МИНИСТЕРСТВО ТРАНСПОРТА РОССИЙСКОЙ ФЕДЕРАЦИИ

ФЕДЕРАЛЬНОЕ ГОСУДАРСТВЕННОЕ АВТОНОМНОЕ ОБРАЗОВАТЕЛЬНОЕ УЧРЕЖДЕНИЕ ВЫСШЕГО ОБРАЗОВАНИЯ

«РОССИЙСКИЙ УНИВЕРСИТЕТ ТРАНСПОРТА»
(РУТ (МИИТ)

Рабочая программа дисциплины (модуля),
как компонент образовательной программы
высшего образования - программы магистратуры
по направлению подготовки
10.04.01 Информационная безопасность,
утвержденной первым проректором РУТ (МИИТ)
Тимониным В.С.

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ (МОДУЛЯ)

Искусственный интеллект в информационной безопасности

Направление подготовки: 10.04.01 Информационная безопасность

Направленность (профиль): Безопасность компьютерных систем и сетей

Форма обучения: Очная

Рабочая программа дисциплины (модуля) в виде
электронного документа выгружена из единой
корпоративной информационной системы управления
университетом и соответствует оригиналу

Простая электронная подпись, выданная РУТ (МИИТ)
ID подписи: 4196
Подписал: заведующий кафедрой Желенков Борис Владимирович
Дата: 27.01.2023

1. Общие сведения о дисциплине (модуле).

Целью освоения учебной дисциплины «Искусственный интеллект в информационной безопасности» является формирование компетенций по основным разделам теоретических и практических основ проектирования подсистем антивирусной защиты компьютерных систем с использованием методов искусственного интеллекта.

Основными задачами дисциплины являются:

• Ознакомление с особенностями работы и проектирования современных систем информационной безопасности, реализующих методы искусственного интеллекта.

• Изучение особенностей практического применения средств антивирусной защиты и ее актуализации с использованием искусственного интеллекта.

• Изучение технологий обнаружения вирусов в современных системах антивирусной защиты с использованием методов искусственного интеллекта.

• Изучение методов построения решающих правил в современных системах информационной безопасности с использованием методов искусственного интеллекта.

• Изучение методов искусственного интеллекта и их применения в современных системах информационной безопасности.

Дисциплина предназначена для получения знаний, необходимых для решения следующих профессиональных задач (в соответствии с видами деятельности):

Научно-исследовательская деятельность

• Анализ и формализация задач информационной безопасности при их решении современными интеллектуальными системами;

• Исследование функциональных и метрологических свойств разрабатываемых интеллектуальных систем информационной безопасности;

• Исследование эффективности и помехоустойчивости разработанных систем информационной безопасности на базе методов искусственного интеллекта.

Проектная деятельность

• Сбор и анализ исходных данных для проектирования интеллектуальных систем информационной безопасности;

• Проектирование программных средств антивирусной защиты (систем, программ, баз данных и т.п.) в соответствии с техническим заданием с использованием методов искусственного интеллекта;

• Разработка и оформление проектной и рабочей технической

документации на системы информационной безопасности, реализующие методы искусственного интеллекта;

• Контроль соответствия разрабатываемых проектов и технической документации стандартам, техническим условиям и другим нормативным документам в области информационной безопасности и искусственного интеллекта.

Организационно-управленческая деятельность

• Разработка организационных методов реализации политики информационной безопасности предприятия при внедрении и эксплуатации современных интеллектуальных систем;

• Организация и управление коллективной разработкой интеллектуальной системы информационной безопасности предприятия.

2. Планируемые результаты обучения по дисциплине (модулю).

Перечень формируемых результатов освоения образовательной программы (компетенций) в результате обучения по дисциплине (модулю):

ОПК-1 - Способен обосновывать требования к системе обеспечения информационной безопасности и разрабатывать проект технического задания на ее создание;

ОПК-2 - Способен разрабатывать технический проект системы (подсистемы либо компонента системы) обеспечения информационной безопасности ;

ПК-1 - Способность проводить обоснование состава, характеристик и функциональных возможностей систем и средств обеспечения информационной безопасности объектов защиты на основе российских и международных стандартов.

Обучение по дисциплине (модулю) предполагает, что по его результатам обучающийся будет:

Знать:

-основные методы и принципы исследований и разработки новых решений при проектировании интеллектуальных средств информационной безопасности.

Уметь:

- искать и анализировать существующие решения в области разработки средств антивирусной защиты компьютерных систем, адаптировать их для решения задач в новых предметных областях.

Владеть:

-навыками анализа методов решения новых задач в области информационной безопасности, а также приемами разрешения проблемных ситуаций с помощью адаптации существующих или разработки новых интеллектуальных систем.

3. Объем дисциплины (модуля).

3.1. Общая трудоемкость дисциплины (модуля).

Общая трудоемкость дисциплины (модуля) составляет 5 з.е. (180 академических часа(ов).

3.2. Объем дисциплины (модуля) в форме контактной работы обучающихся с педагогическими работниками и (или) лицами, привлекаемыми к реализации образовательной программы на иных условиях, при проведении учебных занятий:

Тип учебных занятий	Количество часов	
	Всего	Сем. №3
Контактная работа при проведении учебных занятий (всего):	48	48
В том числе:		
Занятия лекционного типа	32	32
Занятия семинарского типа	16	16

3.3. Объем дисциплины (модуля) в форме самостоятельной работы обучающихся, а также в форме контактной работы обучающихся с педагогическими работниками и (или) лицами, привлекаемыми к реализации образовательной программы на иных условиях, при проведении промежуточной аттестации составляет 132 академических часа (ов).

3.4. При обучении по индивидуальному учебному плану, в том числе при ускоренном обучении, объем дисциплины (модуля) может быть реализован полностью в форме самостоятельной работы обучающихся, а также в форме контактной работы обучающихся с педагогическими работниками и (или) лицами, привлекаемыми к реализации образовательной программы на иных условиях, при проведении промежуточной аттестации.

4. Содержание дисциплины (модуля).

4.1. Занятия лекционного типа.

№ п/п	Тематика лекционных занятий / краткое содержание
1	Искусственный интеллект. Системы распознавания образов, их обучение и применение. Рассматриваемые вопросы: -Искусственный интеллект и системы распознавания вокруг нас: в технической и медицинской диагностике, в экономике, управлении; проблема формализации при постановке задачи распознавания и машинного обучения; - общая структура системы распознавания: рецепторы, классификаторы, эффекторы; - основные классы задач распознавания, терминология: объекты, образы, классы и кластеры; - обучение и самообучение систем распознавания; - эффективность распознавания и ее оценка; - особенности применения систем распознавания в задачах диагностики и управления; -современные системы виртуальной и дополненной реальности; - машинное обучение и самообучение в системах виртуальной и дополненной реальности; -поиск и анализ актуальной информации о современных системах распознавания образов и их использовании в задачах информационной безопасности.
2	Системы искусственного интеллекта. Информативные признаки и решающие правила. Рассматриваемые вопросы: - Количественные, качественные и классификационные признаки и оценка их информативности; - Метрики Фишера и Шеннона; - Построение информативного признакового пространства; - Метод корреляционных плеяд; - Особенности оценки бинарных и качественных признаков; - Расстояния между объектами и классами; - Метрики Евклида, Шеннона, Минковского, Махаланобиса; - Расстояния ближних соседей, дальних соседей, центров классов; - Решающие правила и их классификация; - Параметрические и непараметрические методы; - Дискриминантный анализ; - Метод k-ближайших соседей; - Статистические методы распознавания; - Разработка сложных систем и деревьев решений; - Метод последовательной дихотомии; - Деревья решений и их оптимизация; - Методы поиска; - Качество распознавания и его оценка; - Обучающая и проверяющая выборки; - Вероятностные и экономические методы оценки.
3	Системы искусственного интеллекта. Обучение «без учителя» и кластеризация. Рассматриваемые вопросы: - Обучение «без учителя» и кластеризация; - Понятия «кластер», «класс», «объект», «вектор признаков»; - Кластерный анализ и его применение в задачах обучения «без учителя» и GRID-технологиях: - Методы решения и эвристические процедуры; - Метод последовательных слияний; -Процедура Дубиссона; - Кривая Торндейка и оценка вероятного числа кластеров; - Кластеры-цепочки и их определение;

№ п/п	Тематика лекционных занятий / краткое содержание
	- Применение перспективных методов кластерного анализа при разработке современных GRID-систем.
4	Информационная безопасность и антивирусная защита. Вирусы и их классификация. Рассматриваемые вопросы: - Проблема защиты программ и данных; -Информационная и кибербезопасность; -Проблема криминализации информационного пространства; - Вирусные атаки: потенциальные угрозы и методы защиты; - Решение задач антивирусной защиты на мировом уровне; - Применение перспективных методов исследования и решения профессиональных задач при разработке программ антивирусной защиты в государственных и коммерческих предприятиях России. - Вредоносные программы: компьютерные вирусы, черви, трояны и пр.; - Загрузочные и файловые вирусы; - Макровирусы и скрипт-вирусы; - Шифрование и метаморфизм.; - Черви: сетевые, почтовые, IM, IRC, P2P; - Трояны: клавиатурные шпионы, похитители паролей, утилиты скрытого удаленного управления, анонимные прокси-сервера, утилиты дозвона, логические бомбы, модификаторы настроек браузера; - Условно опасные программы: Riskware, Рекламные утилиты (adware), Pornware, злые шутки. - Российские базы данных вирусов и зарегистрированных инцидентов и организационно-правовые основы их использования в системах антивирусной защиты российских государственных организаций и коммерческих предприятий.
5	Признаки присутствия на компьютере вредоносных программ и методы защиты от них. Рассматриваемые вопросы: - Общие сведения и виды проявлений: явные, косвенные и скрытые; - Изменение настроек браузера; - Всплывающие сообщения; - Несанкционированное обращение к Интернет; - Блокирование антивируса; - Блокирование антивирусных сайтов; - Сбои в системе или в работе других программ; - Почтовые уведомления; - Скрытые проявления: наличие в памяти подозрительных процессов; наличие на компьютере подозрительных файлов; наличие подозрительных ключей в системном реестре Windows; подозрительная сетевая активность; - Применение методов искусственного интеллекта; - Где искать: процессы, автозапуск, системный реестр Windows, конфигурационные файлы, сетевая активность; - Методы обнаружения вредоносных программ и защиты от них; - Организационные методы (правила поведения, политика безопасности); - Технические методы (брэндмауэры, средства борьбы со спамом, закладки и пр.); - Черные и белые списки адресов; - Базы данных образцов спама; - Самообучение; - Анализ служебных заголовков; - Применение методов искусственного интеллекта; - Поиск и анализ актуальной информации о современных признаках присутствия на компьютере вредоносных программ; - Проектирование программ обнаружения признаков присутствия вредоносных программ с использованием методов искусственного интеллекта.

№ п/п	Тематика лекционных занятий / краткое содержание
6	Основы работы антивирусных программ. Применение методов распознавания образов. Рассматриваемые вопросы: - Сигнатурные методы и эвристические методы.; -Сигнатурный анализ; - Эвристики; - Поиск вируса, похожего на известные: вероятность ошибочно определить наличие в файле вируса, невозможность лечения, низкая эффективность; - Поиск вируса, выполняющего подозрительные действия: удаление файла, запись в файл, запись в определенные области системного реестра, открытие порта на прослушивание, перехват данных вводимых с клавиатуры, рассылка писем; - Проблемы: ложные срабатывания, невозможность лечения, невысокая эффективность; - Базовые модули антивирусного ПО: модуль обновления, модуль планирования, модуль управления; - Функционал блока управления: Поддержка удаленного управления и настройки; - - Защита настроек от изменений, карантин; - Тестирование работы антивируса. -Применение перспективных методов при разработке современных антивирусных программ и систем информационной безопасности на базе методов искусственного интеллекта; -Проектирование базовых модулей антивирусного ПО.
7	Современные методы защиты от вирусов на базе методов искусственного интеллекта. Рассматриваемые вопросы: - Методы, основанные на анализе содержимого файлов (как файлов данных, так и файлов с кодами команд). К этой группе относятся сканирование сигнатур вирусов, а также проверка целостности и сканирование подозрительных команд; -Методы, основанные на отслеживании поведения программ при их выполнении. Эти методы заключаются в протоколировании всех событий, угрожающих безопасности системы и происходящих либо при реальном выполнении проверяемого кода, либо при его программной эмуляции; -Методы регламентации порядка работы с файлами и программами. Эти методы относятся к административным мерам обеспечения безопасности. Один из наиболее распространенных методов этой группы состоит в том, что в системе (компьютере или корпоративной сети) выполняются только те программы, запись о которых присутствует в списке программ, разрешенных к выполнению в данной системе. Этот список формируется администратором сети из проверенного программного обеспечения; -Наиболее популярные антивирусные программы и их особенности. McAfee, Norton, Panda, Avira, Bitdefender, Bullguard, Heimdal. Антивирус Касперского; -Применение методов искусственного интеллекта в наиболее популярных антивирусных программах в современных корпоративных системах киберзащиты.
8	Антивирусная защита домашнего компьютера и компьютерной сети с использованием методов искусственного интеллекта. Рассматриваемые вопросы: -Антивирусное программное обеспечение; - Программы для защиты от несанкционированного доступа и сетевых хакерских атак; - Фильтры нежелательной корреспонденции; - Проверка в режиме реального времени; - Проверка по требованию; - Поддержание актуальности антивирусных баз; - Фильтрация нежелательных электронных сообщений; - Персональная антиспамовая программа; - Применение методов искусственного интеллекта в рассмотренных программах; - Применение перспективных методов при разработке антивирусных программ;

№ п/п	Тематика лекционных занятий / краткое содержание
	- Проектирование антивирусного ПО для защиты домашнего компьютера на базе методов искусственного интеллекта; -Основы построения локальной компьютерной сети; - Рабочие станции и сетевые серверы, почтовые серверы и шлюзы; - Уровни антивирусной защиты: уровень защиты рабочих станций и сетевых серверов, уровень защиты почтовых серверов, уровень защиты шлюзов; - Централизованное управление антивирусной защитой; - Компоненты системы удаленного централизованного управления: клиентская антивирусная программа, сервер администрирования, агент администрирования, консоль администрирования; - Организация сбора статистики в системе антивирусной защиты и использование этой информации в интеллектуальных системах информационной безопасности; - Червь Caribe - вредоносная программа для мобильных телефонов; - Антивирусы для мобильных устройств; - Политики обеспечения информационной безопасности при работе с мобильными устройствами. Политика «нулевого доверия»; -Разработка организационных методов реализации политики безопасности предприятия при проектировании системы антивирусной защиты для удаленных рабочих мест; -Организация и управление коллективной разработкой системы антивирусной защиты корпоративной сети предприятия, включающей удаленные рабочие места; Применение методов искусственного интеллекта.

4.2. Занятия семинарского типа.

Практические занятия

№ п/п	Тематика практических занятий/краткое содержание
1	1. Тема: Построение признакового пространства для системы распознавания образов. В результате выполнения практического задания студент получает навыки в построении признакового пространства для разработки системы распознавания (обучение «с учителем»). 2. Тема: Построение решающих правил для системы распознавания образов. В результате выполнения практического задания студент получает навыки в построении решающих правил для разработки системы распознавания (обучение «с учителем»). 3. Тема: Обучение "без учителя". Кластерный анализ в системах машинного обучения. В результате выполнения практического задания студент получает навыки в решении задач обучения «без учителя» в системах искусственного интеллекта. 4. Тема: Антивирусная защита домашнего компьютера В результате выполнения практического задания студент получает навыки в настройке для защиты домашнего компьютера Microsoft Defender, а также навыки в настройке для защиты домашнего компьютера двух популярных антивирусов и содержательном сравнительном анализе их работы. Анализируются методы искусственного интеллекта применяемые в антивирусных программах. 5. Тема: Антивирусная защита компьютерной сети В результате выполнения практического задания студент получает навыки в настройке для защиты компьютерной сети Microsoft Defender, а также навыки в настройке для защиты компьютерной сети двух популярных антивирусов и содержательном сравнительном анализе их работы. Анализируются методы искусственного интеллекта применяемые в антивирусных программах.

4.3. Самостоятельная работа обучающихся.

№ п/п	Вид самостоятельной работы
1	Работа с лекционным материалом
2	Подготовка к практическим занятиям
3	Выполнение курсовой работы
4	Изучение вопросов для самостоятельной дополнительной проработки
5	Выполнение курсовой работы.
6	Подготовка к промежуточной аттестации.
7	Подготовка к текущему контролю.

4.4. Примерный перечень тем курсовых работ

1. Перспективы применения машинного обучения для обнаружения вредоносных программ.

2. Интеллектуальные методы защиты от атак на беспроводные сети.

3. Антивирусная защита ОС семейства Эльбрус с использованием методов искусственного интеллекта.

4. Методы защиты конфиденциальной информации при проведении переговоров в неспециализированных помещениях.

5. Настройка антивирусного программного обеспечения для защиты веб-сайта с использованием методов искусственного интеллекта.

6. Методы защиты новостных порталов от вирусных атак с использованием методов искусственного интеллекта.

7. Методы защиты от атак, связанных с системными структурами жёстких дисков, с использованием методов искусственного интеллекта.

8. Антивирусная защита ИСПДн на основе отечественной аппаратно-программной платформы с использованием методов искусственного интеллекта.

9. Методы защиты технологии SDN

10. Обеспечение антивирусной защиты цифровых систем управления запасами в логистике терминально-складских комплексов с использованием методов искусственного интеллекта.

11. Обеспечение антивирусной защиты Департамента Логистики и Планирования компании Z с использованием методов искусственного интеллекта.

12. Обеспечение антивирусной защиты мультимодальных транспортно-

логистических центров с использованием методов искусственного интеллекта.

13. Обеспечение антивирусной защиты персонального компьютера при разработке платформы имитационной модели складского процесса с использованием методов искусственного интеллекта.

14. Обеспечение антивирусной защиты цифровой платформы «Личные диаметры» с использованием методов искусственного интеллекта.

15. Обеспечение антивирусной защиты в бизнес процессах закупочной логистики с использованием методов искусственного интеллекта.

16. Обеспечение антивирусной защиты при работе оператора, использующего технологию «Физический интернет».

17. Обеспечение антивирусной защиты при работе оператора, использующего цифровую платформу ЭТП ГП.

18. Обеспечение антивирусной защиты контейнерного терминала компании «UNIVERSAL LOGISTICS SERVICES» (ULS) с использованием методов искусственного интеллекта.

19. Обеспечение антивирусной защиты Департамента управления персоналом компании ПГК с использованием методов искусственного интеллекта.

20. Организация антивирусной защиты от автоматизированных методов сбора информации из открытых интернет-ресурсов с использованием методов искусственного интеллекта.

5. Перечень изданий, которые рекомендуется использовать при освоении дисциплины (модуля).

№ п/п	Библиографическое описание	Место доступа
1	Леонтьев А. С. Защита информации: учебное пособие. МИРЭА - Российский технологический университет 2021.-79с. - ISBN 978-5-9948-4110-5	https://e.lanbook.com/book/182491 (дата обращения: 02.10.2022).- Текст электронный.
2	Полупанов Д.В. Нейроинформатика: учебное пособие. Башкирский государственный университет, 2020- 132с. – ISBN 978-5-7477-5229-0	https://e.lanbook.com/book/179917 (дата обращения: 23.11.2022).- Текст электронный.
3	Толмачев С.Г. Основы искусственного интеллекта: учебное пособие. Балтийский государственный технический университет «Военмех» имени Д.Ф. Устинова, 2017.-132с. – ISBN 978-5-906920-53-9	https://e.lanbook.com/book/121872 (дата обращения: 23.11.2022).- Текст электронный.
4	Чио К., Фримэн Д. Машинное обучение и безопасность. – Москва, ДМК-Пресс, 2020.-388с. –	https://e.lanbook.com/book/131707 (дата обращения: 23.11.2022).-

	ISBN 978-5-97060-713-8	Текст электронный.
5	Араки М. Манга: машинное обучение. – Москва, ДМК-Пресс, 2020.-214с. – ISBN 978-5-97060-830-2	https://e.lanbook.com/book/179473 (дата обращения: 23.11.2022).- Текст электронный.
6	https://e.lanbook.com/book/179473 (дата обращения: 23.11.2022).- Текст электронный.	https://e.lanbook.com/book/241211 (дата обращения: 23.11.2022).- Текст электронный.
7	Лекун Я. Как учится машина: Революция в области нейронных сетей и глубокого обучения. — Москва, Альпина Паблишер, 2021.- 351с. - ISBN 978-5-907470-52-5	https://e.lanbook.com/book/213980 (дата обращения: 23.11.2022).- Текст электронный.

6. Перечень современных профессиональных баз данных и информационных справочных систем, которые могут использоваться при освоении дисциплины (модуля).

- Форум специалистов по информационным технологиям http://citforum.ru/
- Интернет-университет информационных технологий http://www.intuit.ru/
- Тематический форум по информационным технологиям http://habrahabr.ru/
- ЭБС "Лань" https://e.lanbook.com/book/

7. Перечень лицензионного и свободно распространяемого программного обеспечения, в том числе отечественного производства, необходимого для освоения дисциплины (модуля).

- Microsoft Windows
- Microsoft Office

При организации обучения по дисциплине (модулю) с применением электронного обучения и дистанционных образовательных технологий необходим доступ каждого студента к информационным ресурсам – библиотечному фонду Университета, сетевым ресурсам и информационно-телекоммуникационной сети «Интернет».

В случае проведении занятий с применением электронного обучения и дистанционных образовательных технологий может понадобиться наличие следующего программного обеспечения (или их аналогов): ОС Windows, Microsoft Office, Интернет-браузер, Microsoft Teams и т.д.

В образовательном процессе, при проведении занятий с применением электронного обучения и дистанционных образовательных технологий, могут применяться следующие средства коммуникаций: ЭИОС РУТ(МИИТ),

Microsoft Teams, электронная почта и т.п.

8. Описание материально-технической базы, необходимой для осуществления образовательного процесса по дисциплине (модулю).

- Учебная аудитория для проведения занятий лекционного типа, групповых и индивидуальных консультаций

Проектор для вывода изображения на экран для студентов, акустическая система, место для преподавателя оснащенное компьютером. Аудитория подключена к интернету РУТ(МИИТ).

- Учебная аудитория для проведения практических работ, персональные компьютеры

- В случае проведении занятий с применением электронного обучения и дистанционных образовательных технологий необходимо наличие компьютерной техники, для организации коллективных и индивидуальных форм общения педагогических работников со студентами, посредством используемых средств коммуникации.

Допускается замена оборудования его виртуальными аналогами.

9. Форма промежуточной аттестации:

Курсовая работа в 3 семестре.
Экзамен в 3 семестре.

10. Оценочные материалы.

Оценочные материалы, применяемые при проведении промежуточной аттестации, разрабатываются в соответствии с локальным нормативным актом РУТ (МИИТ).

Авторы:

доцент, доцент, к.н. кафедры
«Вычислительные системы, сети и
информационная безопасность» С.В. Малинский

Согласовано:

Заведующий кафедрой ВССиИБ Б.В. Желенков

Председатель учебно-методической
комиссии Н.А. Клычева