По умолчанию для Доверенный искусственный интеллект (09.04.01, 2021)/Проверка остаточных знаний (ПК 31.1)

1. **Целостность инновационного цикла – это …**
    a. недопустимость использования искусственного интеллекта в целях умышленного причинения вреда гражданам и юридическим лицам, а также предупреждение и минимизация рисков возникновения негативных последствий использования технологий искусственного интеллекта
    b. осуществление и адаптация в приоритетном порядке существующих мер, направленных на реализацию государственной политики в научно-технической и других областях
    c. обеспечение тесного взаимодействия научных исследований и разработок в области искусственного интеллекта с реальным сектором экономики

    Вопрос 1 (Множественный выбор / Только один ответ)

---

2. **Субхарактеристикой сопровождаемости ИИ (в соответствии с ГОСТ Р 59276-2020) является:**
    a. изучаемость
    b. тестируемость
    c. стабильность

    Вопрос 10 (Множественный выбор / Только один ответ)

---

3. **Примерами непреднамеренного снижения качества систем ИИ являются:**
    a. использование статистически смещенной обучающей выборки, приводящей к появлению «предвзятостей» в результатах работы системы ИИ
    b. отравление данных
    c. отсутствие достоверных и представительных оценок устойчивости системы распознавания изображений к воздействию преднамеренных «состязательных» атак, приводящее к неустойчивой работе системы в процессе ее эксплуатации

    Вопрос 11 (Множественный выбор / Только один ответ)

---

4. **Что позволит устранить статистическую смещенность обучающей выборки, способной привести к предвзятости (необъективности) результатов работы системы в соответствии с ГОСТ Р 59276-2020?**
    a. разработка оптимальной модели данных
    b. кросс-валидация выборки, полученной при разметке данных людьми
    c. соблюдение допустимой области применения системы ИИ

    Вопрос 12 (Множественный выбор / Только один ответ)

---

5. **Что такое инфраструктурный уровень архитектуры в системах ИИ соответствии с ГОСТ Р 59276-2020?**
    a. уровень, включающий аппаратные средства хранения, обработки и передачи информации, включая облачную инфраструктуру, а также системное ПО

b. уровень сенсоров и исполнительных устройств систем ИИ, благодаря которым система осуществляет физическое взаимодействие с окружающей средой и объектами
c. уровень прикладного ПО, реализующего алгоритмы интеллектуальной обработки данных

Вопрос 13 (Множественный выбор / Только один ответ)

---

6. Методика заключения модели в защищенную среду и ее обучение без перемещения данных куда-либо - это ...

a. федеративное обучение
b. централизованное обучение
c. автономное обучение

Вопрос 14 (Множественный выбор / Только один ответ)

---

7. Манипуляция, при которой целенаправленно заложенная на этапе обучения ошибка в обучающих данных, заставляет модель принимать неверные (деструктивные) решения в будущем

a. извлечение данных
b. отравление данных
c. обезличивание данных

Вопрос 15 (Множественный выбор / Только один ответ)

---

8. Форма шифрования, позволяющая производить определённые математические действия с зашифрованным текстом и получать зашифрованный результат, который соответствует результату операций, выполненных с открытым текстом

a. функциональное
b. классическое
c. гомоморфное

Вопрос 16 (Множественный выбор / Только один ответ)

---

9. Потеря конфиденциальных данных отдельных лиц, когда их личная информация используется для создания набора данных. Система публичного обмена информацией о наборе данных (статистическими данными, общими шаблонами, присутствующими в данных и др.) при сокрытии конфиденциальных данных, на основе которых эта информация была получена

a. интегральная конфиденциальность
b. непрерывная конфиденциальность
c. дифференциальная конфиденциальность

Вопрос 17 (Множественный выбор / Только один ответ)

---

10. Что такое физический уровень архитектуры в системах ИИ соответствии с ГОСТ Р 59276-2020?

a. уровень, включающий аппаратные средства хранения, обработки и передачи информации, включая облачную инфраструктуру, а также системное ПО
b. уровень сенсоров и исполнительных устройств систем ИИ, благодаря которым система осуществляет физическое взаимодействие с окружающей средой и объектами

c. уровень прикладного ПО, реализующего алгоритмы интеллектуальной обработки данных

Вопрос 18 (Множественный выбор / Только один ответ)

---

11. Что такое прикладной уровень архитектуры в системах ИИ соответствии с ГОСТ Р 59276-2020?

a. уровень, включающий аппаратные средства хранения, обработки и передачи информации, включая облачную инфраструктуру, а также системное ПО
b. уровень сенсоров и исполнительных устройств систем ИИ, благодаря которым система осуществляет физическое взаимодействие с окружающей средой и объектами
c. уровень прикладного ПО, реализующего алгоритмы интеллектуальной обработки данных

Вопрос 19 (Множественный выбор / Только один ответ)

---

12. В соответствии с Национальной стратегией развития искусственного интеллекта на период до 2030 год, какой принцип описывается следующим тезисом: «набор алгоритмов, предназначенных для разработки технологических решений на основе ИИ, описанных с использованием языков программирования и размещенных в сети "Интернет"»?

a. открытая библиотека искусственного интеллекта
b. общедоступная платформа
c. вычислительная система

Вопрос 2 (Множественный выбор / Только один ответ)

---

13. К обучению без учителя относится задача

a. регрессии
b. кластеризации
c. классификации

Вопрос 20 (Множественный выбор / Только один ответ)

---

14. К обучению с учителем относится задача

a. детерминации
b. кластеризации
c. классификации

Вопрос 21 (Множественный выбор / Только один ответ)

---

15. Биометрический образ злоумышленника, пытающегося преодолеть биометрическую защиту - это ...

a. биометрический образ "Все чужие"
b. биометрический образ "Чужой"
c. биометрический образ "Свой"

Вопрос 22 (Множественный выбор / Только один ответ)

---

16. **С какой проблемой связывают сезонные изменения данных и связанное с этим ухудшение прогностической способности модели?**
    a. дрейф данных
    b. миграция данных
    c. утечка данных

Вопрос 23 (Множественный выбор / Только один ответ)

---

17. **С какой проблемой связывают резкое или постепенное изменение данных (например, в связи с обвалом рынка или медленным изменением предпочтений клиентов) и связанное с этим ухудшение прогностической способности модели?**
    a. дрейф данных
    b. дрейф концепций
    c. повреждение параметров или знаний модели

Вопрос 24 (Множественный выбор / Только один ответ)

---

18. **Какой из принципов Национального кодекса этики в сфере ИИ гарантирует соблюдение законодательства РФ в области ПДн при использовании СИИ, обеспечивать охрану и защиту ПДн, обработка которых осуществляется СИИ или Акторами?**
    a. безопасность работы с данными
    b. подконтрольность
    c. поднадзорность

Вопрос 25 (Множественный выбор / Только один ответ)

---

19. **В человеко-ориентированном и гуманистическом подходе Национального кодекса этики в сфере ИИ:**
    a. когда деятельность Акторов ИИ может привести к морально неприемлемому вреду, наступление которого соответствующий Актор ИИ может разумно предположить в конкретных обстоятельствах, им должны быть приняты меры, чтобы предотвратить или ограничить этот вред
    b. уровень внимания к этическим вопросам в области ИИ должен определяться в соответствии с оценкой уровня рисков, создаваемых конкретными технологиями и системами ИИ для интересов человека и общества
    c. человек рассматривается как наивысшая ценность; технологии и СИИ должны способствовать реализации всех потенциальных возможностей человека для достижения гармонии в социальной, экономической, духовной сфере и наивысшего расцвета личности

Вопрос 26 (Множественный выбор / Только один ответ)

---

20. **Как называется программный продукт, который ориентирован в первую очередь на управление и управление жизненным циклом широкого спектра оперативных моделей искусственного интеллекта и принятия решений, включая машинное обучение, графы знаний, правила, оптимизацию, лингвистические и агент-ориентированные модели?**
    a. ModelOps
    b. MLOps
    c. DevOps

Вопрос 27 (Множественный выбор / Только один ответ)

---

21. **Какой тип алгоритмов можно отнести к автоматическому машинному обучению?**
    a. оптимизация гиперпараметров алгоритма обучения или модели
    b. автоматическое распознавание образов
    c. замена решений человека решениями искусственного интеллекта

Вопрос 28 (Множественный выбор / Только один ответ)

---

22. **Глубокие нейронные сети обладают**
    a. высоким уровнем объяснимости
    b. высоким уровнем робастности обучения
    c. высокими требованиями к обучающей выборке и ее объему

Вопрос 29 (Множественный выбор / Только один ответ)

---

23. **К какому этапу жизненного цикла ИИ относится поиск и исправление логических ошибок в исходных текстах на контрольных примерах?**
    a. разработка алгоритмов обработки данных
    b. опытная эксплуатация
    c. отладка системы

Вопрос 3 (Множественный выбор / Только один ответ)

---

24. **Чем больше слоев нейронной сети, ...**
    a. тем выше риск переобучения
    b. тем ниже риск переобучения
    c. тем выше робастность

Вопрос 30 (Множественный выбор / Только один ответ)

---

25. **К какому этапу жизненного цикла ИИ относится обоснование выбора математической модели по критериям или обоснование необходимости разработки новой модели?**
    a. разработка теоретических основ системы
    b. детальная разработка структур входных, промежуточных и выходных данных
    c. эксплуатация

Вопрос 4 (Множественный выбор / Только один ответ)

---

26. **Подход ИИ, как автоматическое рассуждение, включает:**
    a. глубокое обучение и обучение с подкреплением
    b. интернет вещей и робототехника
    c. планирование, диспетчеризацию, представление знаний, поиск и оптимизацию

Вопрос 5 (Множественный выбор / Только один ответ)

---

27. **Сильный (общий) искусственный интеллект (в соответствии с ГОСТ Р 59276-2020) – это ...**
    a. способность экспертной системы имитировать когнитивные функции человека и получать при выполнении конкретных практически значимых задач обработки

данных результаты, сопоставимые, как минимум, с результатами интеллектуальной деятельности человека
b. способность технической системы, подобно человеку, мыслить, взаимодействовать, адаптироваться к изменяющимся условиям и решать другие задачи в области обработки информации, ассоциирующиеся с естественным интеллектом человека
c. упорядоченная последовательность инструкций (кодов) для вычислительного средства, находящаяся в памяти этого средства и представляющая собой описание алгоритма управления вычислительными средствами и действий с данными

Вопрос 6 (Множественный выбор / Только один ответ)

---

28. **Свойство системы искусственного интеллекта, заключающееся в принятии ошибочных решений, связанных со статистической смещенностью обучающей выборки исходных данных (в соответствии с ГОСТ Р 59276-2020) – это ...**
    a. предсказуемость (predictability)
    b. понятность (transparency)
    c. предвзятость, необъективность (bias)

Вопрос 7 (Множественный выбор / Только один ответ)

---

29. **Функциональными характеристиками для систем распознавания речи являются?**
    a. фонемы и слога
    b. величина уровня пословной ошибки, фактор реального времени преобразования речи в текст на конкретном сервере обработки данных и другие характеристики
    c. вероятность дорожно-транспортного происшествия при автономном управлении, уровень комфорта управления движением для пассажиров

Вопрос 8 (Множественный выбор / Только один ответ)

---

30. **Субхарактеристикой надежности ИИ (в соответствии с ГОСТ Р 59276-2020) является:**
    a. понятность
    b. анализируемость
    c. устойчивость к ошибке

Вопрос 9 (Множественный выбор / Только один ответ)

По умолчанию для Доверенный искусственный интеллект (09.04.01, 2021)/1. Проблемы доверия искусственному интеллекту

1. **В соответствии с Национальной стратегией развития искусственного интеллекта на период до 2030 год, какой принцип описывается следующим тезисом: «объяснимость работы ИИ и процесса достижения им результатов, недискриминационный доступ пользователей продуктов, которые созданы с использованием технологий ИИ, к информации о применяемых в этих продуктах алгоритмах работы искусственного интеллекта»?**
    a. технологический суверенитет
    b. безопасность
    c. прозрачность

Вопрос 1 (Множественный выбор / Только один ответ)

---

2. **Примерами непреднамеренного снижения качества систем ИИ являются**
   a. использование статистически смещенной обучающей выборки, приводящей к появлению «предвзятостей» в результатах работы системы ИИ
   b. отравление данных
   c. отсутствие достоверных и представительных оценок устойчивости системы распознавания изображений к воздействию преднамеренных «состязательных» атак, приводящее к неустойчивой работе системы в процессе ее эксплуатации

Вопрос 10 (Множественный выбор / Только один ответ)

---

3. **Свойство объекта сохранять во времени способность выполнять требуемые функции в заданных режимах и условиях применения, технического обслуживания, хранения и транспортирования (в соответствии с ГОСТ Р 59276-2020) – это ...**
   a. надежность
   b. понятность
   c. предсказуемость

Вопрос 11 (Множественный выбор / Только один ответ)

---

4. **Что позволит устранить статистическую смещенность обучающей выборки, способной привести к предвзятости (необъективности) результатов работы системы в соответствии с ГОСТ Р 59276-2020?**
   a. разработка оптимальной модели данных
   b. кросс-валидация выборки, полученной при разметке данных людьми
   c. соблюдение допустимой области применения системы ИИ

Вопрос 12 (Множественный выбор / Только один ответ)

---

5. **Методика заключения модели в защищенную среду и ее обучение без перемещения данных куда-либо – это ...**
   a. федеративное обучение
   b. централизованное обучение
   c. автономное обучение

Вопрос 13 (Множественный выбор / Только один ответ)

---

6. **Сильный (общий) искусственный интеллект (в соответствии с ГОСТ Р 59276-2020) – это ...**
   a. способность экспертной системы имитировать когнитивные функции человека и получать при выполнении конкретных практически значимых задач обработки данных результаты, сопоставимые, как минимум, с результатами интеллектуальной деятельности человека
   b. способность технической системы, подобно человеку, мыслить, взаимодействовать, адаптироваться к изменяющимся условиям и решать другие задачи в области обработки информации, ассоциирующиеся с естественным интеллектом человека
   c. упорядоченная последовательность инструкций (кодов) для вычислительного средства, находящаяся в памяти этого средства и представляющая собой описание алгоритма управления вычислительными средствами и действий с данными

Вопрос 14 (Множественный выбор / Только один ответ)

---

7. Потеря конфиденциальных данных отдельных лиц, когда их личная информация используется для создания набора данных. Система публичного обмена информацией о наборе данных (статистическими данными, общими шаблонами, присутствующими в данных и др.) при сокрытии конфиденциальных данных, на основе которых эта информация была получена

a. интегральная конфиденциальность
b. непрерывная конфиденциальность
c. дифференциальная конфиденциальность

Вопрос 15 (Множественный выбор / Только один ответ)

---

8. С какой проблемой связывают сезонные изменения данных и связанное с этим ухудшение прогностической способности модели?

a. дрейф данных
b. миграция данных
c. утечка данных

Вопрос 16 (Множественный выбор / Только один ответ)

---

9. С какой проблемой связывают резкое или постепенное изменение данных (например, в связи с обвалом рынка или медленным изменением предпочтений клиентов) и связанное с этим ухудшение прогностической способности модели?

a. дрейф данных
b. дрейф концепций
c. повреждение параметров или знаний модели

Вопрос 17 (Множественный выбор / Только один ответ)

---

10. Какой из принципов Национального кодекса этики в сфере ИИ гарантирует соблюдение законодательства РФ в области ПДн при использовании СИИ, обеспечивать охрану и защиту ПДн, обработка которых осуществляется СИИ или Акторами?

a. безопасность работы с данными
b. подконтрольность
c. поднадзорность

Вопрос 18 (Множественный выбор / Только один ответ)

---

11. Свойство системы искусственного интеллекта, заключающееся в способности принимать решения ожидаемым (естественным, приемлемым) для человека способом

a. предсказуемость
b. необъективность
c. объяснимость

Вопрос 19 (Множественный выбор / Только один ответ)

---

12. Объяснимый искусственный интеллект – это ...

a. обеспечение защиты гарантированных российским и международным законодательством прав и свобод человека, в том числе права на труд, и предоставление гражданам возможности получать знания и приобретать навыки для успешной адаптации к условиям цифровой экономики
b. развитие рыночных отношений и недопустимость действий, направленных на ограничение конкуренции между российскими организациями, осуществляющими деятельность в области искусственного интеллекта
c. вариант машинного обучения, при котором в алгоритмы ИИ встраивается способ сообщать о выполненных шагах и об основаниях для выбора определенной конкретной рекомендации или результата

Вопрос 2 (Множественный выбор / Только один ответ)

---

13. Какой вид объяснимости ИИ можно отнести к принципам работы деревьев решений?

a. определение важности признаков, информативности данных
b. объяснение причинно-следственных связей решений, их интерпретируемость
c. определение предвзятости решений ИИ, соответствия моделей или данных этическим нормам

Вопрос 20 (Множественный выбор / Только один ответ)

---

14. В соответствии с Национальной стратегией развития искусственного интеллекта на период до 2030 год, какой принцип описывается следующим тезисом: «набор алгоритмов, предназначенных для разработки технологических решений на основе ИИ, описанных с использованием языков программирования и размещенных в сети "Интернет"»?

a. общедоступная платформа
b. открытая библиотека искусственного интеллекта
c. вычислительная система

Вопрос 3 (Множественный выбор / Только один ответ)

---

15. Под объяснимостью моделей ИИ (в соответствии с ГОСТ Р 59276-2020) понимается:

a. открытость для общественности информации, касающейся исследования, проектирования, создания, развертывания и применения системы
b. свойство системы искусственного интеллекта, заключающееся в возможности представления причин, приводящих к тому или иному решению системы, в виде, понятном человеку
c. обеспечение уважения, защита и поощрение неприкосновенности частной жизни – права, имеющего важнейшее значение с точки зрения защиты человеческого достоинства и свободы выбора

Вопрос 4 (Множественный выбор / Только один ответ)

---

16. Свойство системы искусственного интеллекта, заключающееся в принятии ошибочных решений, связанных со статистической смещенностью обучающей выборки исходных данных (в соответствии с ГОСТ Р 59276-2020) – это ...

a. предсказуемость (predictability)
b. понятность (transparency)
c. предвзятость, необъективность (bias)

Вопрос 5 (Множественный выбор / Только один ответ)

17. **Субхарактеристикой надежности ИИ (в соответствии с ГОСТ Р 59276-2020) является:**
    a. понятность
    b. анализируемость
    c. устойчивость к ошибке

Вопрос 6 (Множественный выбор / Только один ответ)

---

18. **Под понятностью моделей ИИ (в соответствии с ГОСТ Р 59276-2020) понимается:**
    a. Свойство системы искусственного интеллекта, заключающееся в возможности представления причин, приводящих к тому или иному решению системы, в виде, понятном человеку
    b. Свойство объекта сохранять во времени способность выполнять требуемые функции в заданных режимах и условиях применения, технического обслуживания, хранения и транспортирования
    c. Свойство системы искусственного интеллекта, заключающееся в возможности открытого, исчерпывающего, доступного, четкого и понятного представления информации

Вопрос 7 (Множественный выбор / Только один ответ)

---

19. **В соответствии с ГОСТ Р 59276-2020 система искусственного интеллекта, в отношении которой потребитель и при необходимости, организации, ответственные за регулирование вопросов создания и применения систем искусственного интеллекта, проявляют доверие – это …**
    a. информационная технология
    b. доверенная система искусственного интеллекта
    c. надежная система искусственного интеллекта

Вопрос 8 (Множественный выбор / Только один ответ)

---

20. **Субхарактеристикой сопровождаемости ИИ (в соответствии с ГОСТ Р 59276-2020) является**
    a. изучаемость
    b. тестируемость
    c. стабильность

Вопрос 9 (Множественный выбор / Только один ответ)

По умолчанию для Доверенный искусственный интеллект (09.04.01, 2021)/2. Управление рисками искусственного интеллекта

1. **Как называется процесс оценки качества, выполняемый потребителем систем ИИ?**
    a. Испытание
    b. Контроль разработки
    c. Сертификация

Вопрос 1 (Множественный выбор / Только один ответ)

---

2. Высокоавтономные системы могут создавать риски, связанные с их …

a. Безопасностью и надежностью
b. Конфиденциальностью и целостностью
c. Доступностью и надежностью

Вопрос 10 (Множественный выбор / Только один ответ)

---

3. Системы с высоким уровнем автономности могут демонстрировать неожиданное поведение, которое может быть трудно …

a. Выявить и оценить
b. Локализовать и устранить
c. Обнаружить и контролировать

Вопрос 11 (Множественный выбор / Только один ответ)

---

4. Системы с низкой степенью прозрачности принятия решений могут создавать риски в отношении их …

a. Объяснимости, прозрачности и подотчетности
b. Объективности, прозрачности и подотчетности
c. Защищенности, подотчетности, объективности

Вопрос 12 (Множественный выбор / Только один ответ)

---

5. Высокая степень прозрачности решений может привести к …

a. путанице
b. уязвимости
c. ненадежности

Вопрос 13 (Множественный выбор / Только один ответ)

---

6. Как правило, более сложные среды могут привести к ситуациям, которые не были учтены на этапе_____системы искусственного интеллекта

a. тестирования
b. проектирования
c. ввода в эксплуатацию

Вопрос 14 (Множественный выбор / Только один ответ)

---

7. Сложные среды могут создавать риски, связанные с …

a. подотчетностью и объективностью системы искусственного интеллекта
b. надежностью и безопасностью системы искусственного интеллекта
c. объяснимостью и надежностью объективностью системы искусственного интеллекта

Вопрос 15 (Множественный выбор / Только один ответ)

---

8. **Системная инженерия включает в себя ...**
    a. проектирование, спецификацию, внедрение
    b. проектирование, сертификацию, внедрение
    c. проектирование, сертификацию, регистрацию

Вопрос 16 (Множественный выбор / Только один ответ)

---

9. **Процесс риск-менеджмента может применяться на разных уровнях**
    a. **(50%)** программном
    b. **(50%)** стратегическом
    c. общественно-социальном

Вопрос 17 (Множественный выбор)

---

10. **В каком из вариантов ответов правильно описана последовательность этапов управления рисками?**
    a. Идентификация; оценка риска; выбор метода управления и применение метода управления; мониторинг риска
    b. Выбор метода управления и применение метода управления; мониторинг риска; идентификация; оценка риска
    c. Мониторинг риска; выбор метода управления и применение метода управления; идентификация; оценка риска

Вопрос 18 (Множественный выбор)

---

11. **Помимо идентификации, оценки, риски должны быть расставлены по _____ в соответствии с критериями оценки рисков и целями организации.**
    a. источникам
    b. классам
    c. приоритетам

Вопрос 19 (Множественный выбор)

---

12. **Разработчиком системы ИИ в процессе оценки качества проверяется**
    a. Соответствие внутренним требованиям, открытым требованиям
    b. Соответствие требованиям потребителя
    c. Соответствие требованиям регулятора

Вопрос 2 (Множественный выбор / Только один ответ)

---

13. **В случае, когда анализ рисков связан с принятием решений, используется**
    a. Априорный анализ
    b. Апостериорный анализ
    c. Анализ на ходу

Вопрос 20 (Множественный выбор)

---

14. **При использовании ИИ следует учитывать внутренние и внешние заинтересованные стороны.Например, машинное обучение, в частности, опирается на соответствующий набор данных для реализации своих задач.**

Такие заинтересованные стороны могут помочь в выявлении рисков, связанных с использованием данных в конкретных ситуациях или там, где данные могут являться выбросами – характеризует принцип

a. Персонализованность
b. Инклюзивность
c. Динамичность

Вопрос 3 (Множественный выбор / Только один ответ)

---

15. В каком стандарте дано описание общих принципов управления рисками?

a. ИСО 31000:2019
b. ИСО 31000:2018
c. ИСО 31001:2018

Вопрос 4 (Множественный выбор / Только один ответ)

---

16. При определении рисков систем искусственного интеллекта следует учитывать различные _____ рисков, в зависимости от характера рассматриваемой системы и контекста ее применения.

a. источники
b. причины
c. уровни

Вопрос 5 (Множественный выбор / Только один ответ)

---

17. Дополнительные соображения в контексте разработки и использования систем ИИ - Организации должны выбрать подходящие измерения для оценки вероятности материализации риска в соответствии с общепринятым в отрасли современным уровнем исследований ИИ – относится к соображению по определению критериев риска в соответствии с ИСО 31000:2018

a. последовательность в использовании измерений
b. метод определения уровня риска
c. факторы, связанные со временем

Вопрос 6 (Множественный выбор / Только один ответ)

---

18. Дополнительные соображения в контексте разработки и использования систем ИИ - Организации должны установить последовательный подход к определению уровня риска. Данный подход должен отражать потенциальное влияние системы ИИ на различные цели, связанные с ИИ (см. Пункт 6.3.5 - Цели, связанные с ИИ) относится к соображению по определению критериев риска в соответствии с ИСО 31000:2018

a. способ учета комбинации и последовательности множественных рисков
b. метод определения уровня риска
c. потенциал организации

Вопрос 7 (Множественный выбор / Только один ответ)

---

19. Дополнительные рекомендации по управлению рисками ИИ. Организациям следует рассмотреть: — Изменения в группах клиентов и пользователей систем искусственного интеллекта и предоставляемых ими услугах — Изменения, вызванные использованием систем искусственного интеллекта в организации и

т.д. Относится к … согласно пункту 6.4.2 руководства, приведенного в ИСО 31000:2018

a. материальные и нематериальные источники риска
b. причины и события
c. изменения во внешнем и внутреннем контексте

Вопрос 8 (Множественный выбор / Только один ответ)

---

20. **Дополнительные рекомендации по управлению рисками ИИ. Организациям следует принять во внимание: — Современное состояние техники и отраслевой практики, а также имеющийся внутренний и внешний опыт. — Проблемы, поднятые клиентами и пользователями, а также членами организации, контактирующими с клиентами и пользователями. Относится к … согласно пункту 6.4.2 руководства, приведенного в ИСО 31000:2018**
    a. показатели возникающих рисков
    b. характер и стоимость активов и ресурсов
    c. последствия и их влияние на цели

Вопрос 9 (Множественный выбор / Только один ответ)

По умолчанию для Доверенный искусственный интеллект (09.04.01, 2021)/3. Объяснимость моделей искусственного интеллекта и машинного обучения

1. **Объяснимый искусственный интеллект– это …**
    a. вариант машинного обучения, при котором в алгоритмы ИИ встраивается способ сообщать о выполненных шагах и об основаниях для выбора определенной конкретной рекомендации или результата
    b. обеспечение защиты гарантированных российским и международным законодательством прав и свобод человека, в том числе права на труд, и предоставление гражданам возможности получать знания и приобретать навыки для успешной адаптации к условиям цифровой экономики
    c. развитие рыночных отношений и недопустимость действий, направленных на ограничение конкуренции между российскими организациями, осуществляющими деятельность в области искусственного интеллекта

Вопрос 1 (Множественный выбор / Только один ответ)

---

2. **Предполагается, что объяснимость ИИ будет включать в себя следующие составляющие:**
    a. **(50%)** алгоритмическую прозрачность
    b. **(50%)** симулируемость
    c. детальность

Вопрос 10 (Множественный выбор)

---

3. **_____ означает возможность анализа модели человеком; наиболее важным критерием для … является сложность модели. Простые, но обширные (со слишком большим количеством правил) системы, основанные на правилах**

не соответствуют этой характеристике, тогда как одиночная нейронная сеть персептрона попадает в нее.

a. Алгоритмическая прозрачность
b. Симулируемость
c. Разложимость

Вопрос 11 (Множественный выбор / Только один ответ)

---

4. **_____означает способность пользователя понять процесс, которому следует модель ИИ, чтобы произвести любой заданный вывод из ее входных данных.**
   a. Алгоритмическая прозрачность
   b. Разложимость
   c. Симулируемость

Вопрос 12 (Множественный выбор / Только один ответ)

---

5. **_____означает способность объяснить каждую из частей модели (входные данные, параметры и выходные данные). Громоздкие функции не соответствуют данному критерию.**
   a. Симулируемость
   b. Разложимость
   c. Алгоритмическая прозрачность

Вопрос 13 (Множественный выбор / Только один ответ)

---

6. **Объяснения алгоритмов работы ИИ могут быть представлены в ...**
   a. **(50%)** Текстовой форме
   b. **(50%)** Визуальной форме
   c. Аудио форме

Вопрос 14 (Множественный выбор)

---

7. **Отсутствие _____ может приводить к ситуациям, когда модель присваивает более высокий вес тем входным переменным, которые объективно не должны иметь такого веса.**
   a. объяснимости
   b. тестируемости
   c. стабильности

Вопрос 15 (Множественный выбор / Только один ответ)

---

8. **Алгоритмы машинного обучения, особенно _____, очень хороши в выявлении тонких закономерностей в огромных наборах данных**
   a. случайный лес
   b. деревья принятия решений
   c. глубокие нейронные сети

Вопрос 16 (Множественный выбор / Только один ответ)

---

9. **Основная проблема объяснимости алгоритмов машинного обучения тесно связана с …**
    a. тем, что они могут выявлять тонкие закономерности в наборах данных
    b. тем, что им сложно делать простые причинно-следственные выводы
    c. тем, что они показывают хорошие результаты лишь при работе с огромными наборами данных

Вопрос 17 (Множественный выбор / Только один ответ)

---

10. **В дополнение к этому, большинство текущих успехов машинного обучения сводятся к крупномасштабному распознаванию образов на надлежащим образом собранных …**
    a. случайных и независимых данных
    b. коррелируемых данных и связанных
    c. независимых и идентично распределенных данных

Вопрос 18 (Множественный выбор / Только один ответ)

---

11. **Для генерализации за пределы iid-сетапа требуется изучение …**
    a. статистических ассоциаций между переменными
    b. статистических ассоциаций между переменными и причинно-следственной (каузальной) модели
    c. причинно-следственной (каузальной) модели

Вопрос 19 (Множественный выбор / Только один ответ)

---

12. **Под объяснимостью моделей ИИ (в соответствии с ГОСТ Р 59276-2020) понимается**
    a. открытость для общественности информации, касающейся исследования, проектирования, создания, развертывания и применения системы
    b. свойство системы искусственного интеллекта, заключающееся в возможности представления причин, приводящих к тому или иному решению системы, в виде, понятном человеку
    c. обеспечение уважения, защита и поощрение неприкосновенности частной жизни – права, имеющего важнейшее значение с точки зрения защиты человеческого достоинства и свободы выбора

Вопрос 2 (Множественный выбор / Только один ответ)

---

13. **Причинно-следственная связь также может иметь решающее значение для борьбы с …**
    a. дрейфом модели
    b. состязательными атаками
    c. отравлением данных

Вопрос 20 (Множественный выбор / Только один ответ)

---

14. **Под понятностью моделей ИИ (в соответствии с ГОСТ Р 59276-2020) понимается**
    a. Свойство системы искусственного интеллекта, заключающееся в возможности представления причин, приводящих к тому или иному решению системы, в виде, понятном человеку

b. Свойство объекта сохранять во времени способность выполнять требуемые функции в заданных режимах и условиях применения, технического обслуживания, хранения и транспортирования
c. Свойство системы искусственного интеллекта, заключающееся в возможности открытого, исчерпывающего, доступного, четкого и понятного представления информации

Вопрос 3 (Множественный выбор / Только один ответ)

---

15. Какой вид объяснимости ИИ можно отнести к принципам работы деревьев решений?

a. определение важности признаков, информативности данных
b. объяснение причинно-следственных связей решений, их интерпретируемость
c. определение предвзятости решений ИИ, соответствия моделей или данных этическим нормам

Вопрос 4 (Множественный выбор / Только один ответ)

---

16. Какой из алгоритмов/моделей машинного обучения обладает наилучшей объяснимостью?

a. машина опорных векторов
b. деревья решений
c. искусственные нейронные сети

Вопрос 5 (Множественный выбор / Только один ответ)

---

17. Объяснимый искусственный интеллект (XAI) - это …

a. открытость для общественности информации, касающейся исследования, проектирования, создания, развертывания и применения системы
b. набор процессов и методов, позволяющих пользователям понять, почему именно алгоритмы машинного обучения пришли к тем или иным результатам или выводам
c. определение предвзятости решений ИИ, соответствия моделей или данных этическим нормам

Вопрос 6 (Множественный выбор / Только один ответ)

---

18. Объяснимый ИИ помогает охарактеризовать _____ модели, предназначенной для принятия решений с помощью ИИ

a. **(50%)** Точность и доверенность
b. **(50%)** Прозрачность
c. Предвзятость

Вопрос 7 (Множественный выбор)

---

19. Объяснимый ИИ играет важнейшую роль для повышения …

a. **(50%)** Достоверности производственных моделей ИИ
b. **(50%)** Надежности производственных моделей ИИ
c. Целостности производственных моделей

Вопрос 8 (Множественный выбор)

---

20. **По мере расширения возможностей ИИ, людям становится все сложнее осознать, каким образом алгоритм пришел к тому или иному результату. Процесс вычисления превращается в так называемый _____ ящик**
    a. белый
    b. черный
    c. серый

Вопрос 9 (Множественный выбор / Только один ответ)

По умолчанию для Доверенный искусственный интеллект (09.04.01, 2021)/4. Робастность искусственного интеллекта и нейронных сетей

1. **Способность ИИ поддерживать уровень производительности (примерно равный уровень ошибочных решений) при любых обстоятельствах, в том числе способность модели демонстрировать достаточный уровень производительности при ее обучении в автоматическом режиме**
    a. понятность
    b. предсказуемость
    c. робастность

Вопрос 1 (Множественный выбор / Только один ответ)

---

2. **Особенно, на робастность могут повлиять следующие факторы:**
    a. **(50%)** Состязательные и другие примеры, исследующие крайности гипотетической области
    b. Предобработка данных и качество требований к процессу оценки робастности
    c. **(50%)** Разнообразие, репрезентативность и диапазон выбросов

Вопрос 10 (Множественный выбор)

---

3. **Какая группа подходов обычно основываются на процессе математического тестирования некоторых наборов данных и помогают обеспечить определенный уровень уверенности в результатах?**
    a. Статистические подходы
    b. Формальные методы
    c. Эмпирические методы

Вопрос 11 (Множественный выбор / Только один ответ)

---

4. **Формальные методы полагаются на …**
    a. надежное формальное доказательство, чтобы продемонстрировать математическое свойство в заданной области значений
    b. на эксперименты, наблюдения и экспертные оценки
    c. на математическое тестирование

Вопрос 12 (Множественный выбор / Только один ответ)

---

5. **Методы наблюдения принято разделять на …**

a. математические и логические
b. статистические и эмпирические методы
c. натурные и симуляционные

Вопрос 13 (Множественный выбор / Только один ответ)

---

6. **Продолжите фразу. На практике эти методы в настоящее время не используются для непосредственной оценки ...**
   a. робастности в целом
   b. устойчивости в целом
   c. защиты в целом

Вопрос 14 (Множественный выбор / Только один ответ)

---

7. **Принцип применения таких методов для оценки надежности заключается в том, чтобы оценить, в какой степени эти свойства сохраняются при изменении обстоятельств: При использовании статистических методов -**
   a. по-прежнему ли новые условия относятся к области, в которой свойства доказуемы?
   b. как изменяется измеренное значение производительности при изменении условий?
   c. сохраняются ли эти свойства в других сценариях?

Вопрос 15 (Множественный выбор / Только один ответ)

---

8. **Принцип применения таких методов для оценки надежности заключается в том, чтобы оценить, в какой степени эти свойства сохраняются при изменении обстоятельств: При использовании эмпирических методов -**
   a. по-прежнему ли новые условия относятся к области, в которой свойства доказуемы?
   b. как изменяется измеренное значение производительности при изменении условий?
   c. сохраняются ли эти свойства в других сценариях?

Вопрос 16 (Множественный выбор / Только один ответ)

---

9. **Продолжите фразу. Характеристика робастности нейронных сетей является активной областью исследований, и существуют ограничения как для подходов ...**
   a. к тестированию, так и к верификации
   b. к сбору данных, так и к анализу
   c. к формулировке целей, так и к планированию эксперимента

Вопрос 17 (Множественный выбор / Только один ответ)

---

10. **Сколько основных критериев используют для вычисления робастности в случае применения статистических методов?**
    a. 4
    b. 5
    c. 6

Вопрос 18 (Множественный выбор / Только один ответ)

11. **Какой критерий позволяет робастность с использованием различных параметров модели (например, точность модели, квантованный вес и т. д.)?**
    a. Выбор метрики или метрик эффективности
    b. Выбор настроек модели
    c. Метод определения робастности

Вопрос 19 (Множественный выбор / Только один ответ)

---

12. **Что можно отнести к метрикам робастности?**
    a. стандартное отклонение остатков (ошибок прогнозирования). Остатки - это мера того, насколько далеко от точек данных линии регрессии
    b. отклонение решения ИИ от желаемого
    c. отклонение прогноза ИИ от медианного

Вопрос 2 (Множественный выбор / Только один ответ)

---

13. **Для какой из систем свойство стабильности формализуется следующим способом? Максимальное стабильное пространство вычисляет размер области, в которой нейронная сеть будет иметь стабильную производительность классификации.**
    a. Для систем классификации
    b. Для систем интерполяции
    c. Для систем кластеризации

Вопрос 20 (Множественный выбор / Только один ответ)

---

14. **Сколько выделяют групп методов оценки робастности?**
    a. 3
    b. 4
    c. 2

Вопрос 3 (Множественный выбор / Только один ответ)

---

15. **Что является первым шагом для типового процесса определения робастности нейронной сети?**
    a. Формулировка целей робастности
    b. Интерпретация результатов
    c. Проведение эксперимента

Вопрос 4 (Множественный выбор / Только один ответ)

---

16. **Следующим шагом после формулировки целей робастности является?**
    a. Проведение эксперимента
    b. Планирование эксперимента
    c. Анализ результатов

Вопрос 5 (Множественный выбор / Только один ответ)

---

17. **После завершения эксперимента результаты подлежат …**
    a. Проведение эксперимента
    b. Планирование эксперимента
    c. Анализ результатов

Вопрос 6 (Множественный выбор / Только один ответ)

---

18. **К какому шагу относится решение по робастности системы формулируется по определенным ранее критериям и полученной интерпретации результатов анализа. Если цели тестирования не достигнуты, проводится анализ процесса, и процесс возвращается к соответствующему предыдущему шагу, чтобы устранить недостатки ?**
    a. Анализ результатов
    b. Интерпретация результатов
    c. Принятие решения

Вопрос 7 (Множественный выбор / Только один ответ)

---

19. **_____ представляет собой процесс выбора, производства или генерации требуемых данных**
    a. Отравление данных
    b. Сбор данных
    c. Аугментация данных

Вопрос 8 (Множественный выбор / Только один ответ)

---

20. **Требования и критерии, необходимые для сбора данных содержатся в …**
    a. экспериментальном протоколе
    b. протоколе анализа
    c. протоколе планирования эксперимента

Вопрос 9 (Множественный выбор / Только один ответ)

По умолчанию для Доверенный искусственный интеллект (09.04.01, 2021)/5. Функциональная безопасность искусственного интеллекта

1. **Какие функции относятся к определению аномалий данных?**
    a. проверка дрейфа данных во время, логических выводов и производства, обнаружение утечки данных, обнаружение отравления данных
    b. проверка гипотез о законе распределения признаков
    c. проверка корреляции между признаками и устранение зависимых признаков

Вопрос 1 (Множественный выбор / Только один ответ)

---

2. **Каким образом возможно повысить устойчивость модели к дрейфу концепций?**
    a. обучить на репрезентативной выборке
    b. периодически переобучать, используя заранее заготовленную репрезентативную и неизменную выборку

c. реализовать алгоритм онлайн-обучения модели в процессе функционирования

Вопрос 10 (Множественный выбор / Только один ответ)

---

3. С помощью чего можно устранить дрейф данных?

a. Разработка оптимальной модели данных
b. Улучшенного моделирования и переобучения
c. Автономное обучение

Вопрос 11 (Множественный выбор / Только один ответ)

---

4. С чем часто связан дрейф данных?

a. С повреждениеv параметров или знаний модели
b. **(50%)** С неполным представлением области входных значений во время обучения
c. **(50%)** С изменениями в составе объектов

Вопрос 12 (Множественный выбор)

---

5. К потенциальным подходам, обеспечивающим обнаружение дрейфа, относят ...

a. ANN, INN и повышение точности их работы
b. **(50%)** EDDM, SVM и наблюдение за ошибкой вывода во время обучения
c. **(50%)** MOA, RapidMiner и изучение меняющихся во времени концепций и концепцию отслеживания дрейфа

Вопрос 13 (Множественный выбор)

---

6. Что обеспечивают стандарты ISO/IEC 27001, ISO/IEC 18045 и ISO/IEC 62443?

a. Процесс оценки робастности нейронных сетей
b. Процессы аудита и сертификации горизонтальных требований к ИТ-безопасности
c. Процесс управления рисками для искусственного интеллекта

Вопрос 14 (Множественный выбор / Только один ответ)

---

7. Функциональная безопасность связана с надлежащей разработкой _____ функций безопасности

a. Технических
b. Нетехнических
c. Технических и нетехнических

Вопрос 15 (Множественный выбор / Только один ответ)

---

8. Что такое взлом вознаграждения?

a. Алгоритм машинного обучения без учителя, построенный на комбинации из двух нейронных сетей, одна из которых генерирует образцы , а другая старается отличить правильные образцы от неправильных
b. **(50%)** Явление, когда технология ИИ находит способ воспроизвести свою функцию вознаграждения (reward function) и, таким образом, найти более оптимальное решение проблемы

c. **(50%)** Обучение менее дорогой (less expensive) модели ученика (student model) для имитации более дорогой модели учителя (teacher model), сохраняя, при этом, большую часть первоначальной доли верных ответов (accuracy)

Вопрос 16 (Множественный выбор)

---

9. Что понимается под стратегической зрелостью технологии для внедрения системы ИИ?

a. Будет действовать, скорее всего, только в среднесрочной и долгосрочной перспективе
b. Является предпочтительной для реализации в большинстве приложений
c. Исследуется и тестируется для возможного использования в будущем

Вопрос 17 (Множественный выбор / Только один ответ)

---

10. Взлом вознаграждения является математически выгодным, но опасен тем, что ...

a. может быть ничего не найдено
b. могут быть нарушены границы и предположения
c. всё пройдет по сценарию

Вопрос 18 (Множественный выбор / Только один ответ)

---

11. Самообучающаяся система будучи не отключенной должным образом от опасного процесса

a. не может представлять угроз или рисков для безопасности системы
b. представляет меньшую угрозы или риски для системы безопасности
c. может представлять такие же или большие риски для безопасности

Вопрос 19 (Множественный выбор / Только один ответ)

---

12. Примерами непреднамеренного снижения качества систем ИИ являются

a. использование статистически смещенной обучающей выборки, приводящей к появлению «предвзятостей» в результатах работы системы ИИ
b. отравление данных
c. отсутствие достоверных и представительных оценок устойчивости системы распознавания изображений к воздействию преднамеренных «состязательных» атак, приводящее к неустойчивой работе системы в процессе ее эксплуатации.

Вопрос 2 (Множественный выбор / Только один ответ)

---

13. Сохранение или даже увеличение угроз/рисков безопасности может представлять

a. система, не отключенная должным образом от опасного процесса
b. параллельная система, отключенная от основной функции
c. система, выведенная из работы

Вопрос 20 (Множественный выбор / Только один ответ)

---

14. **Что позволит устранить статистическую смещенность обучающей выборки, способной привести к предвзятости (необъективности) результатов работы системы в соответствии с ГОСТ Р 59276-2020?**
    a. разработка оптимальной модели данных
    b. кросс-валидация выборки, полученной при разметке данных людьми
    c. соблюдение допустимой области применения системы ИИ

Вопрос 3 (Множественный выбор / Только один ответ)

---

15. **Методика заключения модели в защищенную среду и ее обучение без перемещения данных куда-либо - это ...**
    a. федеративное обучение
    b. централизованное обучение
    c. автономное обучение

Вопрос 4 (Множественный выбор / Только один ответ)

---

16. **С какой проблемой связывают сезонные изменения данных и связанное с этим ухудшение прогностической способности модели?**
    a. дрейф данных
    b. миграция данных
    c. утечка данных

Вопрос 5 (Множественный выбор / Только один ответ)

---

17. **Создание промежуточного синтетического биометрического образа(ов), основанное на нахождении некоторого промежуточного значения каждого из биометрических параметров пары биометрических образов-родителей**
    a. Бэггинг биометрических примеров
    b. Морфинг биометрических примеров
    c. Бустинг биометрических примеров

Вопрос 6 (Множественный выбор / Только один ответ)

---

18. **С какой проблемой связывают резкое или постепенное изменение данных (например, в связи с обвалом рынка или медленным изменением предпочтений клиентов) и связанное с этим ухудшение прогностической способности модели?**
    a. дрейф данных
    b. дрейф концепций
    c. повреждение параметров или знаний модели

Вопрос 7 (Множественный выбор / Только один ответ)

---

19. **Какой из принципов Национального кодекса этики в сфере ИИ гарантирует соблюдение законодательства РФ в области ПДн при использовании СИИ, обеспечивать охрану и защиту ПДн, обработка которых осуществляется СИИ или Акторами?**
    a. безопасность работы с данными
    b. подконтрольность
    c. поднадзорность

Вопрос 8 (Множественный выбор / Только один ответ)

20. **Какой из принципов Национального кодекса этики в сфере ИИ гарантирует соблюдение законодательства РФ в области ПДн при использовании СИИ, обеспечивать охрану и защиту ПДн, обработка которых осуществляется СИИ или Акторами?**
    a. использование ИИ внутри функции, связанной с безопасностью, для реализации функциональности
    b. использование функций безопасности, не связанных с ИИ, для обеспечения безопасности оборудования, управляемого ИИ
    c. безопасность инфраструктурных функций, реализуемых ИИ, для защиты данных от предвзятости

Вопрос 9 (Множественный выбор / Только один ответ)

По умолчанию для Доверенный искусственный интеллект (09.04.01, 2021)/6. Компьютерные атаки на искусственный интеллект

1. **В чем заключается суть состязательной атаки на ИИ?**
    a. В добавлении возмущения на входе для вызова ошибки в оценке нейронной сетью данных
    b. В подмене данных для неправильного обучения нейронной сети
    c. В изменении устройства нейронной сети

Вопрос 1 (Множественный выбор / Только один ответ)

---

2. **Какая угроза конфиденциальности существует при предварительной обработке данных?**
    a. Обучение на однотипных данных
    b. Персональные данные доступны из нескольких источников (данные деидентифицированы, возможно, что ИИ деидентифицирует данные, используя выводы, основанные на данных из других источников)
    c. Сбор данных ИИ для последующей манипуляции с целью идентификации

Вопрос 10 (Множественный выбор / Только один ответ)

---

3. **Атака извлечения – это …**
    a. Атака, в ходе которой проходит незаметное получение конфиденциальной информации из системы
    b. Атака, целью которой являются обучающие данные или модель нейронной сети

Вопрос 11 (Множественный выбор / Только один ответ)

---

4. **Атаки уклонения по доступу к обучающийся модели делятся на …**
    a. Целевые и нецелевые
    b. Интеративные и однопроходные
    c. Атаки «черного ящика» и атаки «белого ящика»

Вопрос 12 (Множественный выбор / Только один ответ)

5. **Многие атаки методом «_____» предполагают, что некоторая информация доступна (какая именно модель работает, а также ее структуру модели, прежде чем успешно украсть параметры модели)**
    a. Черного ящика
    b. Белого ящика
    c. Отравления

Вопрос 13 (Множественный выбор / Только один ответ)

---

6. **_____ в основном относится к способности объяснить логику каждого решения / суждения, сделанного ИИ, и как доверять этим решениям**
    a. Прослеживаемость
    b. Интерпретируемость
    c. Исключимость

Вопрос 14 (Множественный выбор / Только один ответ)

---

7. **Развитие какого свойства ИИ выгодно как разработчикам, так и злоумышленникам? «_____» не только обеспечивает безопасность, но также раскрывает тайну нейронной сети и позволяет нам легко понять ее рабочий механизм. Злоумышленники, благодаря «_____» могут исключать диапазон входных данных, доказавших свою безопасность, тем самым сокращая пространство для поиска и более эффективно находя?**
    a. Интерпретируемость
    b. Предсказуемость
    c. Анализируемость

Вопрос 15 (Множественный выбор / Только один ответ)

---

8. **При атаке извлечения модели злоумышленники вводят «_____» данные в модель и получают значения прогноза.**
    a. конфиденциальные
    b. входные
    c. числовые

Вопрос 16 (Множественный выбор / Только один ответ)

---

9. **«_____» защитой называется метод противодействия от атак на модели, при котором может быть применен «_____» пример во время обучения.**
    a. Состязательной
    b. Противодействующей
    c. Концептуальной

Вопрос 17 (Множественный выбор / Только один ответ)

---

10. **Что можно применить в качестве противодействия атакам на уровне железа?**
    a. Ограничения доступа к обучающим данным
    b. Использовать облачные ml-модели
    c. Ограничить доступ к аутсорсинговым ml-моделям

Вопрос 18 (Множественный выбор / Только один ответ)

---

11. Сколько существует категорий атак?

a. 3
b. 5
c. 6

Вопрос 19 (Множественный выбор / Только один ответ)

---

12. Что такое дипфейк (deepfake)?

a. Реалистичная манипуляция аудио- и видеоматериалами с помощью искусственного интеллекта
b. Подмена истинного изображения на измененное, скорректированное для нужд атакующего
c. Метод борьбы с атаками на ИИ

Вопрос 2 (Множественный выбор / Только один ответ)

---

13. Предмет зарождающейся области исследований, занимающейся проблемами обеспечения безопасности с использованием алгоритмов машинного обучения в системах искусственного интеллекта, в том числе методами защиты от потенциальных угроз – это ...

a. вредоносное машинное обучение (Adversarial Machine Learning, AML)
b. Обеспечение безопасности на этапе проектирования
c. Анализ угроз

Вопрос 20 (Множественный выбор / Только один ответ)

---

14. Для чего могут быть применена технология дипфейк (deepfake)?

a. Атаковать безопасность информационных систем и компьютерных сетей
b. Атаковать на общественное мнение
c. Атаковать безопасность системы глубокого обучения

Вопрос 3 (Множественный выбор / Только один ответ)

---

15. На какую цель может быть направлен такой тип атаки как атака на конфиденциальность?

a. Изменить результат работы нейросети
b. Модель машинного обучения
c. Данные для обучения нейросети

Вопрос 4 (Множественный выбор / Только один ответ)

---

16. Что такое атака отравления и с какой целью она проводится?

a. Атаки с отравлением (преднамеренное изменение датасета) данных направлены на то, чтобы позволить обучить плохую модель, которая не может обнаруживать вредоносные атаки
b. Атака с отравлением направлена на хранилище данных для обучения нейросети и ее целью является управление общественным мнением
c. Атака с отравление направлена на входные данные для обученной нейронной сети, а целью является управление общественным мнением

Вопрос 5 (Множественный выбор / Только один ответ)

---

17. Что является отличительной чертой состязательного(враждебного) adversarial perturbations возмущения?

a. необходимо для обнаружения изменения датасета
b. трудно обнаружить или даже можно не заметить глазу рядового наблюдателя
c. меняет структуру модели обучения

Вопрос 6 (Множественный выбор / Только один ответ)

---

18. Что подразумевается под кражей модели (Model stealing) машинного обучения?

a. Путем простой отправки на целевую модель большого количества запросы прогнозирования и использование полученного ответа (прогноза) для обучения другой модели
b. Физическая кража кода модели машинного обучения
c. Извлечение данных на которых обучается модель, с целью обучить модель, созданную на основе украденного датасета

Вопрос 7 (Множественный выбор / Только один ответ)

---

19. Что такое отклоняющая атака (атака уклонения)?

a. Атака на модель машинного обучения, сутью которой является неверное (неправильное) исполнение целей изначальной модели обучения
b. Атака на модель машинного обучения, целью которой является информация, на которой обучают модель
c. Атака на модель машинного обучения, успешно прошедшую обучение на достоверных данных, но изменение входных данных которой позволяет сделать так, чтобы система достигла цели злоумышленника, а не ее создателя

Вопрос 8 (Множественный выбор / Только один ответ)

---

20. Какой из принципов конфиденциальности описан в ISO/IEC 29100 «Информационная безопасность. Методы безопасности. Структура конфиденциальности» для работы с данными?

a. Принцип максимизации данных
b. Принцип минимизации данных
c. Принцип деанонимизации данных

Вопрос 9 (Множественный выбор / Только один ответ)
