1. **Паспорт Образовательной программы**

**«Методы искусственного интеллекта в кибербезопасности»**

|  |  |
| --- | --- |
| **Версия программы** | **1** |
| **Дата Версии** | 10**.**10**.**2020 |

1. **Сведения о Провайдере**

|  |  |  |
| --- | --- | --- |
| 1.1 | Провайдер | Университет ИТМО |
| 1.2 | Логотип образовательной организации |  |
| 1.3 | Провайдер ИНН | 7813045547 |
| 1.4 | Ответственный за программу ФИО | Михайлова Елена Георгиевна |
| 1.5 | Ответственный должность | Директор Высшей школы цифровой культуры, Университет ИТМО |
| 1.6 | Ответственный Телефон | +79219979791 |
| 1.7 | Ответственный Е-mail | e.mikhailova@itmo.ru |

1. **Основные Данные**

|  |  |  |
| --- | --- | --- |
| **№** | **Название** | **Описание** |
| 2.1 | Название программы | Методы искусственного интеллекта в кибербезопасности |
| 2.2 | Ссылка на страницу программы | Приложено в личном кабинете на платформе 20.35 |
| 2.3 | Формат обучения | Онлайн |
| 2.4 | Подтверждение от ОО наличия возможности реализации образовательной программы с применением электронного обучения и (или) дистанционных образовательных технологий с возможностью передачи данных в форме элементов цифрового следа | Приложено в личном кабинете на платформе 20.35 |
| 2.5 | Уровень сложности | Базовый |
| 2.6 | Количество академических часов | 72 |
| 2.7 | Практикоориентированный характер образовательной программы: не менее 50 % трудоёмкости учебной деятельности отведено практическим занятиям и (или) выполнению практических заданий в режиме самостоятельной работы (кол-во академических часов) | 50 |
| 2.8 | Стоимость обучения одного обучающегося по образовательной программе, а также предоставление ссылок на 3 (три) аналогичные образовательные программы иных организаций, осуществляющих обучение, для оценки объективности стоимости или обоснование уникальности представленной образовательной программы в случае отсутствия аналогичных образовательных программ на рынке образовательных услуг | Введение в кибербезопасность от академии ITHUB  https://academy.ithub.ru/course/osnkiber  от 22500 рублей за 24 ак.час.  Курсы повышения квалификации по информационной безопасности от "НОЧУ ДПО "МУЦ"  https://nousro.ru/pk-informatsionnaya-bezopasnost.php  от 20000 до 30000 рублей за 72 ак.час.  Основы кибербезопасности (CCNA Cybersecurity Operations) от Институт дополнительного образования Санкт-Петербургский политехнический университет Петра Великого  http://hse.spbstu.ru/Courses/Course/CCNA-CS-Osnovy-kiberbezopasnosti-CCNA-Cybersecurity-Operations/2316/#nav-about  19200 рублей за 40 ак.час. |
| 2.9 | Минимальное количество человек на курсе | 100 |
| 2.10 | Максимальное количество человек на курсе | Не ограничено |
| 2.11 | Данные о количестве слушателей, ранее успешно прошедших обучение по образовательной программе | 4000 |
| 2.12 | Формы аттестации | Контрольная работа, зачет |
| 2.13 | Указание на область реализации компетенций цифровой экономики, к которой в большей степени относится образовательная программа, в соответствии с Перечнем областей | Кибербезопасность и защита данных |

1. **Аннотация программы**

Наиболее полное и содержательное описание программы, которое включает:

1) общую характеристику компетенций, качественное изменение которых осуществляется в результате обучения или которые формируются в результате освоения образовательной программы;

2) описание требований и рекомендаций для обучения по образовательной программе;

3) краткое описание результатов обучения в свободной форме, а также описание востребованности результатов обучения в профессиональной деятельности.

Ограничение по размеру: не менее 1000 символов -?

Программа посвящена технологиям защиты информации и кибербезопасности.

Не секрет, что в современном мире нас окружает огромное количество информации. Сложно представить отрасли современной и тем более цифровой экономики, в которых в той или иной степени не осуществлялась бы работа с большим объемом данных. Эту информацию нужно хранить, обрабатывать, анализировать и, конечно, защищать. Кибербезопасность является неотъемлемой частью современного информационного мира, и проникает чуть ли не во все его сферы, начиная с банальной индивидуальной информационной безопасности (защита персональных данных, противодействие сетевому мошенничеству, защита от спам сообщений и так далее) и заканчивая многоступенчатыми системами корпоративной информационной безопасности, средствами борьбы с ботнетами, противодействием фейкам и тому подобное.

Назначение программы обучения – познакомить слушателей с основными направлениями кибербезопасности и показать практические аспекты технологий, позволяющих осуществлять обнаружение различного рода угроз и производить их нейтрализацию. Современные методы защиты информации базируются на алгоритмах машинного обучения, поэтому в рамках курса слушатели сначала узнают, какие задачи решает машинное обучение, познакомятся с методами решении задач обучения с учителем: регрессии и классификации. Второй модуль курса посвящен непосредственному применению рассмотренных методов и алгоритмов в задачах кибербезопасности. В процессе выполнения практических упражнений курса слушатели познакомятся с приемами шифрования информации, калькуляторами угроз безопасности информации, методами предсказания и выявления сетевых атак, настройкой алгоритмов биометрической идентификации посредством платформы Azure ML Studio. Для работы с курсом требуется компьютер с выходом в интернет - для выполнения упражнений не потребуется установка программных средств на свой компьютер, все рекомендуемые в курсе инструменты доступны удаленно.

****

**ОБЩАЯ ХАРАКТЕРИСТИКА ПРОГРАММЫ**

**1.Цель программы**

Дать навыки применения методов машинного обучения в задачах обеспечения кибербезопасности.

**2.Планируемые результаты обучения:**

2.1.Знание (осведомленность в областях)

2.1.1. Области применения цифровых технологий в личностной и профессиональной сферах

2.1.2. Основные типы задач, решаемых в рамках областей машинного обучения и искусственного интеллекта

2.1.3. Основные методы, используемые для решения задач областей машинного обучения и искусственного интеллекта

2.1.4. Аналитические методы обработки данных, основы искусственного интеллекта

2.1.5. Существующие методы работы с данными, области их применения, достоинства и недостатки

2.1.6. Особенности информационных потоков в своей профессиональной области, правовые и этические аспекты распространения информации

2.1.7. Основные цифровые технологии и алгоритмы их работы

2.1.8. Области применения алгоритмов машинного и статистического обучений, искусственного интеллекта для решения прикладных задач

2.1.9. Методы анализа данных для хранения, обработки и эффективного использования полученной информации

2.1.10. Терминологию и методы, используемые в машинном обучении и искусственном интеллекте, для решения задач кибербезопасности

2.1.11. Принципы анализа данных из области кибербезопасности

2.1.12. Современные тенденции и тренды в инструментах, используемых для защиты информации

2.1.13. Методы и алгоритмы шифрования информации

2.1.14. Современные инструменты, применяемые в сфере обеспечения информационной безопасности

2.1.15. Методы оценки качества алгоритмов классификации

2.1.16. Приемы работы в инструментах анализа данных

2.1.17. Современные инструменты анализа данных, а также их особенности применительно к сфере кибербезопасности

2.1.18. Особенности применения методов машинного обучения и искусственного интеллекта в различных информационных системах

2.2. Умение (способность к деятельности)

2.2.1. Использовать компьютерную технику и цифровые технологии для автоматизации информационно-аналитической деятельности

применять методы машинного обучения для интерпретации и анализа данных из области информационной безопасности

2.2.2. Отбирать технологии работы с информацией в зависимости от класса задач в области защиты данных

2.2.3. Использовать компьютерную технику и цифровые технологии для автоматизации информационно-аналитической деятельности

2.2.4. Планировать аналитические работы в информационно-технологическом проекте

2.2.5. Применять методы статистического анализа данных

2.2.6. Использовать различные инструменты хранения и обработки данных

2.2.7. Проверять корректность построенной модели

2.2.8. Интерпретировать результаты вероятностной классификации

2.2.9. Подбирать приемы первичной обработки данных в зависимости от их структуры

2.2.10. Использовать инструменты оценки уровня информационных угроз

2.2.11. Применять алгоритмы шифрования и дешифрования информации

2.2.12. Кастомизировать настраиваемые параметры инструмента для улучшения качества анализа данных предметной области

2.2.13. Применять инструменты анализа данных к задачам, решаемым методами машинного обучения и искусственного интеллекта

2.2.14. Настраивать информационные системы под нужды предметной области

2.2.15. Использовать особенности реализации методов машинного обучения и искусственного интеллекта внутри информационной системы для более эффективного решения поставленной задачи

2.3.Навыки (использование конкретных инструментов)

Инструменты: электронные таблицы, Azure ML Studio, WolframAlpha, Калькулятор уязвимостей

2.3.1 Владеть аппаратом цифровых технологий для получения, обработки и передачи информации с помощью технических средств и методов

2.3.2 Владеть методами обработки данных предметной области

2.3.3 Владеть современными инструментами и компьютерными технологиями для решения задач, связанных с обработкой и анализом данных, применительно к любой предметной области.

2.3.4 Владеть современными подходами и методами искусственного интеллекта в целом и машинного обучения в частности применительно к задачам обеспечения информационной безопасности, средствами и информационными технологиями для осуществления интеллектуального анализа данных

2.3.5 Владеть методами описания моделей обрабатываемых данных

2.3.6 Владеть методами концептуального, функционального и логического проектирования систем среднего и крупного масштаба и сложности — методами исследования зависимостей и закономерностей в данных

2.3.7 Владеть подходами к восстановлению различных статистических зависимостей

2.3.8 Владеть инструментами для осуществления качественного анализа построенной модели — широким кругозором как в сфере информационных систем, так и в сфере их адаптации к области обеспечения кибербезопасности

2.3.9 Владеть современными инструментами обнаружения аномалий и атак в сетевом трафике, а также идентификации и биометрии

2.3.10 Владеть навыками кастомизации информационной системы под задачи предметной области, приемами использования информационной системы

2.3.11 Владеть приемами обучения использования информационной системы, настроенной под конкретную предметную область

2.3.12 Владеть методами машинного обучения и искусственного интеллекта, реализованных в информационных системах

**3.Категория слушателей** (возможно заполнение не всех полей)

* 1. Высшее или среднее профессиональное образование
  2. Требований к квалификации не предъявляется
  3. Опыт профессиональной деятельности не требуется
  4. Предварительное освоение иных дисциплин не требуется

**4.Учебный план программы «**Методы искусственного интеллекта в кибербезопасности**»**

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **№ п/п** | **Модуль** | **Всего, час** | **Виды учебных занятий** | | |
| **лекции** | **практические занятия** | **самостоятельная работа** |
| 1 | Методы машинного обучения | 26 | 8 | 8  Обучающие практические задания | 10  Практические контрольные работы |
| 2 | Искусственный интеллект в задачах кибербезопасности | 46 | 14 | 14  Обучающие практические задания | 18  Практические контрольные работы |
| **Итоговая аттестация** | |  | **Указывается вид (экзамен, зачёт, реферат и т.д.)** | | |
| Итоговый зачет по дисциплине | | 72 | зачет | | |

**5.Календарный план-график реализации образовательной** программы

(дата начала обучения – дата завершения обучения) в текущем календарном году, указания на периодичность набора групп (не менее 1 группы в месяц)

|  |  |  |  |
| --- | --- | --- | --- |
| **№ п/п** | **Наименование учебных модулей** | **Трудоёмкость (час)** | **Сроки обучения** |
| **1** | Методы машинного обучения | 26 | 01.11.2020 - 7.11.2020 |
| **2** | Искусственный интеллект в задачах кибербезопасности | 46 | 8.11.2020 - 15.11.2020 |
| **Всего:** | | 72 | 01.11.2020 - 15.11.2020 |

**6.Учебно-тематический план программы «** Методы искусственного интеллекта в кибербезопасности**»**

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| **№ п/п** | **Модуль / Тема** | **Всего, час** | **Виды учебных занятий** | | | **Формы контроля** |
| **лекции** | **практические занятия** | **самостоятельная работа** |
| 1 | Методы машинного обучения | 26 | 8 | 8  Обучающие практические задания | 10  Практические контрольные работы |  |
| 1.1 | Введение в машинное обучение | 8 | 2 | 2  Обучающие практические задания | 4  Практическая контрольная работа | Опросы, итоговое упражнение |
| 1.2 | Задача регрессии | 8 | 3 | 3  Обучающие практические задания | 2  Практическая контрольная работа | Опросы, итоговое упражнение |
| 1.3 | Задача классификации: вероятностный подход | 10 | 3 | 3  Обучающие практические задания | 4  Практическая контрольная работа | Опросы, итоговое упражнение |
| 2 | Искусственный интеллект в задачах кибербезопасности | 46 | 14 | 14  Обучающие практические задания | 18  Практические контрольные работы |  |
| 2.1 | Основы персональной информационной безопасности | 8 | 3 | 3  Обучающие практические задания | 2  Практическая контрольная работа | Опросы, итоговое упражнение |
| 2.2 | Введение в информационную безопасность | 8 | 3 | 3  Обучающие практические задания | 2  Практическая контрольная работа | Опросы, итоговое упражнение |
| 2.3 | Искусственный интеллект в задачах информационной безопасности | 10 | 3 | 3  Обучающие практические задания | 4  Практическая контрольная работа | Опросы, итоговое упражнение |
| 2.4 | Обнаружение аномалий и атак в сетевом трафике | 10 | 2 | 2  Обучающие практические задания | 6  Практическая контрольная работа | Опросы, итоговое упражнение |
| 2.5 | Идентификация. Биометрия | 10 | 3 | 3  Обучающие практические задания | 4  Практическая контрольная работа | Опросы, итоговое упражнение |

**7. Учебная (рабочая) программа повышения квалификации «** Методы искусственного интеллекта в кибербезопасности **»**

**Модуль 1.** Методы машинного обучения **(**26 **час.)**

**Тема 1.1** Введение в машинное обучение **(**8 **час**.**)**

Рассматриваются основные задачи, ветки и методы машинного обучения, а также необходимый для дальнейшего аппарат статистики.

**Тема 1.2** Задача регрессии (8 час.)

Рассматриваются модели простейшей и множественной регрессии. Дается представление о полиномиальной регрессии.

Тема 1.3 Задача классификации: вероятностный подход (10 час.)

Рассматривается вероятностный подход к решению задачи классификации на примере наивного байесовского классификатора и его обобщений.

**Модуль 2.** Прикладные задачи искусственного интеллекта (46 **час.)**

**Тема 2.1.** Основы персональной информационной безопасности (8 час.)

Рассматриваются основы персональной информационной безопасности, вредоносное ПО, парольные системы.

Тема 2.2 Введение в информационную безопасность (8 час.)

Рассматриваются симметричные системы шифрования, несимметричная криптография, алгоритм шифрования RSA и Эль-Гамаля, электронная подпись.

Тема 2.3 Искусственный интеллект в задачах информационной безопасности (10 час.)

Рассматриваются базовые понятия информационной безопасности, методы защиты информации. Роль ИИ в кибербезопасности, оценка алгоритмов машинного обучения.

Тема 2.4 Обнаружение аномалий и атак в сетевом трафике (10 час.)

Рассматривается применение МО для обнаружения сетевых атак и аномалий, межсетевые экраны и системы обнаружения вторжений.

Тема 2.5 Идентификация. Биометрия (10 час.)

Рассматриваются основы биометрии, виды аутентификации и задача отбора признаков. Состязательные атаки на биометрические системы.

**Описание практико-ориентированных заданий и кейсов**

|  |  |  |  |
| --- | --- | --- | --- |
|  | **Номер темы/модуля** | **Наименование практического занятия** | **Описание** |
| **1.1** | Введение в машинное обучение | Основы работы в Azure ML Studio | Рассматриваются популярные инструменты как работы с методами машинного обучения, так и для решения прикладных задач с их помощью |
| **1.2** | Задача регрессии | Построение модели регрессии | Рассматриваются методы построения регрессионных моделей по данному тренировочному набору данных |
| 1.3 | Задача классификации: вероятностный подход | Решение задачи классификации алгоритмом логистической регрессии | Рассматривается применение алгоритма логистической регрессии для решения задачи классификации |
| 2.1 | Основы персональной информационной безопасности | Моделирование атаки на страницу пользователя в социальной сети. Хэширование и дехэширование паролей. | Рассматривается применение методов социального инжиниринга, также методы хэширования информации. |
| 2.2 | Введение в информационную безопасность | Шифрование текстовых данных с использованием ключей, посредством алгоритма RSA | Рассматривается шифрование текстовых данных с использованием таблицы символов ASCII, открытых и закрытых ключей посредством алгоритма RSA. Дешифрование зашифрованной информации |
| 2.3 | Искусственный интеллект в задачах информационной безопасности | Оценка уровня информационных угроз | Рассматриваются методы оценки уязвимостей по базовым, временным и контекстным метрикам для моделируемых ситуаций при помощи калькуляторов уязвимостей. |
| 2.4 | Обнаружение аномалий и атак в сетевом трафике | Классификация траффика | Рассматривается построение классификатора на основе алгоритма логистической регрессии, способного отличать подозрительный трафик от нормального. |
| 2.5 | Идентификация. Биометрия | Моделирование систем биометрической и идентификации | Рассматривается применение алгоритма логистической регрессии для решения задачи идентификации |

**8.Оценочные материалы по образовательной программе**

**8.1. Вопросы тестирования по модулям**

|  |  |  |  |
| --- | --- | --- | --- |
| **№ модуля** | **Вопросы входного тестирования** | **Вопросы промежуточного тестирования** | **Вопросы итогового тестирования** |
| **1.1** | Из приведенных вариантов выберите наименее уязвимый для кибератак пароль:  1) Собственная фамилия  2) Кличка домашнего животного  3) Случайная комбинация букв разного регистра  4) Случайная комбинация букв разного регистра и цифр  Что такое SPAM?  1) Письмо, содержащее вирусы  2) Письмо, содержащее рекламную рассылку  3) Письмо, содержащее длинную историю о том, что Вы получили наследство  4) Письмо, содержащее вредоносное ПО | Какие основные ветки, согласно описанной в лекции классификации, включает в себя обучение без учителя?  1) Кластеризация  2) Классификация  3) Регрессия  4) Уменьшение размерности  5) Поиск ассоциаций | Нейрон имеет четыре входных канала с весами 0.3,0.2,0.7,1.0, по ним проходят значения 3,6,2,8, соответственно. Если нейрон складывает значения со всех входов, какое число он содержит? |
| **1.2** | Выберите соотношение, которым описывается модель простейшей линейной регрессии:  1)  2)  3)  4) | Используя данные из приложенного файла, вычислите значение t-статистики (используя t-тест Стьюдента): | Модель полиномиальной регрессии описывается соотношением:  1)  2)  3) |
| 1.3 | Логистическая регрессия позволяет:  1) Предсказать значение отклика по значению предиктора  2) Предсказать значение предиктора по значению отклика 3) Найти вероятность отнесения данного объекта к определенному классу  4) Найти вероятность отнесения данного класса к определенному объекту | Оцените вероятность получения кредита для дохода 55 тысяч рублей:  1) 0.78 для линейной и 0.6 для логистической  2) 0.6 для линейной и 0.78 для логистической  3) 0.65 для линейной и 0.88 для логистической  4) 0.88 для линейной и 0.65 для логистической | Даны результаты классификации:  Вычислите долю истинно положительных примеров, TPR  Вычислите долю ложно положительных примеров, FPR: |
| 2.1 | Как называется группа компьютеров, объединенная в сеть и используемая хакерами для осуществления кибератак?  1) DDoS  2) DoS  3) ОС  4) Руткит  5) Ботнет  6) Спуфинг | Какой из этих паролей наиболее надежный?  1) password  2) Password1!  3) P@$$w0rd1!  4) 1Little2Little3LittleBuses! | С помощью какого прибора можно обнаружить закладное устройство?  1) Индикатор заряда.  2) Детектор поля.  3) Сотовый телефон. |
| 2.2 | Совпадают ли в несимметричной системе шифрования ключи для шифрования и для дешифрации? | В каком году была впервые предложена идея передачи секретной информации по незашифрованному каналу? | Сколько чисел в открытом ключе алгоритма RSA? |
| 2.3 | Что относится к предотвращению утечек конфиденциальной информации?  1) межсетевые экраны  2) DeepFake  3) DLP-системы  4) криптографические алгоритмы | Что случилось в результате проявления Mirai?  1) Отказали центрифуги для обогащения урана в Иране  2) Зашифровались данные на 300+ тысячах компьютеров во всех странах  3) Была прервана работа PayPal и Sony  4) Осуществлялся сбор информации для последующих фишинговых атак | Какая атака НЕ относится к Adversarial ML?  1) Разведывательная  2) Атака в обход  3) Отравляющая  4) Атака отказа в обслуживании |
| 2.4 | Какая сетевая атака характеризуется резким возрастанием количества запросов к серверу, который, в итоге, перестает отвечать на запросы?  1) DoS  2) Sybil  3) MitM  4) Spoofing | В чем отличие выброса и аномалии?  1) И выброс, и аномалия - ошибки в работе классификатора  2) Выброс - единичное, возможно, ошибочное значение в данных; аномалия - отклонение от нормального поведения  3) Выброс - систематическое проявление ошибки при создании датасета, аномалия - единичное проявление атаки | Какая система обнаружения вторжений плохо справляется с обнаружением новых (неизвестных) видов атак?  1) Сигнатурная  2) На основе обнаружения аномалий  3) Гибридная  4) Межуровневая |
| 2.5 | Что не относится к недостаткам «ручного» профайлинга?  1) отсутствие стандартов  2) отсутствие четкого алгоритма, по которому составляется портрет  3) отсутствие возможности сбора данных | Какая технология идентификации по лицу, считающаяся наиболее надежной, была взломана с помощью трехмерной маски лица с подогревом?  1) liveness detection  2) 3D-GAIN  3) Face-ID  4) Deep Fake | Какой фактор влияет на эффективность идентификации кроме метода классификации?  1) количество анализируемых текстов  2) используемые характеристики электронного сообщения  3) производительность системы  4) количество пользователей в системе |

**8.2.** Оценивание результатов обучения производится следующим образом. По каждой теме обучающимся выдаются индивидуальные задачи (контрольная работа). Задачи включают в себя некоторое количество (1-20) заданий. Задание выполняется обучающимся при помощи сети Интернет и инструментов, рассматриваемых в лекции. Срок выполнения – согласно указанным срокам обучения. Для ввода ответа на задания дается от двух до десяти попыток. Подпункты задачи оцениваются равномерно. Если в задаче N полей ввода, то каждое оценивается согласно формуле 12,5/N. Итого, максимально возможный балл за задачу равен 12,5.**.**

**8.3.** Ниже приведены примеры индивидуальных задач (контрольных работ) по каждой теме:

1.1. В прилагаемом файле представлены данные о средней заработной плате и населению РФ по регионам на 1 января 2019 год по данным Росстата. Представим ситуацию, что из-за невнимательности операциониста, регионы: Республика Башкортостан, Ханты-Мансийский АО (Югра), Оренбургская область оказались не представлены в итоговой сводке.   
Роль невнимательного операциониста придется исполнить Вам (нужно удалить данные по указанным регионам) и удалить данные по населению, а далее работать уже с новой выборкой, сохранив ее в формат CSV. Определите выборочное среднее заработной платы, определите выборочную медиану заработной платы, определите оценку дисперсии заработной платы, определите оценку среднеквадратического отклонения заработной платы.

1.2. Перед вами результаты наблюдений длительности нахождения человека в очереди в зависимости от количества людей в этой очереди:

№ X Y  
1 6 12  
2 14 23  
3 10 32  
4 16 44  
5 2 5  
6 1 5  
7 21 40  
8 7 15  
9 25 40  
10 12 34

Обучите модель линейной регрессии для прогнозирования и введите указанные параметры: выборочное среднее столбца Х, выборочное среднее столбца Y, коэффициенты θ.

1.3. В прилагаемом файле представлены данные, собранные путем голосования за самые лучшие (или, по крайней мере, самые популярные) конфеты Хэллоуина. Обучите модель логистической регрессии. В качестве предикторов выступают поля: chocolate, fruity, caramel, peanutyalmondy, nougat, crispedricewafer, hard, bar, pluribus, sugarpercent, pricepercent, отклик — Y.

В качестве тренировочного набора данных используйте данные из файла, за иключением следующих конфет: Payday, Rolo, Sixlets. Обучите модель.

Если используете Azure ML Studio, укажите random seed = 2019 в параметрах блока Logistic Regression.

Если используете Python, используйте модель с параметрами: LogisticRegression(random\_state=2019, solver='lbfgs').

Обучите модель и выполните предсказание для всех конфет из прилагаемого файла тестовых данных.

Введите вероятность отнесения конфеты Trolli Sour Bites к классу 1:

Десятичный разделитель точка. Введите ответ с точностью до трех знаков.

Введите вероятность отнесения конфеты Sugar Daddy к классу 1:

Десятичный разделитель точка. Введите ответ с точностью до трех знаков

Выполните оценку модели с помощью матрицы ошибок и рассчитайте следующие параметры при пороге отсечения (Treshhold) 0.5

Введите значение Recall, или TPR для тестового набора данных:

Десятичный разделитель точка. Введите ответ с точностью до трех знаков.

Введите значение Precision для тестового набора данных:

Десятичный разделитель точка. Введите ответ с точностью до трех знаков.

Введите значение AUC для тестового набора данных:

2.1 Знакомьтесь, это Лилия Бримс (или Лиля) - https://vk.com/littlelilly2000. Она совсем не знает, как следует вести себя в Интернете. Попробуем взломать ее страничку (понарошку)?

Какой почтовый ящик использует Лиля?

Формат ответа: username@domain.ru

Для восстановления доступа к почте у Лили установлен секретный вопрос. Какой секретный вопрос использует Лиля?

Введите секретный вопрос без знаков препинания

Как вы думаете, каков ответ на секретный вопрос?

2.2. Иван сдал сессию на отлично и решил отдохнуть как следует на каникулах и отправиться в путешествие. Как настоящий патриот своей страны, он отправился по городам и весям России-матушки, а именно в 214127900401321220212391. Название Иван зашифровал открытым ключом {431,6731}, используя алгоритм шифрования RSA. Введите слово, получившееся в результате дешифровки города закрытым ключом {4895,6731}. Будьте внимательны, Иван был коварен, и перепутал регистр букв. Для кодирования букв была использована таблица ASCII символов из трехзначных кодов, указанная выше, но в результате шифрования коды стали длиной 4 знаков. Не забывайте про регистр при вводе ответа!

2.3. Используя калькулятор уязвимостей CVSS V2, оцените уязвимости по указанным метрикам для ситуаций при следующих условиях.

1. Базовые метрики.

Предполагается получение сетевого доступа, при этом сложность получения доступа оценивается как средняя. Требуется множественная аутентификация. Сильное влияние оказывается только на конфиденциальность информации и частичное - на доступность.

Введите оценку уязвимости:

2. Временные метрики.

Предполагается, что есть концепция использования, исправления недоступны, степень доверия к источнику информации об уязвимости не доказана.

Введите оценку уязвимости:

3. Контекстные метрики.

Вероятность нанесения косвенного ущерба повышенная, плотность целей не определена. При этом высокие требования предъявляются только к обеспечению конфиденциальности и целостности, средние - к доступности.

Введите оценку уязвимости:

2.4. Разделите датасет на тренировочный и тестовый набор данных с параметрами размер тестовой выборки = 0.3, Random seed = 65. Используйте стратифицированное разделение по столбцу class: Stratified split = True, Stratification key column = class. Обучите классификатор Two-Class Boosted Decision Tree при Minimum number of samples per leaf node = 31, Maximum number of leaves per tree = 20, Random number seed = 65, Learning rate = 0.1 и Number of trees constructed = 1 на обучающей выборке и произведите оценку полученной модели на тестовой.

Введите следующие метрики:

Precision

Recall

F-score.

2.5. Используя в качестве исходного набора данных датасет из примера, постройте модель для определения, является ли трафик подозрительным.

1. Используйте подготовленный датасет, содержащий изображения мужчин и женщин.

2. При помощи блока Edit Metadata сделайте столбец, содержащий метку класса (gender), категориальным и укажите, что Fields = Label.

3. Разделите полученный набор данных при помощи блока Split Data на обучающую и тестовую выборки.Доля тестовой выборки = 0.3, Random seed = 17. Используйте стратифицированное разделение по колонке gender (позволит разделить датасет по признаку author в заданной пропорции).

4. Выполните обучение модели двухклассовой классификации при помощи алгоритма логистической регрессии на тренировочных данных и оценку на тестовых.

Введите значение метрики Precision (Macro-averaged):

Введите значение метрики Recall(Macro-averaged):.**.**

**8.4.**  Лекция по каждой теме разделена на некоторое количество фрагментов: 7-12. Каждый фрагмент лекции снабжен обучающим практическим опросом-задачей, помогающим организовывать практическую самостоятельную работу студентов. Задания в опросах выполняются на основе прослушанного в лекции материала в рекомендованном инструменте и не оцениваются. Каждый опрос снабжен подробным решением и разбором всевозможных кейсов на случай, если материалов лекций недостаточно для выполнения задания. Итоговые задания (контрольные работы) содержат задачи, аналогичные тем, что приводятся в опросах**.**

**8.5.**  Процедура оценивания бинарна. В случае, если суммарный процент выполнения упражнений не меньше 50, то результат обучающегося — зачтено. Иначе — не зачтено**.**

**9.Организационно-педагогические условия реализации программы**

**9.1. Кадровое обеспечение программы**

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **№**  **п/п** | **Фамилия, имя, отчество (при наличии)** | **Место основной работы и должность, ученая степень и ученое звание (при наличии)** | **Ссылки на веб-страницы с портфолио (при наличии)** | **Фото в формате jpeg** | **Отметка о полученном согласии на обработку персональных данных** |
| **1** | Михайлова Елена Георгиевна | Университет ИТМО, доцент, к.ф.-м.н., доцент. | https://edu.itmo.ru/teacher/252848/ | Михайлова Елена Георгиевна | **Изображение выглядит как рисунок, стол  Автоматически созданное описание** |
| **2** | Графеева Наталья Генриховна | Университет ИТМО, доцент, к.ф.-м.н., доцент. | https://edu.itmo.ru/teacher/262448/ | Графеева Наталья Генриховна | **Изображение выглядит как рисунок  Автоматически созданное описание** |
| 3 | Егорова Ольга Борисовна | Университет ИТМО, преподаватель, к.ф.н. | https://edu.itmo.ru/teacher/262449/ | Егорова Ольга Борисовна | **Изображение выглядит как текст  Автоматически созданное описание** |
| 4 | Бойцев Антон Александрович | Университет ИТМО, доцент, к.ф.-м.н. | https://edu.itmo.ru/teacher/152625/ | Бойцев Антон Александрович | **Изображение выглядит как текст  Автоматически созданное описание** |
| 5 | Волчек Дмитрий Геннадьевич | Университет ИТМО, доцент, к.т.н. | https://edu.itmo.ru/teacher/143712/ | Волчек Дмитрий Геннадьевич |  |
| 6 | Романов Алексей Андреевич | Университет ИТМО, доцент, к.т.н. | https://edu.itmo.ru/teacher/143758/ | Романов Алексей Андреевич |  |

**9.2.Учебно-методическое обеспечение и информационное сопровождение**

|  |  |
| --- | --- |
| **Учебно-методические материалы** | |
| Методы, формы и технологии | Методические разработки,  материалы курса, учебная литература |
| Занятия лекционного плана | Видео лекций, разбитые на фрагменты, полные тексты лекций |
| Занятия практического плана | Упражнения после каждого фрагмента с подробными решениями и пояснениями, дополнительные материалы |
| Контрольные работы | Контрольные задания |
| Форум онлайн-курса | Форум предназначен для общения как участников, так и преподавателей курса по любым вопросам, касающихся материалов курса |

|  |  |
| --- | --- |
| **Информационное сопровождение** | |
| Электронные  образовательные ресурсы | Электронные  информационные ресурсы |
| https://support.google.com/docs/topic/9054603?hl=ru&ref\_topic=1382883 — основы работы с Google Таблицы | https://www.google.com/intl/ru\_ru/sheets/about/ — програмное обеспечение для работы с таблицами |
| https://docs.microsoft.com/en-us/azure/machine-learning/ — документация Azure ML | https://studio.azureml.net — сервис для обработки и анализа данных |
| https://ru.wikibooks.org/wiki/Синтаксис\_Wolfram\_Alpha — Синтаксис Wolfram Alpha | https://www.wolframalpha.com — база знаний и набор вычислительных алгоритмов |
|  | https://bdu.fstec.ru/calc — Банк данных угроз безопасности информации |

**9.3.Материально-технические условия реализации программы**

|  |  |
| --- | --- |
| Вид занятий | Наименование оборудования,  программного обеспечения |
| Занятия лекционного плана | Компьютер с выходом в сеть Интернет |
| Занятия практического плана | Компьютер с выходом в сеть Интернет |
| Контрольные работы | Компьютер с выходом в сеть Интернет |
| Форум онлайн-курса | Компьютер с выходом в сеть Интернет |

**III.Паспорт компетенций (Приложение 2)**

Описание перечня профессиональных компетенций, качественное изменение которых осуществляется в результате обучения.

Планируемые результаты обучения должны быть определены в виде знаний, умений, навыков и (или) опыта деятельности, характеризующих формирование/развитие компетенции(-й) в области цифровой экономики и представлены в виде Паспорта компетенций в машиночитаемом текстовом формате. Структура паспорта представлена в приложении.

ПАСПОРТ КОМПЕТЕНЦИИ

Методы искусственного интеллекта в кибербезопасности

Университет ИТМО

|  |  |  |  |
| --- | --- | --- | --- |
| 1. | Наименование компетенции | УК.1 Способен осуществлять целенаправленную самостоятельную деятельность по оптимальному удовлетворению индивидуальных и профессиональных информационных потребностей с использованием цифровых технологий и искусственного интеллекта | |
| 2. | Указание типа компетенции | универсальная | |
| 3. | Определение, содержание и основные сущностные характеристики компетенции | Слушатель должен:  знать:   - области применения цифровых технологий в личностной и профессиональной сферах  уметь:  - использовать компьютерную технику и цифровые технологии для автоматизации информационно-аналитической деятельности  владеть:  - аппаратом цифровых технологий для получения, обработки и передачи информации с помощью технических средств и методов | |
| 4. | Дескриптор знаний, умений и навыков по уровням | Уровни сформирован ности компетенции  обучающегося | Индикаторы |
|  | Начальный уровень  (Компетенция недостаточно развита. Частично проявляет навыки, входящие в состав компетенции. Пытается, стремится проявлять нужные навыки, понимает их необходимость, но у него не всегда получается.) | знает: основные области применения цифровых технологий в личностной и профессиональной сферах  умеет: применять простейшие инструменты для поиска, обработки и передачи данных  владеет: базовыми принципами обработки данных предметной области |
|  | Базовый уровень  (Уверенно владеет навыками, способен, проявлять соответствующие навыки в ситуациях с элементами неопределён-ности, сложности.) | знает: информационные потоки и методы их обработки в профессиональной сфере  умеет: отбирать технологии работы с информацией в зависимости от класса задач в области данных  владеет: инструментами и методами обработки и хранения данных в предметной области |
|  | Продвинутый  (Владеет сложными навыками, способен активно влиять на происходящее, проявлять соответствующие навыки в ситуациях повышенной сложности.) | знает: аналитические методы обработки данных  умеет: использовать компьютерную технику и цифровые технологии для автоматизации информационно-аналитической деятельности  владеет: современными инструментами и компьютерными технологиями для решения задач, связанных с обработкой и анализом данных, применительно к любой предметной области. |
|  | Профессиональный  (Владеет сложными навыками, создает новые решения для сложных проблем со многими взаимодействую-щими факторами, предлагает новые идеи и процессы, способен активно влиять на происходящее, проявлять соответствующие навыки  в ситуациях повышенной сложности.) | знает: существующие продвинутые методы работы информационными потоками, области их применения, достоинства и недостатки  умеет: использовать компьютерную технику и цифровые технологии для создания новых подходов к автоматизации информационно-аналитической деятельности  владеет: современными подходами и методами искусственного интеллекта в целом и машинного обучения в частности применительно к задачам профессиональной области |
| 5. | Характеристика взаимосвязи данной компетенции с другими компетенциями/ необходимость владения другими компетенциями для формирования данной компетенции | Компетенция является самодостаточной | |
| 6. | Средства и технологии оценки | Контрольные задания | |

|  |  |  |  |
| --- | --- | --- | --- |
| 1. | Наименование компетенции | ПК.1. Способен получать и использовать знания в области профессиональной деятельности с применением цифровых технологий | |
| 2. | Указание типа компетенции | профессиональная | |
| 3. | Определение, содержание и основные сущностные характеристики компетенции | Слушатель должен:  знать:  - основные типы задач, решаемых в рамках областей машинного обучения и искусственного интеллекта  - основные методы, используемые для решения задач областей машинного обучения и искусственного интеллекта  - аналитические методы обработки данных, основы искусственного интеллекта  - существующие методы работы с данными, области их применения, достоинства и недостатки  уметь:  - применять методы машинного обучения для интерпретации и анализа данных профессиональной области  - отбирать технологии работы с информацией в зависимости от класса задач в области данных  - использовать компьютерную технику и цифровые технологии для автоматизации информационно-аналитической деятельности  владеть:  - методами обработки данных предметной области  - современными инструментами и компьютерными технологиями для решения задач, связанных с обработкой и анализом данных, применительно к любой предметной области.  - современными подходами и методами искусственного интеллекта в целом и машинного обучения в частности применительно к задачам профессиональной области | |
| 4. | Дескриптор знаний, умений и навыков по уровням | Уровни сформирован ности компетенции  обучающегося | Индикаторы |
|  | Начальный уровень  (Компетенция недостаточно развита. Частично проявляет навыки, входящие в состав компетенции. Пытается, стремится проявлять нужные навыки, понимает их необходимость, но у него не всегда получается.) | знает: основные типы задач, решаемых в рамках областей машинного обучения и искусственного интеллекта  умеет: применять простейшие методы машинного обучения для интерпретации и анализа данных профессиональной области  владеет: базовыми принципами обработки данных предметной области |
|  | Базовый уровень  (Уверенно владеет навыками, способен, проявлять соответствующие навыки в ситуациях с элементами неопределён-ности, сложности.) | знает: основные методы, используемые для решения задач областей машинного обучения и искусственного интеллекта  умеет: отбирать технологии работы с информацией в зависимости от класса задач в области данных  владеет: методами обработки данных предметной области |
|  | Продвинутый  (Владеет сложными навыками, способен активно влиять на происходящее, проявлять соответствующие навыки в ситуациях повышенной сложности.) | знает: аналитические методы обработки данных, основы искусственного интеллекта  умеет: использовать компьютерную технику и цифровые технологии для автоматизации информационно-аналитической деятельности  владеет: современными инструментами и компьютерными технологиями для решения задач, связанных с обработкой и анализом данных, применительно к любой предметной области. |
|  | Профессиональный  (Владеет сложными навыками, создает новые решения для сложных проблем со многими взаимодействую-щими факторами, предлагает новые идеи и процессы, способен активно влиять на происходящее, проявлять соответствующие навыки  в ситуациях повышенной сложности.) | знает: существующие продвинутые методы работы с данными, области их применения, достоинства и недостатки  умеет: использовать компьютерную технику и цифровые технологии для создания новых подходов к автоматизации информационно-аналитической деятельности  владеет: современными подходами и методами искусственного интеллекта в целом и машинного обучения в частности применительно к задачам профессиональной области |
| 5. | Характеристика взаимосвязи данной компетенции с другими компетенциями/ необходимость владения другими компетенциями для формирования данной компетенции | Компетенция является самодостаточной | |
| 6. | Средства и технологии оценки | Контрольные задания | |

|  |  |  |  |
| --- | --- | --- | --- |
| 1. | Наименование компетенции | ПК.2. Способен ставить задачи, выполнять и координировать работы по созданию, настройке (адаптации, кастомизации) и сопровождению информационной системы | |
| 2. | Указание типа компетенции | профессиональная | |
| 3. | Определение, содержание и основные сущностные характеристики компетенции | Слушатель должен:  знать:  - особенности информационных потоков в области защиты информации, правовые и этические аспекты распространения информации  - основные цифровые технологии и алгоритмы их работы  - области применения алгоритмов машинного и статистического обучений, искусственного интеллекта для решения прикладных задач  - методы анализа данных для хранения, обработки и эффективного использования полученной информации  уметь:  - планировать аналитические работы в информационно-технологическом проекте  - применять методы статистического анализа данных  - использовать различные инструменты хранения и обработки данных  владеть:  - средствами и информационными технологиями для осуществления интеллектуального анализа данных  - методами описания моделей обрабатываемых данных  - методами концептуального, функционального и логического проектирования систем среднего и крупного масштаба и сложности | |
| 4. | Дескриптор знаний, умений и навыков по уровням | Уровни сформирован ности компетенции  обучающегося | Индикаторы |
|  | Начальный уровень  (Компетенция недостаточно развита. Частично проявляет навыки, входящие в состав компетенции. Пытается, стремится проявлять нужные навыки, понимает их необходимость, но у него не всегда получается.) | знает: базовые цифровые технологии и алгоритмы их работы  умеет: использовать простейшие инструменты для хранения и анализа данных  владеет: основными методами описания моделей обрабатываемых данных |
|  | Базовый уровень  (Уверенно владеет навыками, способен, проявлять соответствующие навыки в ситуациях с элементами неопределён-ности, сложности.) | знает: особенности информационных потоков в области информационной безопасности, правовые и этические аспекты распространения информации  умеет: планировать аналитические работы в информационно-технологическом проекте  владеет: средствами и информационными технологиями для осуществления интеллектуального анализа данных |
|  | Продвинутый  (Владеет сложными навыками, способен активно влиять на происходящее, проявлять соответствующие навыки в ситуациях повышенной сложности.) | знает: области применения алгоритмов машинного и статистического обучений, искусственного интеллекта для решения прикладных задач кибербезопасности  умеет: применять методы статистического анализа данных  владеет: средствами и информационными технологиями для осуществления интеллектуального анализа данных |
|  | Профессиональный  (Владеет сложными навыками, создает новые решения для сложных проблем со многими взаимодействую-щими факторами, предлагает новые идеи и процессы, способен активно влиять на происходящее, проявлять соответствующие навыки  в ситуациях повышенной сложности.) | знает: продвинутые методы анализа данных для хранения, обработки и эффективного использования полученной информации  умеет: использовать различные современные инструменты хранения и обработки данных  владеет: методами концептуального, функционального и логического проектирования систем среднего и крупного масштаба и сложности |
| 5. | Характеристика взаимосвязи данной компетенции с другими компетенциями/ необходимость владения другими компетенциями для формирования данной компетенции | Компетенция является самодостаточной | |
| 6. | Средства и технологии оценки | Контрольные задания | |

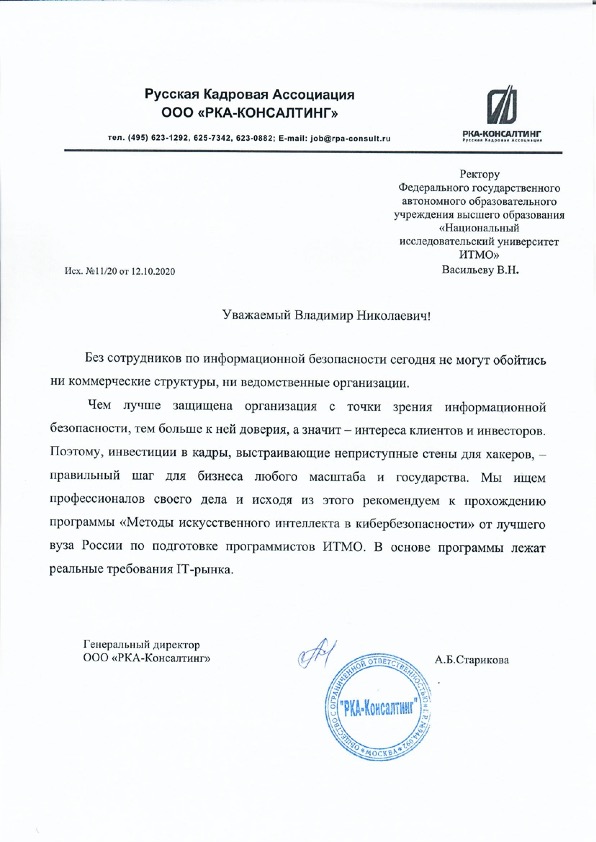
|  |  |  |  |
| --- | --- | --- | --- |
| 1. | Наименование компетенции | ПК.3. Способен взаимодействовать с заказчиком на предмет выяснения первоначальных потребностей | |
| 2. | Указание типа компетенции | профессиональная | |
| 3. | Определение, содержание и основные сущностные характеристики компетенции | Слушатель должен:  знать:  - терминологию и методы, используемые в машинном обучении и искусственном интеллекте, для решения задач обеспечения кибербезопасности  - принципы анализа данных в области защиты информации  - современные тенденции и тренды в инструментах, используемых для анализа данных  уметь:  - проверять корректность построенной модели  - интерпретировать результаты вероятностной классификации  - подбирать приемы первичной обработки данных в зависимости от их структуры  владеть:  - методами исследования зависимостей и закономерностей в данных  - подходами к восстановлению различных статистических зависимостей  - инструментами для осуществления качественного анализа построенной модели | |
| 4. | Дескриптор знаний, умений и навыков по уровням | Уровни сформирован ности компетенции  обучающегося | Индикаторы |
|  | Начальный уровень  (Компетенция недостаточно развита. Частично проявляет навыки, входящие в состав компетенции. Пытается, стремится проявлять нужные навыки, понимает их необходимость, но у него не всегда получается.) | знает: терминологию, используемую в машинном обучении и искусственном интеллекте, для решения задач из области защиты информации  умеет: интерпретировать отклик моделей классификации и регрессии  владеет: простейшими методами исследования зависимостей между переменными |
|  | Базовый уровень  (Уверенно владеет навыками, способен, проявлять соответствующие навыки в ситуациях с элементами неопределён-ности, сложности.) | знает: терминологию и методы, используемые в машинном обучении и искусственном интеллекте, для решения задач обеспечения защиты информации  умеет: проверять корректность построенной модели  владеет: методами исследования зависимостей и закономерностей в данных |
|  | Продвинутый  (Владеет сложными навыками, способен активно влиять на происходящее, проявлять соответствующие навыки в ситуациях повышенной сложности.) | знает: принципы анализа данных разных предметных областей  умеет: интерпретировать результаты вероятностной классификации  владеет: подходами к восстановлению различных статистических зависимостей |
|  | Профессиональный  (Владеет сложными навыками, создает новые решения для сложных проблем со многими взаимодействую-щими факторами, предлагает новые идеи и процессы, способен активно влиять на происходящее, проявлять соответствующие навыки  в ситуациях повышенной сложности.) | знает: современные тенденции и новейшие тренды в инструментах, используемых для анализа данных  умеет: подбирать, использовать и совершенствовать приемы первичной обработки данных в зависимости от их структуры  владеет: инструментами для осуществления качественного анализа построенной модели |
| 5. | Характеристика взаимосвязи данной компетенции с другими компетенциями/ необходимость владения другими компетенциями для формирования данной компетенции | Компетенция является самодостаточной | |
| 6. | Средства и технологии оценки | Контрольные задания | |

|  |  |  |  |
| --- | --- | --- | --- |
| 1. | Наименование компетенции | ПК.4. Способен принимать решения о выборе информационной системы и работе по ее кастомизации, | |
| 2. | Указание типа компетенции | профессиональная | |
| 3. | Определение, содержание и основные сущностные характеристики компетенции | Слушатель должен:  знать:  - приемы анализа сетевого трафика и методы обеспечения идентификации и аутинетификации  - современные инструменты для анализа сетевого трафика и обеспечения идентификации и аутинетификации  - методы оценки качества алгоритмов классификации  уметь:  - выбирать правильный инструмент для работы с данными, передающимися по сети, исходя из особенностей поставленной задачи обеспечения информационной безопасности  - использовать инструменты идентификации и аутинетификации  - кастомизировать настраиваемые параметры инструмента для улучшения качества анализа данных при обеспечении кибербезопасности  владеть:  - широким кругозором как в сфере информационных систем, так и в сфере их адаптации к области защиты информации  - современными инструментами анализа данных, передающихся по сети  - навыками кастомизации информационной системы под задачи кибербезопасности | |
| 4. | Дескриптор знаний, умений и навыков по уровням | Уровни сформирован ности компетенции  обучающегося | Индикаторы |
|  | Начальный уровень  (Компетенция недостаточно развита. Частично проявляет навыки, входящие в состав компетенции. Пытается, стремится проявлять нужные навыки, понимает их необходимость, но у него не всегда получается.) | знает: базовые приемы обработки данных, передающихся по сети  умеет: использовать инструменты обеспечения идентификации и аутинетификации  владеет: некоторыми приемами адаптации информационных систем к области кибербезопасности |
|  | Базовый уровень  (Уверенно владеет навыками, способен, проявлять соответствующие навыки в ситуациях с элементами неопределён-ности, сложности.) | знает: продвинутые методы обработки сетевого трафика  умеет: выбирать правильный инструмент для работы с системами идентификации и аутинетификации, исходя из особенностей предметной области  владеет: широким кругозором как в сфере информационных систем, так и в сфере их адаптации к области информационной безопасности |
|  | Продвинутый  (Владеет сложными навыками, способен активно влиять на происходящее, проявлять соответствующие навыки в ситуациях повышенной сложности.) | знает: современные инструменты для анализа сетевого траффика  умеет: работать с данными, полученными в процессе решения задачи идентификации  владеет: современными инструментами анализа информации, передаваемой по сети |
|  | Профессиональный  (Владеет сложными навыками, создает новые решения для сложных проблем со многими взаимодействую-щими факторами, предлагает новые идеи и процессы, способен активно влиять на происходящее, проявлять соответствующие навыки  в ситуациях повышенной сложности.) | знает: методы оценки качества алгоритмов классификации  умеет: кастомизировать настраиваемые параметры инструмента для улучшения качества анализа данных в области кибербезопасности  владеет: продвинутыми приемами кастомизации информационной системы под задачи обеспечения защиты информации |
| 5. | Характеристика взаимосвязи данной компетенции с другими компетенциями/ необходимость владения другими компетенциями для формирования данной компетенции | Компетенция является самодостаточной | |
| 6. | Средства и технологии оценки | Контрольные задания | |

|  |  |  |  |
| --- | --- | --- | --- |
| 1. | Наименование компетенции | ПК.5. Способен консультировать пользователей кастомизированной информационной системы | |
| 2. | Указание типа компетенции | профессиональная | |
| 3. | Определение, содержание и основные сущностные характеристики компетенции | Слушатель должен:  знать:  - приемы работы в инструментах анализа данных  - современные инструменты анализа данных, а также их особенности применительно к области защиты информации  - особенности применения методов машинного обучения и искусственного интеллекта в различных информационных системах  уметь:  - применять инструменты анализа данных к задачам, решаемым методами машинного обучения и искусственного интеллекта  - настраивать информационные системы под нужды области информационной защиты  - использовать особенности реализации методов машинного обучения и искусственного интеллекта внутри информационной системы для более эффективного решения поставленной задачи  владеть:  - приемами использования информационной системы  - приемами обучения использования информационной системы, настроенной под конкретную предметную область  - методами машинного обучения и искусственного интеллекта, реализованных в информационных системах | |
| 4. | Дескриптор знаний, умений и навыков по уровням | Уровни сформирован ности компетенции  обучающегося | Индикаторы |
|  | Начальный уровень  (Компетенция недостаточно развита. Частично проявляет навыки, входящие в состав компетенции. Пытается, стремится проявлять нужные навыки, понимает их необходимость, но у него не всегда получается.) | знает: базовые приемы работы в инструментах анализа данных  умеет: использовать простейшие информационные системы анализа данных  владеет: начальными приемами использования информационной системы |
|  | Базовый уровень  (Уверенно владеет навыками, способен, проявлять соответствующие навыки в ситуациях с элементами неопределён-ности, сложности.) | знает: продвинутые приемы работы в инструментах анализа данных  умеет: применять инструменты анализа данных к задачам, решаемым методами машинного обучения и искусственного интеллекта  владеет: приемами использования информационной системы |
|  | Продвинутый  (Владеет сложными навыками, способен активно влиять на происходящее, проявлять соответствующие навыки в ситуациях повышенной сложности.) | знает: современные инструменты анализа данных, а также их особенности применительно к области кибербезопасности  умеет: настраивать информационные системы под нужды предметной области  владеет: приемами обучения использования информационной системы, настроенной под конкретную предметную область |
|  | Профессиональный  (Владеет сложными навыками, создает новые решения для сложных проблем со многими взаимодействую-щими факторами, предлагает новые идеи и процессы, способен активно влиять на происходящее, проявлять соответствующие навыки  в ситуациях повышенной сложности.) | знает: особенности применения методов машинного обучения и искусственного интеллекта в различных информационных системах  умеет: использовать особенности реализации методов машинного обучения и искусственного интеллекта внутри информационной системы для более эффективного решения поставленной задачи  владеет: методами машинного обучения и искусственного интеллекта, реализованных в информационных системах |
| 5. | Характеристика взаимосвязи данной компетенции с другими компетенциями/ необходимость владения другими компетенциями для формирования данной компетенции | Компетенция является самодостаточной | |
| 6. | Средства и технологии оценки | Контрольные задания | |

**VI.Иная информация о качестве и востребованности образовательной программы** (результаты профессионально-общественной аккредитации образовательной программы, включение в системы рейтингования, призовые места по результатам проведения конкурсов образовательных программ и др.) (при наличии)

**V.Рекомендаций к программе от работодателей**: наличие не менее двух писем и/или подтверждения на цифровой платформе Государственной системы предоставления ПЦС от работодателей о рекомендации образовательной программы для реализации в рамках Государственной системы предоставления ПЦС на формирование у трудоспособного населения компетенций цифровой экономики с указанием востребованности результатов освоения программы в сфере деятельности соответствующих компаний и готовности к рассмотрению заявок наиболее успешно освоивших образовательную программу граждан на прохождение стажировки и (или) собеседования на предмет трудоустройства путем проставления отметки в профиле программы

****

****

**VI.Указание на возможные сценарии профессиональной траектории граждан** по итогам освоения образовательной программы (в соответствии с приложением)

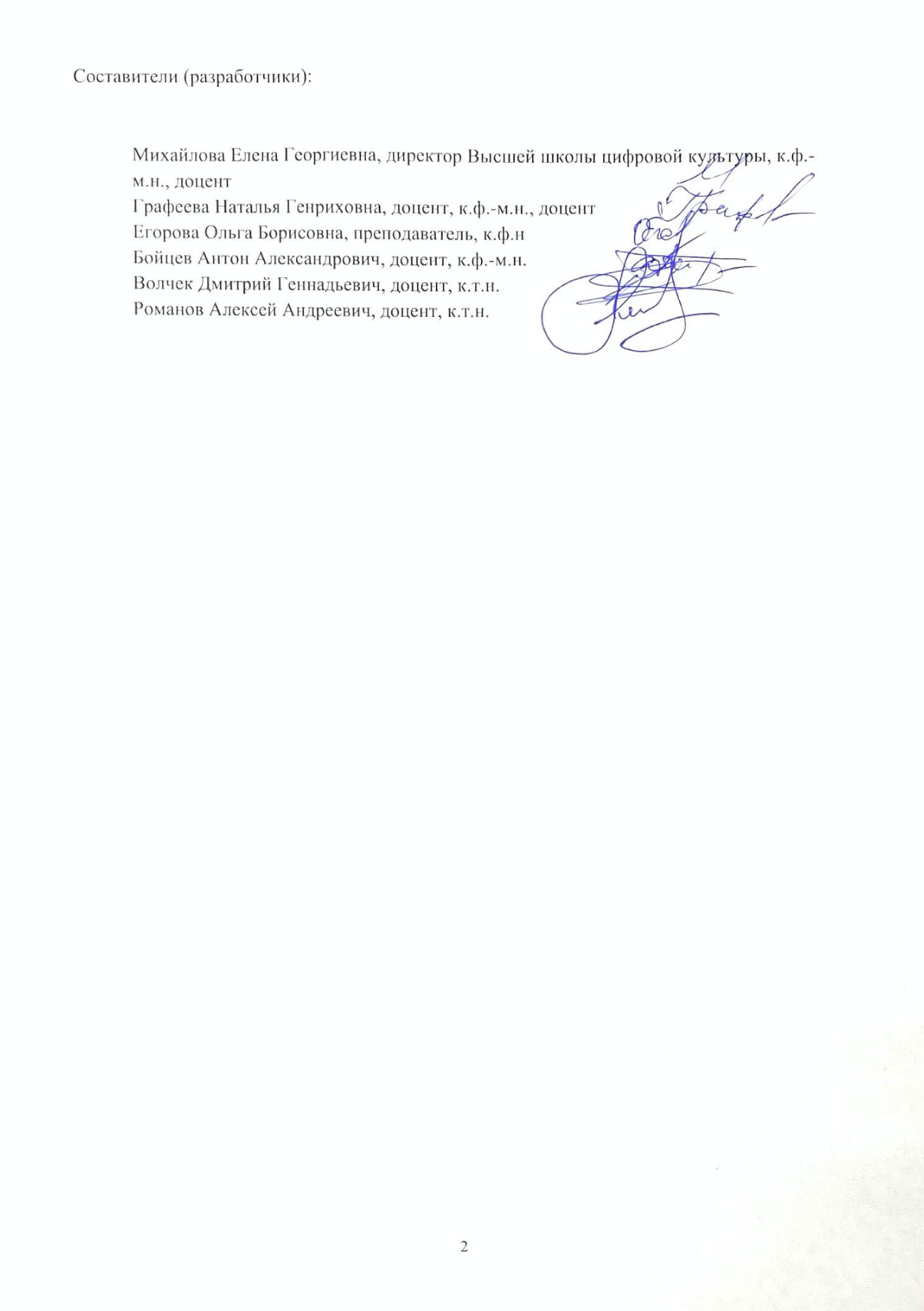
Развитие компетенций в текущей сфере занятости, переход в новую сферу деятельности.

**VII.Дополнительная информация**

**VIII.Приложенные Скан-копии**

Утвержденной рабочей программа (подпись, печать, в формате pdf)





1. ОБЩАЯ ХАРАКТЕРИСТИКА ПРОГРАММЫ

**1.1. Нормативные правовые основания разработки программы**

Нормативную правовую основу разработки программы составляют:

* Федеральный закон от 29 декабря 2012 г. № 273-ФЗ «Об образовании в Российской Федерации»;
* постановление Правительства Российской Федерации от 22 января 2013 г. № 23 «О Правилах разработки, утверждения и применения профессиональных стандартов»;
* приказ Минтруда России от 12 апреля 2013 г. № 148н «Об утверждении уровней квалификаций в целях разработки проектов профессиональных стандартов»;
* приказ Минобрнауки России от 1 июля 2013 г. № 499 «Об утверждении Порядка организации и осуществления образовательной деятельности по дополнительным профессиональным программам»;
* распоряжение Правительства Российской Федерации от 31 марта 2014 г. № 487-р «Об утверждении комплексного плана мероприятий по разработке профессиональных стандартов, их независимой профессионально-общественной экспертизе и применению на 2014 - 2016 годы»;
* рекомендации Минобрнауки России от 22 апреля 2015 г. № ВК-1030/06 «Методические рекомендации-разъяснения по разработке дополнительных профессиональных программ на основе профессиональных стандартов».

**1.2. Характеристика программы**

*Программа посвящена технологиям защиты информации и кибербезопасности. Не секрет, что в современном мире нас окружает огромное количество информации. Сложно представить отрасли современной и тем более цифровой экономики, в которых в той или иной степени не осуществлялась бы работа с большим объемом данных. Эту информацию нужно хранить, обрабатывать, анализировать и, конечно, защищать. Кибербезопасность является неотъемлемой частью современного информационного мира, и проникает чуть ли не во все его сферы, начиная с банальной индивидуальной информационной безопасности (защита персональных данных, противодействие сетевому мошенничеству, защита от спам сообщений и так далее) и заканчивая многоступенчатыми системами корпоративной информационной безопасности, средствами борьбы с ботнетами, противодействием фейкам и тому подобное.*

*Назначение программы обучения – познакомить слушателей с основными направлениями кибербезопасности и показать практические аспекты технологий, позволяющих осуществлять обнаружение различного рода угроз и производить их нейтрализацию. Современные методы защиты информации базируются на алгоритмах машинного обучения, поэтому в рамках курса слушатели сначала узнают, какие задачи решает машинное обучение, познакомятся с методами решении задач обучения с учителем: регрессии и классификации. Второй модуль курса посвящен непосредственному применению рассмотренных методов и алгоритмов в задачах кибербезопасности. В процессе выполнения практических упражнений курса слушатели познакомятся с приемами шифрования информации, калькуляторами угроз безопасности информации, методами предсказания и выявления сетевых атак, настройкой алгоритмов биометрической идентификации посредством платформы Azure ML Studio.*

**1.3. Цель реализации программы**

*Сформировать навыки применения методов машинного обучения в задачах обеспечения кибербезопасности. Формируемые компетенции:*

*УК.1 Способен осуществлять целенаправленную самостоятельную деятельность по оптимальному удовлетворению индивидуальных и профессиональных информационных потребностей с использованием цифровых технологий и искусственного интеллекта*

*ПК.1. Способен получать и использовать знания в области профессиональной деятельности с применением цифровых технологий*

*ПК.2. Способен ставить задачи, выполнять и координировать работы по созданию, настройке (адаптации, кастомизации) и сопровождению информационной системы*

*ПК.3. Способен взаимодействовать с заказчиком на предмет выяснения первоначальных потребностей*

*ПК.4. Способен принимать решения о выборе информационной системы и работе по ее кастомизации*

*ПК.5. Способен консультировать пользователей кастомизированной информационной системы*

**1.4. Требования к слушателям**

* *Высшее или среднее профессиональное образование*
* *Требований к квалификации не предъявляется*
* *Опыт профессиональной деятельности не требуется*
* *Предварительное освоение иных дисциплин не требуется*

**1.5. Планируемые результаты обучения**

*2.1. Знание (осведомленность в областях)*

*2.1.1. Области применения цифровых технологий в личностной и профессиональной сферах*

*2.1.2. Основные типы задач, решаемых в рамках областей машинного обучения и искусственного интеллекта*

*2.1.3. Основные методы, используемые для решения задач областей машинного обучения и искусственного интеллекта*

*2.1.4. Аналитические методы обработки данных, основы искусственного интеллекта*

*2.1.5. Существующие методы работы с данными, области их применения, достоинства и недостатки*

*2.1.6. Особенности информационных потоков в своей профессиональной области, правовые и этические аспекты распространения информации*

*2.1.7. Основные цифровые технологии и алгоритмы их работы*

*2.1.8. Области применения алгоритмов машинного и статистического обучений, искусственного интеллекта для решения прикладных задач*

*2.1.9. Методы анализа данных для хранения, обработки и эффективного использования полученной информации*

*2.1.10. Терминологию и методы, используемые в машинном обучении и искусственном интеллекте, для решения задач кибербезопасности*

*2.1.11. Принципы анализа данных из области кибербезопасности*

*2.1.12. Современные тенденции и тренды в инструментах, используемых для защиты информации*

*2.1.13. Методы и алгоритмы шифрования информации*

*2.1.14. Современные инструменты, применяемые в сфере обеспечения информационной безопасности*

*2.1.15. Методы оценки качества алгоритмов классификации*

*2.1.16. Приемы работы в инструментах анализа данных*

*2.1.17. Современные инструменты анализа данных, а также их особенности применительно к сфере кибербезопасности*

*2.1.18. Особенности применения методов машинного обучения и искусственного интеллекта в различных информационных системах*

*2.2. Умение (способность к деятельности)*

*2.2.1. Использовать компьютерную технику и цифровые технологии для автоматизации информационно-аналитической деятельности*

*применять методы машинного обучения для интерпретации и анализа данных из области информационной безопасности*

*2.2.2. Отбирать технологии работы с информацией в зависимости от класса задач в области защиты данных*

*2.2.3. Использовать компьютерную технику и цифровые технологии для автоматизации информационно-аналитической деятельности*

*2.2.4. Планировать аналитические работы в информационно-технологическом проекте*

*2.2.5. Применять методы статистического анализа данных*

*2.2.6. Использовать различные инструменты хранения и обработки данных*

*2.2.7. Проверять корректность построенной модели*

*2.2.8. Интерпретировать результаты вероятностной классификации*

*2.2.9. Подбирать приемы первичной обработки данных в зависимости от их структуры*

*2.2.10. Использовать инструменты оценки уровня информационных угроз*

*2.2.11. Применять алгоритмы шифрования и дешифрования информации*

*2.2.12. Кастомизировать настраиваемые параметры инструмента для улучшения качества анализа данных предметной области*

*2.2.13. Применять инструменты анализа данных к задачам, решаемым методами машинного обучения и искусственного интеллекта*

*2.2.14. Настраивать информационные системы под нужды предметной области*

*2.2.15. Использовать особенности реализации методов машинного обучения и искусственного интеллекта внутри информационной системы для более эффективного решения поставленной задачи*

*2.3. Навыки (использование конкретных инструментов)*

*Инструменты: электронные таблицы, Azure ML Studio, WolframAlpha, Калькулятор уязвимостей*

*2.3.1 Владеть аппаратом цифровых технологий для получения, обработки и передачи информации с помощью технических средств и методов*

*2.3.2 Владеть методами обработки данных предметной области*

*2.3.3 Владеть современными инструментами и компьютерными технологиями для решения задач, связанных с обработкой и анализом данных, применительно к любой предметной области.*

*2.3.4 Владеть современными подходами и методами искусственного интеллекта в целом и машинного обучения в частности применительно к задачам обеспечения информационной безопасности, средствами и информационными технологиями для осуществления интеллектуального анализа данных*

*2.3.5 Владеть методами описания моделей обрабатываемых данных*

*2.3.6 Владеть методами концептуального, функционального и логического проектирования систем среднего и крупного масштаба и сложности — методами исследования зависимостей и закономерностей в данных*

*2.3.7 Владеть подходами к восстановлению различных статистических зависимостей*

*2.3.8 Владеть инструментами для осуществления качественного анализа построенной модели — широким кругозором как в сфере информационных систем, так и в сфере их адаптации к области обеспечения кибербезопасности*

*2.3.9 Владеть современными инструментами обнаружения аномалий и атак в сетевом трафике, а также идентификации и биометрии*

*2.3.10 Владеть навыками кастомизации информационной системы под задачи предметной области, приемами использования информационной системы*

*2.3.11 Владеть приемами обучения использования информационной системы, настроенной под конкретную предметную область*

*2.3.12 Владеть методами машинного обучения и искусственного интеллекта, реализованных в информационных системах*

**1.6. Формы освоения программы**

*Форма обучения — заочная, с применением электронного обучения, дистанционных образовательных технологий.*

**1.7. Трудоемкость программы**

*72 часа*

*.*

**2. СОДЕРЖАНИЕ ПРОГРАММЫ**

**2.1. Формат и структура программы**

*Режим обучения дистанционный, с помощью разработанного онлайн курса. Предполагается изучение материалов лекций, выполнение заданий самопроверки и оцениваемых упражнений. Зачет за дисциплину ставится в случае, когда суммарный балл за верно выполненные упражнения оказывается не меньше 50% от максимально возможного суммарного балла.*

**2.2. Учебный (учебно-тематический) план**

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| **№ п/п** | **Модуль / Тема** | **Всего, час** | **Виды учебных занятий** | | | **Формы контроля** |
| **лекции** | **практические занятия** | **самостоятельная работа** |
| 1 | Методы машинного обучения | 26 | 8 | 8  Обучающие практические задания | 10  Практические контрольные работы |  |
| 1.1 | Введение в машинное обучение | 8 | 2 | 2  Обучающие практические задания | 4  Практическая контрольная работа | Опросы, итоговое упражнение |
| 1.2 | Задача регрессии | 8 | 3 | 3  Обучающие практические задания | 2  Практическая контрольная работа | Опросы, итоговое упражнение |
| 1.3 | Задача классификации: вероятностный подход | 10 | 3 | 3  Обучающие практические задания | 4  Практическая контрольная работа | Опросы, итоговое упражнение |
| 2 | Искусственный интеллект в задачах кибербезопасности | 46 | 14 | 14  Обучающие практические задания | 18  Практические контрольные работы |  |
| 2.1 | Основы персональной информационной безопасности | 8 | 3 | 3  Обучающие практические задания | 2  Практическая контрольная работа | Опросы, итоговое упражнение |
| 2.2 | Введение в информационную безопасность | 8 | 3 | 3  Обучающие практические задания | 2  Практическая контрольная работа | Опросы, итоговое упражнение |
| 2.3 | Искусственный интеллект в задачах информационной безопасности | 10 | 3 | 3  Обучающие практические задания | 4  Практическая контрольная работа | Опросы, итоговое упражнение |
| 2.4 | Обнаружение аномалий и атак в сетевом трафике | 10 | 2 | 2  Обучающие практические задания | 6  Практическая контрольная работа | Опросы, итоговое упражнение |
| 2.5 | Идентификация. Биометрия | 10 | 3 | 3  Обучающие практические задания | 4  Практическая контрольная работа | Опросы, итоговое упражнение |

**2.3. Рабочая программа курса**

*Модуль 1. Методы машинного обучения (26 час.)*

*Тема 1.1 Введение в машинное обучение (8 час.)*

*Рассматриваются основные задачи, ветки и методы машинного обучения, а также необходимый для дальнейшего аппарат статистики.*

*Тема 1.2 Задача регрессии (8 час.)*

*Рассматриваются модели простейшей и множественной регрессии. Дается представление о полиномиальной регрессии.*

*Тема 1.3 Задача классификации: вероятностный подход (10 час.)*

*Рассматривается вероятностный подход к решению задачи классификации на примере наивного байесовского классификатора и его обобщений.*

*Модуль 2. Прикладные задачи искусственного интеллекта (46 час.)*

*Тема 2.1. Основы персональной информационной безопасности (8 час.)*

*Рассматриваются основы персональной информационной безопасности, вредоносное ПО, парольные системы.*

*Тема 2.2 Введение в информационную безопасность (8 час.)*

*Рассматриваются симметричные системы шифрования, несимметричная криптография, алгоритм шифрования RSA и Эль-Гамаля, электронная подпись.*

*Тема 2.3 Искусственный интеллект в задачах информационной безопасности (10 час.)*

*Рассматриваются базовые понятия информационной безопасности, методы защиты информации. Роль ИИ в кибербезопасности, оценка алгоритмов машинного обучения.*

*Тема 2.4 Обнаружение аномалий и атак в сетевом трафике (10 час.)*

*Рассматривается применение МО для обнаружения сетевых атак и аномалий, межсетевые экраны и системы обнаружения вторжений.*

*Тема 2.5 Идентификация. Биометрия (10 час.)*

*Рассматриваются основы биометрии, виды аутентификации и задача отбора признаков. Состязательные атаки на биометрические системы.*

**2.4. Требования к знаниям и умениям перед началом изучения программы**

*Базовые знания цифровой культуры*

**3. ТРЕБОВАНИЯ К ИТОГОВОЙ АТТЕСТАЦИИ**

**3.1. Форма аттестации**

*Оценивание результатов обучения производится следующим образом. По каждой теме обучающимся выдаются индивидуальные задачи (контрольная работа). Задачи включают в себя некоторое количество (1-20) заданий. Задание выполняется обучающимся при помощи сети Интернет и инструментов, рассматриваемых в лекции. Срок выполнения – согласно указанным срокам обучения. Для ввода ответа на задания дается от двух до десяти попыток. Подпункты задачи оцениваются равномерно. Если в задаче N полей ввода, то каждое оценивается согласно формуле 12,5/N. Итого, максимально возможный балл за задачу равен 12,5.*

*Процедура оценивания бинарна. В случае, если суммарный балл за верно выполненные упражнения оказывается не меньше 50% от максимально возможного суммарного балла, то результат обучающегося — зачтено. Иначе — не зачтено.*

**3.2. Виды и формы аттестации**

|  |  |  |  |
| --- | --- | --- | --- |
|  | **Номер темы/модуля** | **Наименование практического занятия** | **Описание** |
| **1.1** | Введение в машинное обучение | Основы работы в Azure ML Studio | Рассматриваются популярные инструменты как для работы с методами машинного обучения, так и для решения прикладных задач с их помощью |
| **1.2** | Задача регрессии | Построение модели регрессии | Рассматриваются методы построения регрессионных моделей по данному тренировочному набору данных |
| 1.3 | Задача классификации: вероятностный подход | Решение задачи классификации алгоритмом логистической регрессии | Рассматривается применение алгоритма логистической регрессии для решения задачи классификации |
| 2.1 | Основы персональной информационной безопасности | Моделирование атаки на страницу пользователя в социальной сети. Хэширование и дехэширование паролей. | Рассматривается применение методов социального инжиниринга, также методы хэширования информации. |
| 2.2 | Введение в информационную безопасность | Шифрование текстовых данных с использованием ключей, посредством алгоритма RSA | Рассматривается шифрование текстовых данных с использованием таблицы символов ASCII, открытых и закрытых ключей посредством алгоритма RSA. Дешифрование зашифрованной информации |
| 2.3 | Искусственный интеллект в задачах информационной безопасности | Оценка уровня информационных угроз | Рассматриваются методы оценки уязвимостей по базовым, временным и контекстным метрикам для моделируемых ситуаций при помощи калькуляторов уязвимостей. |
| 2.4 | Обнаружение аномалий и атак в сетевом трафике | Классификация траффика | Рассматривается построение классификатора на основе алгоритма логистической регрессии, способного отличать подозрительный трафик от нормального. |
| 2.5 | Идентификация. Биометрия | Моделирование систем биометрической и идентификации | Рассматривается применение алгоритма логистической регрессии для решения задачи идентификации |

**4. УЧЕБНО-МЕТОДИЧЕСКОЕ ОБЕСПЕЧЕНИЕ ПРОГРАММЫ**

**4.1. Информационное сопровождение**

|  |  |
| --- | --- |
| **Информационное сопровождение** | |
| Электронные  образовательные ресурсы | Электронные  информационные ресурсы |
| https://support.google.com/docs/topic/9054603?hl=ru&ref\_topic=1382883 — основы работы с Google Таблицы | https://www.google.com/intl/ru\_ru/sheets/about/ — програмное обеспечение для работы с таблицами |
| https://docs.microsoft.com/en-us/azure/machine-learning/ — документация Azure ML | https://studio.azureml.net — сервис для обработки и анализа данных |
| https://ru.wikibooks.org/wiki/Синтаксис\_Wolfram\_Alpha — Синтаксис Wolfram Alpha | https://www.wolframalpha.com — база знаний и набор вычислительных алгоритмов |
|  | https://bdu.fstec.ru/calc — Банк данных угроз безопасности информации |

**5. МАТЕРИАЛЬНО-ТЕХНИЧЕСКОЕ ОБЕСПЕЧЕНИЕ УЧЕБНОГО ПРОЦЕССА**

**5.1. Требования к оборудованию**

|  |  |
| --- | --- |
| Вид занятий | Наименование оборудования,  программного обеспечения |
| Занятия лекционного плана | Компьютер с выходом в сеть Интернет |
| Занятия практического плана | Компьютер с выходом в сеть Интернет |
| Контрольные работы | Компьютер с выходом в сеть Интернет |
| Форум онлайн-курса | Компьютер с выходом в сеть Интернет |

**5.2. Требования к программным средствам**

*Не предъявляются*