МИНОБРНАУКИ РОССИИ

Федеральное государственное автономное образовательное учреждение высшего образования "Пермский государственный национальный исследовательский университет"

Институт компьютерных наук и технологий

Авторы-составители: **Рабчевский Андрей Николаевич**

Рабочая программа дисциплины

БЕЗОПАСНОСТЬ НЕЙРОСЕТЕВЫХ ТЕХНОЛОГИЙ

Код УМК 100624

Утверждено
Протокол №1
от «28» июня 2024 г.

Пермь, 2024

1. Наименование дисциплины

Безопасность нейросетевых технологий

2. Место дисциплины в структуре образовательной программы

Дисциплина входит в базовую часть Блока « С.1 » образовательной программы по направлениям подготовки (специальностям):

Специальность: **10.05.04** Информационно-аналитические системы безопасности
специализация Информационная безопасность финансовых и экономических структур

3. Планируемые результаты обучения по дисциплине

В результате освоения дисциплины **Безопасность нейросетевых технологий** у обучающегося должны быть сформированы следующие компетенции:

10.05.04 Информационно-аналитические системы безопасности (специализация : Информационная безопасность финансовых и экономических структур)

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

4. Объем и содержание дисциплины

Специальность	10.05.04 Информационно-аналитические системы безопасности (специализация: Информационная безопасность финансовых и экономических структур)
форма обучения	очная
№№ семестров, выделенных для изучения дисциплины	10
Объем дисциплины (з.е.)	4
Объем дисциплины (ак.час.)	144
Контактная работа с преподавателем (ак.час.), в том числе:	108
Проведение лекционных занятий	18
Проведение практических занятий, семинаров	36
Проведение лабораторных работ, занятий по иностранному языку	54
Самостоятельная работа (ак.час.)	36
Формы текущего контроля	Защищаемое контрольное мероприятие (4) Итоговое контрольное мероприятие (1)
Формы промежуточной аттестации	Экзамен (10 семестр)

5. Аннотированное описание содержания разделов и тем дисциплины

Безопасность нейросетевых технологий 1 семестр.
Курс знакомит слушателей с методами выявления угроз и обеспечения мер безопасности в нейросетевых технологиях.

Обеспечение конфиденциальности данных
В данном разделе дается материал, касающийся обеспечения конфиденциальности данных, используемых в нейросетевых технологиях.

Безопасность персептронных нейросетевых моделей
Раздел посвящен обеспечению безопасности многослойных персептронов и данных, на которых они обучаются или тестируются.

Безопсаность глубоких сверточных сетей
Раздел посвящен вопросам обеспечения безопасности в глубоких сверточных сетях, а также мерам обеспечения безопасности используемых данных.

Безопасность нейросетей- трансформеров
Раздел посвящен вопросам обеспечения безопасности в нейросетях на базе трансформеров, а также мерам обеспечения безопасности используемых данных.

Безопасность больших языковых моделей
Раздел посвящен вопросам обеспечения безопасности в больших языковых моделях, а также мерам обеспечения безопасности используемых данных.

6. Методические указания для обучающихся по освоению дисциплины

Освоение дисциплины требует систематического изучения всех тем в той последовательности, в какой они указаны в рабочей программе.

Основными видами учебной работы являются аудиторные занятия. Их цель - расширить базовые знания обучающихся по осваиваемой дисциплине и систему теоретических ориентиров для последующего более глубокого освоения программного материала в ходе самостоятельной работы. Обучающемуся важно помнить, что контактная работа с преподавателем эффективно помогает ему овладеть программным материалом благодаря расстановке необходимых акцентов и удержанию внимания интонационными модуляциями голоса, а также подключением аудио-визуального механизма восприятия информации.

Самостоятельная работа преследует следующие цели:

– закрепление и совершенствование теоретических знаний, полученных на лекционных занятиях;

- формирование навыков подготовки текстовой составляющей информации учебного и научного назначения для размещения в различных информационных системах;

- совершенствование навыков поиска научных публикаций и образовательных ресурсов, размещенных в сети Интернет;

- самоконтроль освоения программного материала.

Обучающемуся необходимо помнить, что результаты самостоятельной работы контролируются преподавателем во время проведения мероприятий текущего контроля и учитываются при промежуточной аттестации.

Обучающимся с ОВЗ и инвалидов предоставляется возможность выбора форм проведения мероприятий текущего контроля, альтернативных формам, предусмотренным рабочей программой дисциплины. Предусматривается возможность увеличения в пределах 1 академического часа времени, отводимого на выполнение контрольных мероприятий.

Процедура оценивания результатов обучения инвалидов и лиц с ограниченными возможностями здоровья по дисциплине предусматривает предоставление информации в формах, адаптированных к ограничениям их здоровья и восприятия информации.

При проведении текущего контроля применяются оценочные средства, обеспечивающие передачу информации, от обучающегося к преподавателю, с учетом психофизиологических особенностей здоровья обучающихся.

7. Перечень учебно-методического обеспечения для самостоятельной работы обучающихся по дисциплине

При самостоятельной работе обучающимся следует использовать:

– конспекты лекций;

– литературу из перечня основной и дополнительной учебной литературы, необходимой для освоения дисциплины (модуля);

– текст лекций на электронных носителях;

– ресурсы информационно-телекоммуникационной сети "Интернет", необходимые для освоения дисциплины;

– лицензионное и свободно распространяемое программное обеспечение из перечня информационных технологий, используемых при осуществлении образовательного процесса по дисциплине;

– методические указания для обучающихся по освоению дисциплины.

8. Перечень основной и дополнительной учебной литературы

Основная:

1. Ясницкий, Л. Н. Интеллектуальные системы : учебник / Л. Н. Ясницкий. — 2-е изд. — Москва : Лаборатория знаний, 2020. — 222 с. — ISBN 978-5-00101-897-1. — Текст : электронный // Цифровой образовательный ресурс IPR SMART : [сайт]. https://www.iprbookshop.ru/98549.html

Дополнительная:

1. Рабчевский, А. Н. Синтетические данные и развитие нейросетевых технологий : учебное пособие для вузов / А. Н. Рабчевский. — Москва : Издательство Юрайт, 2024. — 187 с. — (Высшее образование). — ISBN 978-5-534-17716-9. — Текст : электронный // Образовательная платформа Юрайт [сайт]. https://urait.ru/bcode/545036

9. Перечень ресурсов сети Интернет, необходимых для освоения дисциплины

При освоении дисциплины использование ресурсов сети Интернет не предусмотрено.

10. Перечень информационных технологий, используемых при осуществлении образовательного процесса по дисциплине

Образовательный процесс по дисциплине **Безопасность нейросетевых технологий** предполагает использование следующего программного обеспечения и информационных справочных систем:
Необходимое лицензионное и (или) свободно распространяемое программное обеспечение:
- приложение позволяющее просматривать и воспроизводить медиаконтент PDF-файлов «Adobe Acrobat Reader DC»;
- офисный пакет приложений «LibreOffice»;
- ОС "Альт Образование"
Специализированное программное обеспечение Компьютерного класса.

При освоении материала и выполнения заданий по дисциплине рекомендуется использование материалов, размещенных в Личных кабинетах обучающихся ЕТИС ПГНИУ (**student.psu.ru**).

При организации дистанционной работы и проведении занятий в режиме онлайн могут использоваться:

система видеоконференцсвязи на основе платформы BigBlueButton (https://bigbluebutton.org/).

система LMS Moodle (http://e-learn.psu.ru/), которая поддерживает возможность использования текстовых материалов и презентаций, аудио- и видеоконтент, а так же тесты, проверяемые задания, задания для совместной работы.

система тестирования Indigo (https://indigotech.ru/).

11. Описание материально-технической базы, необходимой для осуществления образовательного процесса по дисциплине

Для лекционных занятий, семинарских (практических) занятий требуется аудитория, оснащенная: специализированной мебелью, презентационной техникой (проектор, экран, компьютер/ноутбук) с соответствующим программным обеспечением, меловой (и) или маркерной доской.
Для проведения лабораторных занятий - Компьютерный класс, оснащенный специализированной мебелью, меловой (и) или маркерной доской, компьютерами, экраном/телевизором со специализированным программным обеспечением.
Для групповых (индивидуальных) консультаций, текущего контроля и промежуточной аттестации - специализированной мебелью, презентационной техникой (проектор, экран, компьютер/ноутбук) с соответствующим программным обеспечением, меловой (и) или маркерной доской.

Помещения научной библиотеки ПГНИУ для обеспечения самостоятельной работы обучающихся:

1. Научно-библиографический отдел, корп.1, ауд. 142. Оборудован 3 персональными компьютера с доступом к локальной и глобальной компьютерным сетям.

2. Читальный зал гуманитарной литературы, корп. 2, ауд. 418. Оборудован 7 персональными компьютерами с доступом к локальной и глобальной компьютерным сетям.

3. Читальный зал естественной литературы, корп.6, ауд. 107а. Оборудован 5 персональными компьютерами с доступом к локальной и глобальной компьютерным сетям.

4. Отдел иностранной литературы, корп.2 ауд. 207. Оборудован 1 персональным компьютером с доступом к локальной и глобальной компьютерным сетям.

5. Библиотека юридического факультета, корп.9, ауд. 4. Оборудована 11 персональными компьютерами с доступом к локальной и глобальной компьютерным сетям.

6. Читальный зал географического факультета, корп.8, ауд. 419. Оборудован 6 персональными компьютерами с доступом к локальной и глобальной компьютерным сетям.

Все компьютеры, установленные в помещениях научной библиотеки, оснащены следующим программным обеспечением:

Операционная система ALT Linux;

Офисный пакет Libreoffice.

Справочно-правовая система «КонсультантПлюс»

Фонды оценочных средств для аттестации по дисциплине
Безопасность нейросетевых технологий

Планируемые результаты обучения по дисциплине для формирования компетенции. Индикаторы и критерии их оценивания

ОПК.4

Способен применять физические законы и модели для решения задач профессиональной деятельности

Индикатор	Планируемые результаты обучения	Критерии оценивания результатов обучения
ОПК.4.1 Анализирует физические явления и процессы, идентифицирует и формулирует проблемы в профессиональной области	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.	**Неудовлетворител** Не знает основы безопасности автоматизированных систем. Не умеет анализировать физические явления и процессы, идентифицировать и формулировать проблемы в профессиональной области. Не владеет сведениями о методах обеспечения конфиденциальности данных в нейросетевых моделях. **Удовлетворительн** Знает основы безопасности автоматизированных систем. Не умеет анализировать физические явления и процессы, идентифицировать и формулировать проблемы в профессиональной области. Не владеет сведениями о методах обеспечения конфиденциальности данных в нейросетевых моделях. **Хорошо** Знает основы безопасности автоматизированных систем. Умеет анализировать физические явления и процессы, идентифицировать и формулировать проблемы в профессиональной области. Не владеет сведениями о методах обеспечения конфиденциальности данных в нейросетевых моделях. **Отлично** Знает основы безопасности автоматизированных систем. Умеет анализировать физические явления и процессы, идентифицировать и формулировать проблемы в

Индикатор	Планируемые результаты обучения	Критерии оценивания результатов обучения
		Отлично профессиональной области. Владеет сведениями о методах обеспечения конфиденциальности данных в нейросетевых моделях.
ОПК.4.2 Применяет знания физических основ современных информационно-телекоммуникационных технологий для решения профессиональных задач	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.	**Неудовлетворител** Не знает основы безопасности автоматизированных систем. Не умеет применять знания физических основ современных информационно-телекоммуникационных технологий для решения профессиональных задач. Не владеет сведениями о методах обеспечения безопасности нейросетевых моделей на базе глубоких сверточных сетей. **Удовлетворительн** Знает основы безопасности автоматизированных систем. Не умеет применять знания физических основ современных информационно-телекоммуникационных технологий для решения профессиональных задач. Не владеет сведениями о методах обеспечения безопасности нейросетевых моделей на базе глубоких сверточных сетей. **Хорошо** Знает основы безопасности автоматизированных систем. Умеет применять знания физических основ современных информационно-телекоммуникационных технологий для решения профессиональных задач. Не владеет сведениями о методах обеспечения безопасности нейросетевых моделей на базе глубоких сверточных сетей. **Отлично** 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.11

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

Индикатор	Планируемые результаты обучения	Критерии оценивания результатов обучения
ОПК.11.2 Анализирует программные, архитектурно-технические и схемотехнические решения компонентов автоматизированных систем с целью выявления потенциальных уязвимостей безопасности информации	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.	**Неудовлетворител** Не знает основы безопасности автоматизированных систем. Не умеет анализировать программные, архитектурно-технические и схемотехнические решения компонентов автоматизированных систем с целью выявления потенциальных уязвимостей безопасности информации. Не владеет сведениями о методах обеспечения конфиденциальности данных в нейросетевых моделях. **Удовлетворительн** Знает основы безопасности автоматизированных систем. Не умеет анализировать программные, архитектурно-технические и схемотехнические решения компонентов автоматизированных систем с целью выявления потенциальных уязвимостей безопасности информации. Не владеет сведениями о методах обеспечения конфиденциальности данных в нейросетевых моделях. **Хорошо** Знает основы безопасности автоматизированных систем. Умеет анализировать программные, архитектурно-технические и схемотехнические решения компонентов автоматизированных систем с целью выявления потенциальных уязвимостей безопасности информации. Не владеет сведениями о методах обеспечения конфиденциальности данных в нейросетевых моделях. **Отлично** Знает основы безопасности автоматизированных систем. Умеет анализировать программные, архитектурно-технические и схемотехнические решения компонентов автоматизированных систем с целью выявления потенциальных уязвимостей безопасности информации. Ве

Индикатор	Планируемые результаты обучения	Критерии оценивания результатов обучения
		Отлично владеет сведениями о методах обеспечения конфиденциальности данных в нейросетевых моделях.
ОПК.11.1 Контролирует эффективность принятых мер по реализации политик безопасности информации автоматизированных систем	Знает основы безопасности автоматизированных систем. Умеет контролировать эффективность принятых мер по реализации политик безопасности информации автоматизированных систем. Владеет сведениями о методах обеспечения конфиденциальности данных.	**Неудовлетворител** Не знает основы безопасности автоматизированных систем. Не умеет контролировать эффективность принятых мер по реализации политик безопасности информации автоматизированных систем. Не владеет сведениями о методах обеспечения конфиденциальности данных. **Удовлетворительн** Знает основы безопасности автоматизированных систем. Не умеет контролировать эффективность принятых мер по реализации политик безопасности информации автоматизированных систем. Не владеет сведениями о методах обеспечения конфиденциальности данных. **Хорошо** Знает основы безопасности автоматизированных систем. Умеет контролировать эффективность принятых мер по реализации политик безопасности информации автоматизированных систем. Не владеет сведениями о методах обеспечения конфиденциальности данных. **Отлично** 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.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

Индикатор	Планируемые результаты обучения	Критерии оценивания результатов обучения
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	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.	**Неудовлетворител** Не знает основы безопасности автоматизированных систем. Не 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. Не владеет сведениями о методах обеспечения конфиденциальности данных. **Удовлетворительн** Знает основы безопасности автоматизированных систем. Не 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. Не владеет сведениями о методах обеспечения конфиденциальности данных. **Хорошо** 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. Не владеет сведениями о методах обеспечения конфиденциальности данных. **Отлично** 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

Индикатор	Планируемые результаты обучения	Критерии оценивания результатов обучения
		Отлично экспортному контролю. Владеет сведениями о методах обеспечения конфиденциальности данных.
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	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.	**Неудовлетворител** Не знает основы безопасности автоматизированных систем. Не 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. Не владеет сведениями о методах обеспечения безопасности персептронных нейросетевых моделей. **Удовлетворительн** Знает основы безопасности автоматизированных систем. Не 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. Не владеет сведениями о методах обеспечения безопасности персептронных нейросетевых моделей. **Хорошо** 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. Не владеет сведениями о методах обеспечения безопасности персептронных

Индикатор	Планируемые результаты обучения	Критерии оценивания результатов обучения
		Хорошо нейросетевых моделей. **Отлично** 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.6.1 Ориентируется в нормативных правовых актах и нормативных методических документах Федеральной службы безопасности Российской Федерации, Федеральной службы по техническому и экспортному контролю	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.	**Неудовлетворител** Не знает основы безопасности автоматизированных систем. Не умеет ориентироваться в нормативных правовых актах и нормативных методических документах Федеральной службы безопасности Российской Федерации, Федеральной службы по техническому и экспортному контролю. Не владеет сведениями о методах обеспечения безопасности нейросетевых моделей на базе глубоких сверточных сетей. **Удовлетворительн** Знает основы безопасности автоматизированных систем. Не умеет ориентироваться в нормативных правовых актах и нормативных методических документах Федеральной службы безопасности Российской Федерации, Федеральной службы по техническому и экспортному контролю. Не владеет сведениями о методах обеспечения безопасности нейросетевых моделей на базе глубоких сверточных сетей. **Хорошо** Знает основы безопасности автоматизированных систем. Умеет ориентироваться в нормативных правовых актах и нормативных методических

Индикатор	Планируемые результаты обучения	Критерии оценивания результатов обучения
		Хорошо документах Федеральной службы безопасности Российской Федерации, Федеральной службы по техническому и экспортному контролю. Не владеет сведениями о методах обеспечения безопасности нейросетевых моделей на базе глубоких сверточных сетей. **Отлично** 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.

Оценочные средства текущего контроля и промежуточной аттестации

Схема доставки : для ИАСБ

Вид мероприятия промежуточной аттестации : Экзамен
Способ проведения мероприятия промежуточной аттестации : Оценка по дисциплине в рамках промежуточной аттестации определяется на основе баллов, набранных обучающимся на контрольных мероприятиях, проводимых в течение учебного периода.
Максимальное количество баллов : 100

Конвертация баллов в отметки

«отлично» - от 81 до 100
«хорошо» - от 61 до 80
«удовлетворительно» - от 45 до 60
«неудовлетворительно» / «незачтено» менее 45 балла

Компетенция (индикатор)	Мероприятие текущего контроля	Контролируемые элементы результатов обучения
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.6.1** Ориентируется в нормативных правовых актах и нормативных методических документах Федеральной службы безопасности Российской Федерации, Федеральной службы по техническому и экспортному контролю	Обеспечение конфиденциальности данных **Защищаемое контрольное мероприятие**	Знает методы обеспечения конфиденциальности данных, используемых в нейросетевых моделях.

Компетенция (индикатор)	Мероприятие текущего контроля	Контролируемые элементы результатов обучения
ОПК.4.1 Анализирует физические явления и процессы, идентифицирует и формулирует проблемы в профессиональной области **ОПК.11.2** Анализирует программные, архитектурно-технические и схемотехнические решения компонентов автоматизированных систем с целью выявления потенциальных уязвимостей безопасности информации	Безопасность персептронных нейросетевых моделей **Защищаемое контрольное мероприятие**	Знает методы обеспечения безопасности персептронных нейросетевых моделей и данных, используемых для их обучения
ОПК.4.2 Применяет знания физических основ современных информационно-телекоммуникационных технологий для решения профессиональных задач **ОПК.11.1** Контролирует эффективность принятых мер по реализации политик безопасности информации автоматизированных систем	Безопсаность глубоких сверточных сетей **Защищаемое контрольное мероприятие**	Знает методы обеспечения безопасности глубоких сверточных сетей и данных, используемых для их обучения

Компетенция (индикатор)	Мероприятие текущего контроля	Контролируемые элементы результатов обучения
ОПК.4.1 Анализирует физические явления и процессы, идентифицирует и формулирует проблемы в профессиональной области **ОПК.11.2** Анализирует программные, архитектурно-технические и схемотехнические решения компонентов автоматизированных систем с целью выявления потенциальных уязвимостей безопасности информации **ОПК.11.1** Контролирует эффективность принятых мер по реализации политик безопасности информации автоматизированных систем	Безопасность нейросетей-трансформеров **Защищаемое контрольное мероприятие**	Знает методы обеспечения безопасности нейросетевых моделей на базе трансформеров и данных, используемых для их обучения

Компетенция (индикатор)	Мероприятие текущего контроля	Контролируемые элементы результатов обучения
ОПК.4.2 Применяет знания физических основ современных информационно-телекоммуникационных технологий для решения профессиональных задач **ОПК.4.1** Анализирует физические явления и процессы, идентифицирует и формулирует проблемы в профессиональной области **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.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	Безопасность больших языковых моделей **Итоговое контрольное мероприятие**	Знает методы обеспечения безопасности больших языковых моделей и данных, используемых для их обучения

Компетенция (индикатор)	Мероприятие текущего контроля	Контролируемые элементы результатов обучения
экспортному контролю **ОПК.11.2** Анализирует программные, архитектурно-технические и схемотехнические решения компонентов автоматизированных систем с целью выявления потенциальных уязвимостей безопасности информации **ОПК.11.1** Контролирует эффективность принятых мер по реализации политик безопасности информации автоматизированных систем		

Спецификация мероприятий текущего контроля

Обеспечение конфиденциальности данных

Продолжительность проведения мероприятия промежуточной аттестации: **2 часа**
Условия проведения мероприятия: **в часы аудиторной работы**
Максимальный балл, выставляемый за мероприятие промежуточной аттестации: **30**
Проходной балл: **12.5**

Показатели оценивания	Баллы
Тест. За каждый правильный ответ	1

Безопасность персептронных нейросетевых моделей

Продолжительность проведения мероприятия промежуточной аттестации: **2 часа**
Условия проведения мероприятия: **в часы аудиторной работы**
Максимальный балл, выставляемый за мероприятие промежуточной аттестации: **10**
Проходной балл: **5**

Показатели оценивания	Баллы
Тест. За каждый правильный ответ	.5

Безопсаность глубоких сверточных сетей

Продолжительность проведения мероприятия промежуточной аттестации: **2 часа**
Условия проведения мероприятия: **в часы аудиторной работы**
Максимальный балл, выставляемый за мероприятие промежуточной аттестации: **10**
Проходной балл: **5**

Показатели оценивания	Баллы
Тест. За каждый правильный ответ	.5

Безопасность нейросетей- трансформеров

Продолжительность проведения мероприятия промежуточной аттестации: **2 часа**
Условия проведения мероприятия: **в часы аудиторной работы**
Максимальный балл, выставляемый за мероприятие промежуточной аттестации: **10**
Проходной балл: **5**

Показатели оценивания	Баллы
Тест. За каждый правильный ответ	.5

Безопасность больших языковых моделей

Продолжительность проведения мероприятия промежуточной аттестации: **4 часа**
Условия проведения мероприятия: **в часы аудиторной работы**
Максимальный балл, выставляемый за мероприятие промежуточной аттестации: **40**
Проходной балл: **17**

Показатели оценивания	Баллы
Презентация и защита проекта	40