Федеральное государственное бюджетное образовательное учреждение высшего образования «Алтайский государственный университет»

УТВЕРЖДАЮ

Директор Института математики

и информационных технологий

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_Е.В. Журавлев

«29» октября 2021 г.

**РАБОЧАЯ ПРОГРАММА МОДУЛЯ**

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

**Барнаул, 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 |

**Рекомендовано учебно-методическим советом Института математики и информационных технологий**

Протокол №3 от 28.09.2021 г.

1. **ОБЩАЯ ХАРАКТЕРИСТИКА МОДУЛЯ Искусственный интеллект для информационной безопасности** 
   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.

**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. **Последовательность освоения модуля в образовательной программе**

|  |  |
| --- | --- |
| **Пререквизиты модуля** | *отсутствуют* |
| **Постреквизиты и корреквизиты модуля** | *отсутствуют* |

* 1. **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 | 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. |

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 |
| 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. **Форма обучения**

Обучение по дисциплине модуля может осуществляться в очной форме.

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

**Рекомендовано учебно-методическим советом Института математики и информационных технологий**

Протокол №3 от 28.09.2021 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. СПС КонсультантПлюс (инсталлированный ресурс АлтГУ или <http://www.consultant.ru/>)
5. Электронная база данных «Scopus» (<http://www.scopus.com>)
6. Электронная библиотечная система Алтайского государственного университета (http://elibrary.asu.ru/)
7. Электронный научный архив УрФУ <https://elar.urfu.ru/>
8. Зональная научная библиотека (УрФУ) - <http://lib.urfu.ru/>
9. Портал информационно-образовательных ресурсов УрФУ <https://study.urfu.ru/>
10. Электронно-библиотечная система «Лань» – <https://e.lanbook.com/>
11. Университетская библиотека ONLINE – <https://biblioclub.ru/>
12. Электронно-библиотечная система "Библиокомплектатор" (IPRbooks) <http://www.bibliocomplectator.ru/available>
13. Электронные информационные ресурсы Российской государственной библиотеки <https://www.rsl.ru/>
14. 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 программного обеспечения.** |
| 1 | Лекции; Практические занятия. | Компьютерный класс.  Мультимедийный проектор с экраном.  Сетевое оборудование.  Локальная сеть с выходом в глобальную сеть Internet. | Используется бесплатно-распространяемое программное 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/> |