МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ РФ
ПЕРМСКИЙ ГОСУДАРСТВЕННЫЙ НАЦИОНАЛЬНЫЙ
ИССЛЕДОВАТЕЛЬСКИЙ УНИВЕРСИТЕТ

# Фонды оценочных средств по дисциплине «БЕЗОПАСНОСТЬ НЕЙРОСЕТЕВЫХ ТЕХНОЛОГИЙ»

**Индикаторы (детализация) компетенции**

ОПК.4 Способен применять физические законы и модели для решения задач профессиональной деятельности

Индикаторы:

ОПК.4.1 Анализирует физические явления и процессы, идентифицирует и формулирует проблемы в профессиональной области

ОПК.4.2 Применяет знания физических основ современных информационно-телекоммуникационных технологий для решения профессиональных задач

ОПК.6 Способен при решении профессиональных задач проверять выполнение требований защиты информации ограниченного доступа в информационно-аналитических системах в соответствии с нормативными правовыми актами и нормативными методическими документами Федеральной службы безопасности Российской Федерации, Федеральной службы по техническому и экспортному контролю

Индикаторы:

ОПК.6.1 Ориентируется в нормативных правовых актах и нормативных методических документах

Федеральной службы безопасности Российской Федерации, Федеральной службы по техническому и экспортному контролю

ОПК.6.2 Определяет необходимые для решения профессиональной задачи нормативные правовые акты и нормативные методические документы Федеральной службы безопасности Российской Федерации, Федеральной службы по техническому и экспортному контролю

ОПК.6.3 Организует защиту информации ограниченного доступа в компьютерных системах и сетях в соответствии с нормативными правовыми актами и нормативными методическими документами Федеральной службы безопасности Российской Федерации, Федеральной службы по техническому и экспортному контролю

ОПК.11 Способен осуществлять синтез технологий и основных компонентов функциональной и обеспечивающей частей создаваемых информационно-аналитических систем, в том числе выбор мероприятий по защите информации

Индикаторы:

ОПК.11.1 Контролирует эффективность принятых мер по реализации политик безопасности информации автоматизированных систем

ОПК.11.2 Анализирует программные, архитектурно-технические и схемотехнические решения компонентов автоматизированных систем с целью выявления потенциальных уязвимостей безопасности информации

**2. Планируемые результаты обучения**

| **Коды индикаторов компетенций** | **Планируемый результат** |
|---|---|
| ОПК.4.1 | Знает основы безопасности автоматизированных систем. Умеет анализировать физические явления и процессы, идентифицировать и формулировать проблемы в профессиональной области. Владеет сведениями о методах обеспечения конфиденциальности данных в нейросетевых моделях. |
| ОПК.4.2 | Знает основы безопасности автоматизированных систем. Умеет применять знания физических основ современных информационно-Телекоммуникационных технологий для решения профессиональных задач. Владеет сведениями о методах обеспечения безопасности нейросетевых моделей на базе глубоких сверточных сетей. |
| ОПК.6.1 | Знает основы безопасности автоматизированных систем. Умеет ориентироваться в нормативных правовых актах и нормативных |

| | |
|---|---|
| | методических документах Федеральной службы безопасности Российской Федерации, Федеральной службы по техническому и экспортному контролю. Владеет сведениями о методах обеспечения безопасности нейросетевых моделей на базе глубоких сверточных сетей. |
| ОПК.6.2 | Знает основы безопасности автоматизированных систем. Умеет определять необходимые для решения профессиональной задачи нормативные правовые акты и нормативные методические документы Федеральной службы безопасности Российской Федерации, Федеральной службы по техническому и экспортному контролю. Владеет сведениями о методах обеспечения конфиденциальности данных. |
| ОПК.6.3 | Знает основы безопасности автоматизированных систем. Умеет организовать защиту информации ограниченного доступа в компьютерных системах и сетях в соответствии с нормативными правовыми актами и нормативными методическими документами Федеральной службы безопасности Российской Федерации, Федеральной службы по техническому и экспортному контролю. Владеет сведениями о методах обеспечения безопасности персептронных нейросетевых моделей. |
| ОПК.11.1 | Знает основы безопасности автоматизированных систем. Умеет контролировать эффективность принятых мер по реализации политик безопасности информации автоматизированных систем. Владеет сведениями о методах обеспечения конфиденциальности данных. |
| ОПК.11.2 | Знает основы безопасности автоматизированных систем. Умеет анализировать программные, архитектурно- технические и схемотехнические решения компонентов автоматизированных систем с целью выявления потенциальных уязвимостей безопасности информации. Владеет сведениями о методах обеспечения конфиденциальности данных в нейросетевых моделях. |

**3. Спецификация теста**

Тест по дисциплине «Безопасность нейросетевых технологий» представляет собой перечень примерных вопросов, предлагаемых студентам с учетом тем и заданий для контрольных мероприятий, предусмотренных по дисциплине.

**Вариант 1**

1. Какой из следующих методов используется для выявления угроз в нейросетевых технологиях?
а) Шифрование данных
б) Аномалия детектирования
в) Моделирование данных
г) Визуализация данных

2. Что из перечисленного является мерой обеспечения конфиденциальности данных?

а) Открытые данные
б) Анонимизация
в) Увеличение объема данных
г) Публикация данных

3. Какой из следующих подходов наиболее эффективен для защиты многослойных персептронов?
а) Увеличение числа слоев
б) Регуляризация
в) Упрощение архитектуры
г) Увеличение объема обучающих данных

4. Какой из методов можно использовать для защиты данных, на которых обучаются глубокие сверточные сети?
а) Изменение формата данных
б) Шифрование данных
в) Удаление данных
г) Публикация данных

5. Какой из следующих аспектов важен для обеспечения безопасности нейросетей на базе трансформеров?
а) Увеличение числа параметров
б) Обучение на открытых данных
в) Защита от атак с использованием подмены данных
г) Упрощение архитектуры

6. Какие данные должны быть защищены при использовании больших языковых моделей?
а) Только текстовые данные
б) Все данные, включая метаданные
в) Только метаданные
г) Данные, относящиеся к обучению

7. Какой метод можно использовать для защиты от атак на нейросети?
а) Увеличение объема данных
б) Применение методов adversarial training
в) Упрощение модели
г) Использование только симметричного шифрования

8. Что такое "adversarial examples"?
а) Примеры, которые помогают обучению
б) Примеры, созданные для обмана модели
в) Примеры, используемые для оценки производительности
г) Примеры, которые не влияют на модель

9. Какой из следующих методов является мерой обеспечения безопасности данных в нейросетях?
а) Публикация исходного кода
б) Удаление данных после использования
в) Шифрование данных
г) Открытие доступа к данным

10. Какой из следующих аспектов важен для обеспечения безопасности в глубоких

сверточных сетях?
а) Использование только одного типа данных
б) Защита от атак с использованием подмены входных данных
в) Увеличение числа слоев
г) Публикация архитектуры сети

11. Что такое "privacy-preserving machine learning"?
а) Обучение моделей без использования данных
б) Обучение моделей с учетом конфиденциальности данных
в) Обучение моделей на открытых данных
г) Обучение моделей с использованием только анонимизированных данных

12. Какой из следующих методов может помочь в обеспечении безопасности данных в нейросетях?
а) Использование неструктурированных данных
б) Применение дифференциальной приватности
в) Упрощение архитектуры нейросети
г) Увеличение объема данных

13. Что такое "data poisoning"?
а) Уничтожение данных
б) Внедрение вредоносных данных в обучающую выборку
в) Защита данных от утечек
г) Применение методов шифрования

14. Какой из следующих методов может повысить безопасность нейросетей?
а) Использование открытых данных
б) Анонимизация данных
в) Упрощение модели
г) Увеличение числа параметров

15. Какой из следующих аспектов важен для обеспечения безопасности больших языковых моделей?
а) Использование только текстовых данных
б) Защита от утечек конфиденциальной информации
в) Упрощение архитектуры
г) Публикация всех данных

16. Какой метод может помочь в защите от атак на нейросети?
а) Увеличение числа слоев
б) Использование методов adversarial training
в) Упрощение архитектуры
г) Обучение на открытых данных

17. Какой из следующих подходов может помочь в защите данных, используемых в нейросетях?
а) Публикация данных
б) Шифрование данных
в) Упрощение архитектуры
г) Увеличение объема данных

18. Что такое "model inversion attack"?

а) Атака на данные
б) Атака на архитектуру модели
в) Атака на параметры модели с целью извлечения информации
г) Атака на вычислительные ресурсы

19. Какой из следующих методов может помочь в обеспечении безопасности нейросетей?
а) Использование только анонимизированных данных
б) Упрощение архитектуры
в) Увеличение числа параметров
г) Публикация данных

20. Какой из следующих аспектов важен для обеспечения безопасности в нейросетях на базе трансформеров?
а) Защита от утечек конфиденциальной информации
б) Упрощение архитектуры
в) Увеличение числа параметров
г) Публикация всех данных

21. Какой из следующих документов регламентирует требования к защите информации в автоматизированных системах в России?
а) Законодательный акт о защите персональных данных
б) Федеральный закон "О техническом регулировании"
в) Постановление Правительства Российской Федерации о защите информации
г) Федеральный закон "О государственной тайне"

22. Какой из следующих методов используется для обеспечения конфиденциальности данных в автоматизированных системах?
а) Аудит безопасности
б) Шифрование данных
в) Регуляризация моделей
г) Открытие доступа к данным

23. Какой из следующих актов регулирует экспорт технологий и товаров двойного назначения в России?
а) Федеральный закон "О защите информации"
б) Федеральный закон "О техническом и экспортном контроле"
в) Постановление Правительства о лицензировании
г) Закон о персональных данных

24. Что такое "персональные данные" в контексте законодательства Российской Федерации?
а) Данные, которые могут быть использованы для идентификации физического лица
б) Все данные, хранящиеся в автоматизированных системах
в) Данные, относящиеся к коммерческой тайне
г) Данные, которые не подлежат защите

25. Какой из следующих методов не является средством обеспечения безопасности автоматизированных систем?
а) Аудит безопасности
б) Шифрование данных

в) Увеличение объема данных
г) Обучение сотрудников по вопросам безопасности

**Вариант 2**

1. Какой метод используется для защиты данных в нейросетях?
а) Шифрование данных
б) Увеличение объема данных
в) Упрощение модели
г) Публикация данных

2. Что такое "дифференциальная приватность"?
а) Метод шифрования данных
б) Метод обеспечения конфиденциальности данных
в) Метод увеличения объема данных
г) Метод оценки производительности модели

3. Какой из следующих методов может помочь в обеспечении безопасности многослойных персептронов?
а) Упрощение архитектуры
б) Регуляризация
в) Увеличение числа слоев
г) Использование открытых данных

4. Какой из следующих аспектов важен для защиты глубоких сверточных сетей?
а) Защита от атак с использованием подмены входных данных
б) Увеличение числа слоев
в) Публикация архитектуры сети
г) Упрощение модели

5. Какие данные должны быть защищены при использовании нейросетей на базе трансформеров?
а) Только текстовые данные
б) Все данные, включая метаданные
в) Только метаданные
г) Данные, относящиеся к обучению

6. Какой из методов можно использовать для защиты от атак на нейросети?
а) Увеличение объема данных
б) Применение методов adversarial training
в) Упрощение модели
г) Использование только симметричного шифрования

7. Что такое "adversarial examples"?
а) Примеры, которые помогают обучению
б) Примеры, созданные для обмана модели
в) Примеры, используемые для оценки производительности
г) Примеры, которые не влияют на модель

8. Какой из следующих методов является мерой обеспечения безопасности данных в нейросетях?

а) Публикация исходного кода
б) Удаление данных после использования
в) Шифрование данных
г) Открытие доступа к данным

9. Какой из следующих аспектов важен для обеспечения безопасности в глубоких сверточных сетях?
а) Использование только одного типа данных
б) Защита от атак с использованием подмены входных данных
в) Увеличение числа слоев
г) Публикация архитектуры сети

10. Что такое "privacy-preserving machine learning"?
а) Обучение моделей без использования данных
б) Обучение моделей с учетом конфиденциальности данных
в) Обучение моделей на открытых данных
г) Обучение моделей с использованием только анонимизированных данных

11. Какой из следующих методов может помочь в обеспечении безопасности данных в нейросетях?
а) Использование неструктурированных данных
б) Применение дифференциальной приватности
в) Упрощение архитектуры нейросети
г) Увеличение объема данных

12. Что такое "data poisoning"?
а) Уничтожение данных
б) Внедрение вредоносных данных в обучающую выборку
в) Защита данных от утечек
г) Применение методов шифрования

13. Какой из следующих методов может повысить безопасность нейросетей?
а) Использование открытых данных
б) Анонимизация данных
в) Упрощение модели
г) Увеличение числа параметров

14. Какой из следующих аспектов важен для обеспечения безопасности больших языковых моделей?
а) Использование только текстовых данных
б) Защита от утечек конфиденциальной информации
в) Упрощение архитектуры
г) Публикация всех данных

15. Какой метод может помочь в защите от атак на нейросети?
а) Увеличение числа слоев
б) Использование методов adversarial training
в) Упрощение архитектуры
г) Обучение на открытых данных

16. Какой из следующих подходов может помочь в защите данных, используемых в нейросетях?

а) Публикация данных
б) Шифрование данных
в) Упрощение архитектуры
г) Увеличение объема данных

17. Что такое "model inversion attack"?
а) Атака на данные
б) Атака на архитектуру модели
в) Атака на параметры модели с целью извлечения информации
г) Атака на вычислительные ресурсы

18. Какой из следующих методов может помочь в обеспечении безопасности нейросетей?
а) Использование только анонимизированных данных
б) Упрощение архитектуры
в) Увеличение числа параметров
г) Публикация данных

19. Какой из следующих аспектов важен для обеспечения безопасности в нейросетях на базе трансформеров?
а) Защита от утечек конфиденциальной информации
б) Упрощение архитектуры
в) Увеличение числа параметров
г) Публикация всех данных

20. Какой метод может помочь в обеспечении конфиденциальности данных?
а) Открытые данные
б) Анонимизация
в) Увеличение объема данных
г) Публикация данных

21. Какой из следующих нормативных актов определяет правила работы с конфиденциальной информацией в России?
а) Закон "О персональных данных"
б) Закон "О защите информации"
в) Закон "О государственной тайне"
г) Все вышеперечисленные

22. Какой из следующих методов может быть использован для защиты данных в автоматизированных системах от несанкционированного доступа?
а) Анонимизация данных
б) Упрощение модели
в) Увеличение числа пользователей
г) Публикация данных

23. Какой из следующих аспектов является ключевым при разработке политики безопасности автоматизированной системы?
а) Упрощение процессов
б) Определение ролей и ответственности
в) Увеличение числа сотрудников
г) Открытие доступа к данным

24. Какой из следующих документов может служить основой для разработки системы

управления безопасностью информации?
а) ISO/IEC 27001
б) Федеральный закон "О защите информации"
в) Постановление Правительства о защите информации
г) Все вышеперечисленные

25. Какой из следующих подходов рекомендуется для оценки рисков в автоматизированных системах?
а) Метод экспертных оценок
б) Метод случайного выбора
в) Метод увеличения объема данных
г) Метод открытых данных