Министерство науки и высшего образования Российской Федерации
Федеральное государственное автономное образовательное учреждение
высшего образования
«Уральский федеральный университет имени первого Президента России Б.Н. Ельцина»

УТВЕРЖДАЮ
Директор по образовательной деятельности
_____ С.Т. Князев
«__» _____ 2021 г.

РАБОЧАЯ ПРОГРАММА МОДУЛЯ

Код модуля
М.1.14

Модуль
Искусственный интеллект для информационной безопасности

Екатеринбург, 2021

Перечень сведений о рабочей программе модуля	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

Области образования, в рамках которых реализуется модуль образовательной программы по СУОС УрФУ:

№ п/п	Перечень областей образования, для которых разработан СУОС УрФУ	Уровень подготовки
1.	Инженерное дело, технологии и технические науки	магистратура

Программа модуля составлена авторами:

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

Рекомендовано учебно-методическим советом института радиоэлектроники и информационных технологий - РТФ

Протокол № 7 от 11.10.2021 г.

1. ОБЩАЯ ХАРАКТЕРИСТИКА МОДУЛЯ Искусственный интеллект для информационной безопасности

1.1. Аннотация содержания модуля

Модуль «Искусственный интеллект для информационной безопасности» состоит из одноименной дисциплины. Студенты изучат возможные пути использования искусственного интеллекта в области обеспечения информационной безопасности. В рамках курса сделают выводы о потенциале использования технологий искусственного интеллекта для предотвращения несанкционированного доступа к информации, а также уменьшения последствий при нарушении информационной безопасности.

1.2. Структура и объем модуля

Таблица 1

№ п/п	Перечень дисциплин модуля в последовательности их освоения	Объем дисциплин модуля и всего модуля в зачетных единицах и часах
1.	Искусственный интеллект для информационной безопасности	3 з.е. /108 ч.
	ИТОГО по модулю:	**3 з.е. /108 ч.**

1.3. Последовательность освоения модуля в образовательной программе

Пререквизиты модуля	*отсутствуют*
Постреквизиты и корреквизиты модуля	*отсутствуют*

1.4. Распределение компетенций по дисциплинам модуля, планируемые результаты обучения (индикаторы) по модулю

Таблица 2.1

Перечень дисциплин модуля	Код и наименование компетенции	Планируемые результаты обучения (индикаторы)
1	2	3
Искусственный интеллект для информационной безопасности	УК-7 Способен обрабатывать, анализировать, передавать данные и информацию с использованием цифровых средств для эффективного решения поставленных задач с учетом требований информационной безопасности	УК-7. З-1. Сделать обзор угроз информационной безопасности, основных принципов организации безопасной работы в информационных системах и в сети интернет. УК-7. З-2. Описать способы и средства защиты персональных данных и данных в организации в соответствии с действующим законодательством. УК-7. У-1. Определять основные угрозы безопасности при использовании информационных технологий и выбирать оптимальные способы и средства защиты

		персональных данных и данных организации от мошенников и вредоносного ПО. УК-7. П-1. Обосновать выбор технических и программных средств защиты персональных данных и данных организации при работе с информационными системами на основе анализа потенциальных и реальных угроз безопасности информации. УК-7. П-2. Решать поставленные задачи, используя эффективные цифровые средства и средства информационной безопасности

Таблица 2.2

Перечень дисциплин модуля	**Код и наименование компетенции**	**Индикаторы достижения компетенции**	**Планируемые результаты обучения**
1	2	3	4
Искусственный интеллект для информационной безопасности	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. З-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 и аппаратное обеспечение технологий и систем искусственного интеллекта с учетом требований информационной безопасности для решения профессиональных задач в различных предметных областях

1.5. Форма обучения

Обучение по дисциплине модуля может осуществляться в очной форме.

2. СОДЕРЖАНИЕ И ОБЕСПЕЧЕНИЕ РЕАЛИЗАЦИИ ДИСЦИПЛИН МОДУЛЯ

ПРОГРАММА МОДУЛЯ
ИСКУССТВЕННЫЙ ИНТЕЛЛЕКТ ДЛЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

РАЗДЕЛ 2. СОДЕРЖАНИЕ И ОБЕСПЕЧЕНИЕ РЕАЛИЗАЦИИ ДИСЦИПЛИН МОДУЛЯ

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ
ИСКУССТВЕННЫЙ ИНТЕЛЛЕКТ ДЛЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

Рабочая программа дисциплины составлена авторами:

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

Рекомендовано учебно-методическим советом института радиоэлектроники и информационных технологий - РТФ

Протокол № 7 от 11.10.2021 г.

2. СОДЕРЖАНИЕ И ОСОБЕННОСТИ РЕАЛИЗАЦИИ ДИСЦИПЛИНЫ Искусственный интеллект для информационной безопасности

2.1. Технологии обучения, используемые при изучении дисциплины модуля

- Традиционная (репродуктивная) технология;
- Смешанная модель обучения с использованием онлайн-курса;
- Исключительно электронного обучения с использованием онлайн-курса;

2.2. Содержание дисциплины

Таблица 1.3

Код раздела, темы	Раздел, тема дисциплины*	Содержание
1	Основы компьютерной безопасности	Типы атак в информационной безопасности. Криптография. Хэш-функции. Безопасность компьютерных сетей и сетевых протоколов. Безопасность в ОС Linux. Инъекции. Бинарные уязвимости.
2	Применение машинного обучения для задач информационной безопасности	Определение спама. Классификация сетевых атак. Определение распределенной сетевой атаки “отказ в обслуживании”. Определение злонамеренных (malicious) сайтов. Определение инъекций. Поиск злонамеренного программного обеспечения (malware). Анализ аномалий в активности пользователей.
3	Проекты искусственного интеллекта в области информационной безопасности	Жизненный цикл проекта создания приложений искусственного интеллекта для информационной безопасности. Подготовка набора данных в информационной безопасности. Выбор модели и ее обучение. Оценка качества модели. Разработка приложения, использующего модель. Внедрение приложения в практическое использование.

2.3. Программа дисциплины реализуется на государственном языке Российской Федерации.

2.4. УЧЕБНО-МЕТОДИЧЕСКОЕ И ИНФОРМАЦИОННОЕ ОБЕСПЕЧЕНИЕ ДИСЦИПЛИНЫ Искусственный интеллект для информационной безопасности

Электронные ресурсы (издания)

1. Онлайн-курс “Основы компьютерной безопасности”. URL: https://ulearn.me/Course/Hackerdom/ (дата обращения: 05.10.2021).
2. Cyber Data Science – https://cyberdatascientist.com/ (дата обращения: 05.10.2021).
3. 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).
4. A summary of cybersecurity datasets highlighting diverse attack-types and machine learning-based usage in different cyber applications. URL: https://journalofbigdata.springeropen.com/articles/10.1186/s40537-020-00318-5/tables/2 (дата

обращения: 05.10.2021).
5. CS 259D Data Mining for Cyber Security. URL: https://web.stanford.edu/class/cs259d/ (дата обращения: 05.10.2021).
6. Awesome Machine Learning for Cyber Security. URL: https://github.com/jivoi/awesome-ml-for-cybersecurity (дата обращения: 05.10.2021).
7. Machine Learning for Security. URL: https://security.kiwi/docs/introduction/ (дата обращения: 05.10.2021).
8. Clarence Chio, David Freeman. Machine Learning and Security: Protecting Systems with Data and Algorithms book repository. URL: https://github.com/oreilly-mlsec/book-resources (дата обращения: 05.10.2021).

Профессиональные базы данных, информационно-справочные системы

1. Applied Science & Technology Source. EBSCO publishing http://search.ebscohost.com
2. Wiley Online Library http://onlinelibrary.wiley.com/
3. Гугл Академия https://scholar.google.ru/

Материалы для лиц с ОВЗ
Весь контент ЭБС представлен в виде файлов специального формата для воспроизведения синтезатором речи, а также в тестовом виде, пригодном для прочтения с использованием экранной лупы и настройкой контрастности.

Базы данных, информационно-справочные и поисковые системы

1. Academic Search Ultimate EBSCO publishing – http://search.ebscohost.com
2. eBook Collections Springer Nature – https://link.springer.com/
3. Гугл Академия – https://scholar.google.ru/
4. Электронный научный архив УрФУ https://elar.urfu.ru/
5. Зональная научная библиотека (УрФУ) - http://lib.urfu.ru/
6. Портал информационно-образовательных ресурсов УрФУ https://study.urfu.ru/
7. Электронно-библиотечная система «Лань» – https://e.lanbook.com/
8. Университетская библиотека ONLINE – https://biblioclub.ru/
9. Электронно-библиотечная система "Библиокомплектатор" (IPRbooks) http://www.bibliocomplectator.ru/available
10. Электронные информационные ресурсы Российской государственной библиотеки https://www.rsl.ru/
11. Научная электронная библиотека «КиберЛенинка» https://cyberleninka.ru/

2.5. МАТЕРИАЛЬНО-ТЕХНИЧЕСКОЕ ОБЕСПЕЧЕНИЕ ДИСЦИПЛИНЫ

Искусственный интеллект для информационной безопасности

Сведения об оснащенности дисциплины специализированным и лабораторным оборудованием и программным обеспечением

Таблица 3.1

№ п/п	Виды занятий	Оснащенность специальных помещений и помещений для самостоятельной работы	Перечень лицензионного программного обеспечения. Реквизиты подтверждающего документа
1	Лекции; Практические	Компьютерный класс. Мультимедийный проектор с	Используется бесплатно-распространяемое программное

	занятия.	экраном. Сетевое оборудование. Локальная сеть с выходом в глобальную сеть Internet.	обеспечение: 1. Python – https://www.python.org/ 2. TensorFlow – https://www.tensorflow.org/ 3. Веб - среда разработки для языка программирования Python: google colab - https://colab.research.google.com/ 4. WireShark – https://www.wireshark.org/ 5. Suricata – https://suricata.io/

ОЦЕНОЧНЫЕ МАТЕРИАЛЫ

Код модуля	**Модуль**
М.1.14	Искусственный интеллект для информационной безопасности

Екатеринбург, 2021

Оценочные материалы по модулю составлены авторами:

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

1. СТРУКТУРА И ОБЪЕМ МОДУЛЯ ИСКУССТВЕННЫЙ ИНТЕЛЛЕКТ ДЛЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

№ п/п	Перечень дисциплин модуля в последовательности их освоения	Объем дисциплин модуля и всего модуля в зачетных единицах и часах	Форма итоговой промежуточной аттестации по дисциплинам модуля и в целом по модулю
1.	Искусственный интеллект для информационной безопасности	3 з.е. /108 час.	Зачет
	ИТОГО по модулю:	**3 з.е. /108 час.**	

2. ОЦЕНОЧНЫЕ МАТЕРИАЛЫ ПО МОДУЛЮ

Не предусмотрено

Раздел 3. ОЦЕНОЧНЫЕ МАТЕРИАЛЫ ПО ДИСЦИПЛИНЕ
ИСКУССТВЕННЫЙ ИНТЕЛЛЕКТ ДЛЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

Модуль М 1.14 Искусственный интеллект для информационной безопасности

Оценочные материалы составлены автором(ами):

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

1. ПЛАНИРУЕМЫЕ РЕЗУЛЬТАТЫ ОБУЧЕНИЯ (ИНДИКАТОРЫ) ПО ДИСЦИПЛИНЕ МОДУЛЯ ИСКУССТВЕННЫЙ ИНТЕЛЛЕКТ ДЛЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

Таблица 1.1

Код и наименование компетенций, формируемые с участием дисциплины	**Планируемые результаты обучения**	**Контрольно-оценочные средства для оценивания достижения результата обучения по дисциплине**
1	**2**	**3**
УК-7 Способен обрабатывать, анализировать, передавать данные и информацию с использованием цифровых средств для эффективного решения поставленных задач с учетом требований информационной безопасности	УК-7. З-1. Сделать обзор угроз информационной безопасности, основных принципов организации безопасной работы в информационных системах и в сети интернет. УК-7. З-2. Описать способы и средства защиты персональных данных и данных в организации в соответствии с действующим законодательством. УК-7. У-1. Определять основные угрозы безопасности при использовании информационных технологий и выбирать оптимальные способы и средства защиты персональных данных и данных организации от мошенников и вредоносного ПО. УК-7. П-1. Обосновать выбор технических и программных средств защиты персональных данных и данных организации при работе с информационными системами на основе анализа потенциальных и реальных угроз безопасности информации. УК-7. П-2. Решать поставленные задачи, используя эффективные цифровые средства и средства информационной безопасности	1) Контрольная работа 2) Домашние работы 3) Выполнение практических работ 4) Зачет

Таблица 1.2

Код и наименование компетенций, формируемые с участием дисциплины	**Индикаторы достижения компетенции**	**Планируемые результаты обучения**	**Контрольно-оценочные средства для оценивания достижения результата обучения по дисциплине**
1	**2**	**3**	**4**
ПК-8. Способен	ПК-8.1. Разрабатывает	ПК-8.1. З-1. Знает новые	1) Контрольная

разрабатывать и модернизировать программное и аппаратное обеспечение технологий и систем искусственного интеллекта с учетом требований информационной безопасности в различных предметных областях	программное и аппаратное обеспечение технологий и систем искусственного интеллекта для решения профессиональных задач с учетом требований информационной безопасности в различных предметных областях	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 и аппаратное обеспечение технологий и систем искусственного интеллекта с учетом требований информационной безопасности для решения профессиональных задач в различных предметных областях	работа 2) Домашние работы 3) Выполнение практических работ 4) Зачет

2. ВИДЫ САМОСТОЯТЕЛЬНОЙ РАБОТЫ СТУДЕНТОВ, ВКЛЮЧАЯ МЕРОПРИЯТИЯ ТЕКУЩЕЙ АТТЕСТАЦИИ

2.1. Распределение объема времени по видам учебной работы

Таблица 2

№ п/п	Наименование дисциплины модуля Искусственный интеллект для информационной безопасности	Объем времени, отведенный на освоение дисциплины модуля								
		Аудиторные занятия, час.				Промежуточная аттестация (форма итогового контроля)	Контактная работа (час.)	Самостоятельная работа студента, включая текущую аттестацию (час.)	Всего по дисциплине	
		Занятия лекционного типа	Практические работы	Лабораторные работы	Всего				Час.	Зач. ед.
1	2	3	4	5	6	7	8	9	10	11
1.	Искусственный интеллект для информационной безопасности	18	18	0	36	Зачет	41.65	66.35	108	3

2.2. Виды СРС, количество и объем времени на контрольно-оценочные мероприятия СРС по дисциплине

Контрольно-оценочные мероприятия СРС включают самостоятельное изучение материала, подготовку к аудиторным занятиям и мероприятиям текущего контроля, выполнение и оформление внеаудиторных мероприятий текущего контроля и подготовку к мероприятиям промежуточного контроля.

Таблица 3

№ п/п	Вид самостоятельной работы студента по дисциплине модуля	Количество контрольно-оценочных мероприятий СРС	Объем контрольно-оценочных мероприятий СРС (час.)
1.	Подготовка к аудиторным занятиям и мероприятиям текущего контроля: лекционным, практическим занятиям.		13,5 час.
2	Выполнение и оформление мероприятий текущего контроля:		
2.1	Контрольная работа	1	5 час.
2.2	Домашняя работа	2	10 час.
3.	Подготовка к зачету	зачет	12 час.
4.	Самостоятельное изучение материала		25,85 час.
	Итого на СРС по дисциплине:		66,35 час.

3. ПРОЦЕДУРЫ КОНТРОЛЯ И ОЦЕНИВАНИЯ РЕЗУЛЬТАТОВ ОБУЧЕНИЯ В РАМКАХ ТЕКУЩЕЙ И ПРОМЕЖУТОЧНОЙ АТТЕСТАЦИИ ПО ДИСЦИПЛИНЕ МОДУЛЯ В БАЛЬНО-РЕЙТИНГОВОЙ СИСТЕМЕ (ТЕХНОЛОГИЧЕСКАЯ КАРТА БРС)

Процедуры текущей и промежуточной аттестации по дисциплине

1.Лекции: коэффициент значимости совокупных результатов лекционных занятий – 0.5		
Текущая аттестация на лекциях	**Сроки – семестр, учебная неделя**	**Максимальная оценка в баллах**
Контрольная работа	3 сем.	*80*
Самостоятельное изучение материала	3 сем.	*20*
Весовой коэффициент значимости результатов текущей аттестации по лекциям – 0.5		
Промежуточная аттестация по лекциям – *Зачет* **Весовой коэффициент значимости результатов промежуточной аттестации по лекциям – 0.5**		
2. Практические/семинарские занятия: коэффициент значимости совокупных		

результатов практических/семинарских занятий – 0.5		
Текущая аттестация на практических/семинарских занятиях	**Сроки – семестр, учебная неделя**	**Максимальная оценка в баллах**
Выполнение и оформление практических работ	3 сем.	40
Домашняя работа №1	3 сем.	30
Домашняя работа №2	3 сем.	30
Весовой коэффициент значимости результатов текущей аттестации по практическим/семинарским занятиям – 1		
Промежуточная аттестация по практическим/семинарским занятиям– не предусмотрена **Весовой коэффициент значимости результатов промежуточной аттестации по практическим/семинарским занятиям – 0**		
3. Лабораторные занятия: Не предусмотрены коэффициент значимости совокупных результатов лабораторных занятий – 0		

4. КРИТЕРИИ И УРОВНИ ОЦЕНИВАНИЯ РЕЗУЛЬТАТОВ ОБУЧЕНИЯ ПО ДИСЦИПЛИНЕ МОДУЛЯ

4.1. В рамках БРС применяются утвержденные на кафедре/институте критерии (признаки) оценивания достижений студентов по дисциплине модуля (табл. 4) в рамках контрольно-оценочных мероприятий на соответствие указанным в табл.1 результатам обучения (индикаторам).

Таблица 4

Критерии оценивания учебных достижений обучающихся

Результаты обучения	**Критерии оценивания учебных достижений, обучающихся на соответствие результатам обучения/индикаторам**
Знания	Студент демонстрирует знания и понимание в области изучения на уровне указанных индикаторов и необходимые для продолжения обучения и/или выполнения трудовых функций и действий, связанных с профессиональной деятельностью.
Умения	Студент может применять свои знания и понимание в контекстах, представленных в оценочных заданиях, демонстрирует освоение умений на уровне указанных индикаторов и необходимых для продолжения обучения и/или выполнения трудовых функций и действий, связанных с профессиональной деятельностью.
Опыт /владение	Студент демонстрирует опыт в области изучения на уровне указанных индикаторов.
Личностные качества	Студент демонстрирует ответственность в освоении результатов обучения на уровне запланированных индикаторов. Студент способен выносить суждения, делать оценки и формулировать выводы в области изучения. Студент может сообщать преподавателю и коллегам своего уровня собственное понимание и умения в области изучения.

4.2. Для оценивания уровня выполнения критериев (уровня достижений обучающихся при проведении контрольно-оценочных мероприятий по дисциплине модуля) используется универсальная шкала (табл. 5).

Таблица 5

Шкала оценивания достижения результатов обучения (индикаторов) по уровням

Характеристика уровней достижения результатов обучения (индикаторов)				
№ п/п	**Содержание уровня выполнения критерия оценивания результатов обучения (выполненное оценочное задание)**	**Шкала оценивания**		
		Традиционная характеристика уровня		**Качественная характеристика уровня**
1.	Результаты обучения (индикаторы) достигнуты в полном объеме, замечаний нет	Отлично (80-100 баллов)	Зачтено	Высокий (В)
2.	Результаты обучения (индикаторы) в целом достигнуты, имеются замечания, которые не требуют обязательного устранения	Хорошо (60-79 баллов)		Средний (С)
3.	Результаты обучения (индикаторы) достигнуты не в полной мере, есть замечания	Удовлетворительно (40-59 баллов)		Пороговый (П)
4.	Освоение результатов обучения не соответствует индикаторам, имеются существенные ошибки и замечания, требуется доработка	Неудовлетворительно (менее 40 баллов)	Не зачтено	Недостаточный (Н)
5.	Результат обучения не достигнут, задание не выполнено	Недостаточно свидетельств для оценивания		Нет результата

5. СОДЕРЖАНИЕ КОНТРОЛЬНО-ОЦЕНОЧНЫХ МЕРОПРИЯТИЙ ПО ДИСЦИПЛИНЕ МОДУЛЯ

Задания по контрольно-оценочным мероприятиям в рамках текущей и промежуточной аттестации должны обеспечивать освоение и достижение результатов обучения (индикаторов) и предметного содержания дисциплины на соответствующем уровне.

5.1. Описание контрольно-оценочных мероприятий и средств текущего контроля по дисциплине модуля

5.1.1. Практические занятия

Номер занятия	**Примерный перечень тем практических занятий**
1	Основы информационной безопасности. Модели атак.
2	Злонамеренное программное обеспечение (malware, malicious software)
3	Анализ сетевого трафика.
4	Инъекции кода. SQL инъекции.
5	Определение спама.
6	Обнаружение и классификация сетевых атак.

7	Поиск злонамеренного программного обеспечения.
8	Определение злонамеренных сайтов.
9	Определение инъекций.

5.1.2. Лабораторные занятия
Не предусмотрено

5.1.3. Курсовая работа / Курсовой проект
Не предусмотрено

5.1.4. Контрольная работа

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.

5.1.5. Домашняя работа

Примерная тематика домашних работ***:***
Домашняя работа №1:
Определение сетевых атак.

Домашняя работа №2:
Обнаружение злонамеренных сайтов.

Примерные задания в составе домашних 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 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

5.1.6. Расчетная работа / Расчетно-графическая работа
Не предусмотрено

5.1.7. Реферат / эссе / творческая работа
Не предусмотрено

5.1.8. Проектная работа
Не предусмотрено

5.1.9. Деловая (ролевая) игра / Дебаты / Дискуссия / Круглый стол
Не предусмотрено

5.1.10. Кейс-анализ
Не предусмотрено

5.2. Описание контрольно-оценочных мероприятий промежуточного контроля по дисциплине модуля

5.2.1. Зачет в форме независимого тестового контроля (НТК).
НТК по дисциплине модуля не проводится.

5.2.2. Зачет в традиционной форме (устные /письменные ответы на вопросы)

Список примерных тем для зачёта:
1. Модели атак в информационной безопасности.
2. Решение задач информационной безопасности с использованием классификации.
3. Решение задач информационное безопасности с использованием кластеризации.
4. Решение задач информационной безопасности с использованием определения аномалий.
5. Решение задач информационной безопасности с использованием состязательного машинного обучения.
6. Определение спама с помощью методов машинного обучения.
7. Злонамеренное программное обеспечение и его определение с помощью методов машинного обучения.
8. Злонамеренные сайты и их определение с помощью методов машинного обучения.
9. Анализ сетевого трафика с помощью методов машинного обучения.
10. Обнаружение сетевых вторжений с помощью методов машинного обучения.
11. Обнаружение распределенных сетевых атак с помощью методов машинного обучения.
12. Обнаружение аномалий в активности пользователей с помощью методов машинного обучения.
13. Обнаружение SQL-инъекций с помощью методов машинного обучения.
14. Жизненный цикл проекта создания приложений искусственного интеллекта для информационной безопасности.
15. Подготовка набора данных для систем искусственного интеллекта для информационной безопасности. Качество данных. Очистка данных.
16. Формирование признаков для для систем искусственного интеллекта для информационной безопасности.
17. Выбор модели машинного обучения для систем искусственного интеллекта для информационной безопасности.
18. Оценка качества систем искусственного интеллекта для информационной безопасности.
19. Разработка приложений искусственного интеллекта для информационной безопасности.
20. Открытое программное обеспечение для информационной безопасности. Интеграция с системами искусственного интеллекта.