ПК-8	менее 3	3 - 5	5 - 8	8 - 10
2	Выполнение практической работы	ПР	ПК-8	менее 3	3 - 5	5 - 8	8 - 10

2	Выполнение практической работы	ПР	ПК-8	менее 3	3 - 5	5 - 8	8 - 10
3	Выполнение практической работы	ПР	ПК-8	менее 3	3 - 5	5 - 8	8 - 10
3	Выполнение практической работы	ПР	ПК-8	менее 3	3 - 5	5 - 8	8 - 10
3	Выполнение практической работы	ПР	ПК-8	менее 3	3 - 5	5 - 8	8 - 10
3	Выполнение практической работы	ПР	ПК-8	менее 3	3 - 5	5 - 8	8 - 10
3	Выполнение практической работы	ПР	ПК-8	менее 3	3 - 4	5 - 7	8 - 10
Всего баллов				0 - 29	30-49	50-79	80-100

2. Перечень оценочных средств

Краткая характеристика оценочных средств, используемых при текущем контроле успеваемости и промежуточной аттестации обучающегося по дисциплине:

Наименование оценочного средства	Краткая характеристика оценочного средства	Оценочные материалы
Контрольная работа (КР)	Отчет по контрольной работе выполняется индивидуально каждым из студентов согласно Методическим указаниям, выданным на занятии. Отчет загружается в электронном виде в соответствующее задание на курсе в LMS Moodle. Преподаватель после проверки проставляет оценку по шкале "зачтено/не зачтено" с указанием замечаний, при необходимости отправляет отчет на доработку.	Здания к контрольной работе
Отчет по практической работе (ОПР)	Отчет по практической работе выполняется индивидуально каждым из студентов согласно Методическим указаниям, выданным на занятии. Отчет загружается в электронном виде в соответствующее задание на курсе в LMS Moodle. Преподаватель после проверки проставляет оценку по шкале "зачтено/не зачтено" с указанием замечаний, при необходимости отправляет отчет на доработку.	Задание к практической работе
Зачет (З)	Зачет по результатам сдачи работ в течение семестра	Отсутствуют

3. Оценочные материалы текущего контроля успеваемости обучающихся

Наименование оценочного средства	Контрольная работа
Представление и содержание оценочных материалов	Примерная тематика контрольных работ: Модели и типы атак в информационной безопасности. Примерные задания в составе контрольных работ: 1. Атака “отказ в обслуживании”. 2. Атака “распределенный отказ в обслуживании”. 3. Атака “человек посередине”. 4. Атака “SQL-инъекции”. 5. Атака “переполнение буфера”. 6. Неавторизованный доступ. 7. Получение привилегий администратора. 8. Злонамеренное программное обеспечение. 9. Злонамеренные сайты. Примерные задания в составе контрольных работ: 1. Используя набор данных о сетевых атаках KDD Cup 1999 (http://kdd.ics.uci.edu/databases/kddcup99/kddcup99.html) обучите модель машинного обучения находить сетевые атаки и определять их тип. Точность работы модели необходимо измерять на тестовом наборе данных KDD Cup 1999. 2. Создайте и обучите модель машинного обучения для определения злонамеренных сайтов. Для обучения используйте набор данных Malicious and Benign Websites – https://www.kaggle.com/xwolf12/malicious-and-benign-websites
Критерии оценки и шкала оценивания в баллах	Отлично - Результаты обучения (индикаторы) достигнуты в полном объеме, замечаний нет Хорошо - Результаты обучения (индикаторы) в целом достигнуты, имеются замечания, которые не требуют обязательного устранения Удовлетворительно - Результаты обучения (индикаторы) достигнуты не в полной мере, есть замечания Неудовлетворительно - Освоение результатов обучения не соответствует индикаторам, имеются существенные ошибки и замечания, требуется доработка Недостаточно свидетельств для оценивания - Результат обучения не достигнут, задание не выполнено
Наименование оценочного средства	Отчет по практической работе (ОПР)

Представление и содержание оценочных материалов	Задания представлены в методических указаниях к практическим работам. Примерный перечень тем практических занятий: – Основы информационной безопасности. Модели атак. – Злонамеренное программное обеспечение (malware, malicious software) – Анализ сетевого трафика. – Инъекции кода. SQL инъекции. – Определение спама. – Обнаружение и классификация сетевых атак. – Поиск злонамеренного программного обеспечения. – Определение злонамеренных сайтов. – Определение инъекций.
Критерии оценки и шкала оценивания в баллах	Отлично - Результаты обучения (индикаторы) достигнуты в полном объеме, замечаний нет Хорошо - Результаты обучения (индикаторы) в целом достигнуты, имеются замечания, которые не требуют обязательного устранения Удовлетворительно - Результаты обучения (индикаторы) достигнуты не в полной мере, есть замечания Неудовлетворительно - Освоение результатов обучения не соответствует индикаторам, имеются существенные ошибки и замечания, требуется доработка Недостаточно свидетельств для оценивания - Результат обучения не достигнут, задание не выполнено

4. Оценочные материалы промежуточной аттестации

Наименование оценочного средства	Зачет
Представление и содержание оценочных материалов	Отсутствуют
Критерии оценки и шкала оценивания в баллах	Студент, своевременно и качественно выполнивший в течение семестра все практические работы и тесты, набирает проходные 55 баллов и получает оценку «зачтено». В противном случае для добора баллов студент сдает необходимое количество работ и тестов.