**ОЦЕНОЧНЫЕ МАТЕРИАЛЫ**

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

**Барнаул, 2021**

**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

**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 | Терновой О.С. | К.тех. н., нет | Доцент каф. информатики | Кафедра информатики |

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

Таблица 1.1

|  |  |  |
| --- | --- | --- |
| **Код и наименование компетенций, формируемые с участием дисциплины** | **Индикаторы достижения компетенции** | **Контрольно-оценочные средства для оценивания достижения результата обучения по дисциплине** |
| **1** | **2** | **3** |
| ОПК-2. Способен разрабатывать оригинальные алгоритмы и программные средства, в том числе с использованием современных интеллектуальных технологий, для решения профессиональных задач | ОПК-2.1. Знать: современные информационно-коммуникационные и интеллектуальные технологии, инструментальные среды, программно-технические платформы для решения профессиональных задач.  ОПК-2.2. Уметь: обосновывать выбор современных информационно-коммуникационных и интеллектуальных технологий, разрабатывать оригинальные программные средства для решения профессиональных задач.  ОПК-2.3. Владеть: методами разработки оригинальных программных средств, в том числе с использованием современных информационно-коммуникационных и интеллектуальных технологий, для решения профессиональных задач. | 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** |
| Искусственный интеллект для информационной безопасности | 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) Контрольная работа  2) Домашние работы  3) Выполнение практических работ  4) Зачет |
| 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. З-1. Знает особенности модернизации программного и аппаратного обеспечения 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 |

1. **ВИДЫ САМОСТОЯТЕЛЬНОЙ РАБОТЫ СТУДЕНТОВ, ВКЛЮЧАЯ МЕРОПРИЯТИЯ ТЕКУЩЕЙ АТТЕСТАЦИИ**
   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 |
|  | Искусственный интеллект для информационной безопасности | 18 | 18 | 0 | 36 | Зачет | 41.65 | 66.35 | 108 | 3 |

* 1. **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. |

1. **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** | | |

1. **КРИТЕРИИ И УРОВНИ ОЦЕНИВАНИЯ РЕЗУЛЬТАТОВ ОБУЧЕНИЯ ПО ДИСЦИПЛИНЕ МОДУЛЯ** 
   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. |

* 1. 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 |

1. **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.