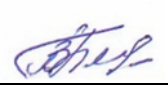
МИНОБРНАУКИ РОССИИ

Федеральное государственное бюджетное
образовательное учреждение высшего образования
«Тульский государственный университет»

Политехнический институт
Кафедра «Инструментальные и метрологические системы»

Утверждено на заседании кафедры
«Инструментальные и метрологические системы»
18 сентября 2024 г., протокол № 1

И.о заведующего кафедрой

 В.А. Белякова

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ (МОДУЛЯ)
Информационная безопасность и технологии искусственного интеллекта

основной профессиональной образовательной программы
высшего образования – программы бакалавриата

по направлению подготовки
27.03.04 Управление в технических системах

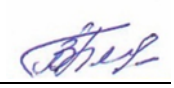
с направленностью (профилем)
Цифровые технологии в системах обеспечения качества

Форма обучения: очная

Идентификационный номер образовательной программы: 270304-01-24

Тула 2024 год

Разработчик:

Белякова В.А. к.т.н., доцент 

(ФИО, должность, ученая степень, ученое звание) *(подпись)*

1 Цель и задачи освоения дисциплины (модуля)

Целью освоения дисциплины (модуля) является усвоение формирование компетенций по основным разделам теоретических и практических основ проектирования подсистем антивирусной защиты компьютерных систем с использованием методов искусственного интеллекта

Задачами освоения дисциплины (модуля) 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.

2 Место дисциплины (модуля) в структуре основной профессиональной образовательной программы

Дисциплина (модуль) относится к обязательной части основной профессиональной образовательной программы.

Дисциплина (модуль) изучается в 8 семестре.

3 Перечень планируемых результатов обучения по дисциплине (модулю)

Перечень планируемых результатов обучения по дисциплине (модулю), соотнесенных с планируемыми результатами освоения основной профессиональной образовательной программы (формируемыми компетенциями) и индикаторами их достижения, установленными в общей характеристике основной профессиональной образовательной программы, приведён ниже.

В результате освоения дисциплины (модуля) обучающийся должен:

Знать:

1) нормативные правовые акты, регулирующие сферу интеллектуальной собственности; виды интеллектуальной собственности; права и обязанности авторов произведений, изобретений, промышленных образцов, полезных моделей и товарных знаков и др.; способы защиты прав в сфере интеллектуальной собственности. (код компетенции – ОПК-5 код индикатора - ОПК-5.1).

Уметь:

1) анализировать особенности правоотношений, возникающих в сфере интеллектуальной собственности; оперировать понятиями и определениями курса; реализовать полученные теоретические знания в условиях практической деятельности (код компетенции – ОПК-5, код индикатора - ОПК-5.2).

Владеть:

1) навыками работы с нормативными правовыми актами РФ, регулирующими сферу интеллектуальной собственности; применения способов защиты интеллектуальной собственности в практической деятельности. (код компетенции – ОПК-5, код индикатора - ОПК-5.3).

Полные наименования компетенций индикаторов их достижения представлены в общей характеристике основной профессиональной образовательной программы.

4 Объем и содержание дисциплины (модуля)

4.1 Объем дисциплины (модуля), объем контактной и самостоятельной работы обучающегося при освоении дисциплины (модуля), формы промежуточной аттестации по дисциплине (модулю)

Номер семестра	Формы промежуточной аттестации	Общий объем в зачетных единицах	Общий объем в академических часах	Объем контактной работы в академических часах						Объем самостоятельной работы в академических часах
				Лекционные занятия	Практические (семинарские) занятия	Лабораторные работы	Клинические практические занятия	Консультации	Промежуточная аттестация	
Очная форма обучения										
8	ДЗ	4	144	36	24	-	-	-	0,25	83,75
Итого	-	4	144	36	24	-	-	-	0,25	83,75

Условные сокращения: Э – экзамен, ЗЧ – зачет, ДЗ – дифференцированный зачет (зачет с оценкой), КП – защита курсового проекта, КР – защита курсовой работы.

4.2 Содержание лекционных занятий

Очная форма обучения

№ п/п	Темы лекционных занятий
8 семестр	
	1. Искусственный интеллект. Системы распознавания образов, их обучение и применение. - 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;

№ п/п	Темы лекционных занятий
1	- 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. - 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. - 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; - Применение перспективных методов кластерного анализа при разработке современных GRIDсистем 4. Информационная безопасность и антивирусная защита. Вирусы и их классификация. - 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;

№ п/п	Темы лекционных занятий
	- 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. - 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	Темы лекционных занятий
	6. Основы работы антивирусных программ. Применение методов распознавания образов. - 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. - 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. -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	Темы лекционных занятий
	- 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.

4.3 Содержание практических (семинарских) занятий

Очная форма обучения

№ п/п	Темы практических (семинарских) занятий
	8 семестр
1	Информационная безопасность (ИБ) в области искусственного интеллекта. Основные понятия
2	Основные стандарты в области обеспечения информационной безопасности систем искусственного интеллекта. Политика безопасности
3	Основные виды сетевых и компьютерных угроз. Средства и методы защиты от сетевых компьютерных угроз
4	Методы анализа рисков. Понятие уязвимости. Классификация угроз. Методы оценки ущерба от реализации угроз информационной безопасности систем искусственного интеллекта.
5	Специализированные программноаппаратные средства защиты информации для систем искусственного интеллекта. Основные направления применения криптографических технологий при защите систем искусственного интеллекта
6	Особенности защиты информации в базах данных
7	Шифрование информации методом простой замены

№ п/п	Темы практических (семинарских) занятий
8	Методы представления знаний: процедурные представления, логические представления, семантические сети, фреймы. Анализ процессов и систем информационной безопасности
9	Анализ параметров безопасности сетей и систем. Нечеткий аппроксиматор. Эффективность нечетких систем управления информационной безопасностью
10	Моделирование интеллектуальной системы информационной безопасности
11	Защита документов, созданных в Microsoft Word. Защита документов, созданных в Microsoft Excel Защита документов, созданных в Microsoft Access. Защита файла паролем.
12	Защита ПК от вредоносных закладок (разрушающих программных средств)

4.4 Содержание лабораторных работ

Занятия указанного типа не предусмотрены основной профессиональной образовательной программой.

4.5 Содержание клинических практических занятий

Занятия указанного типа не предусмотрены основной профессиональной образовательной программой.

4.6 Содержание самостоятельной работы обучающегося

Очная форма обучения

№ п/п	Виды и формы самостоятельной работы
	8 **семестр**
1	*Подготовка к практическим (семинарским) занятиям*
2	*Подготовка к промежуточной аттестации и ее прохождение*

5 Система формирования оценки результатов обучения по дисциплине (модулю) в рамках текущего контроля успеваемости и промежуточной аттестации обучающегося

Очная форма обучения *(если предусмотрено основной профессиональной образовательной программой)*

Мероприятия текущего контроля успеваемости и промежуточной аттестации обучающегося			Максимальное количество баллов
		8 **семестр**	
Текущий контроль успеваемости	Первый рубежный контроль	**Оцениваемая учебная деятельность обучающегося:**	
		Посещение лекционных занятий	5
		Работа на практических (семинарских) занятиях	5
		Подготовка реферата	10
		Контрольная работа	10
		Итого	30
	Второй рубежный	**Оцениваемая учебная деятельность обучающегося:**	

Мероприятия текущего контроля успеваемости и промежуточной аттестации обучающегося			Максимальное количество баллов
	контроль	Посещение лекционных занятий	5
		Работа на практических (семинарских) занятиях	5
		Подготовка реферата	5
		Подготовка эссе	5
		Контрольная работа	10
		Итого	30
Промежуточная аттестация	Дифференцированный зачет		40 (100*)

* В случае отказа обучающегося от результатов текущего контроля успеваемости

Шкала соответствия оценок в стобалльной и академической системах оценивания результатов обучения по дисциплине (модулю)

Система оценивания результатов обучения	Оценки			
Стобалльная система оценивания	0 – 39	40 – 60	61 – 80	81 – 100
Академическая система оценивания (экзамен, дифференцированный зачет, защита курсового проекта, защита курсовой работы)	Неудовлетворительно	Удовлетворительно	Хорошо	Отлично
Академическая система оценивания (зачет)	Не зачтено	Зачтено		

6 Описание материально-технической базы (включая оборудование и технические средства обучения), необходимой для осуществления образовательного процесса по дисциплине (модулю)

Для осуществления образовательного процесса по дисциплине (модулю) требуется аудитория оснащенная видеопроектором, настенным экраном, ноутбуком. Специализированная мебель: столы и стулья обучающихся, стол и стул преподавателя.

Демонстрационное оборудование: доска для написания мелом – 1 шт., проектор – 1 шт., экран настенный – 1 шт., ноутбук - 1 шт

7 Перечень основной и дополнительной учебной литературы, необходимой для освоения дисциплины (модуля)

7.1 Основная литература

Васильков А.В. Безопасность и управление доступом в информационных системах / А.В. Васильков, И.А. Васильков.— Москва : ФОРУМ: ИНФРА-М, 2013.— 368 с.

2. Жигулин Г.П. Организационное и правовое обеспечение информационной безопасности / Г.П. Жигулин.— Санкт-Петербург : СПбНИУИТМО, 2014.— 173 с.

3. Теоретические основы компьютерной безопасности / П.Н. Девянин [и др.].— Москва : Радио и связь, 2000.— 192 с.

4. Бардаев Э.А. Документоведение : учебник для студ. высш. учеб. заведений / Э.А. Бардаев, В.Б. Кравченко.— Москва : Издательский центр «Академия», 2008.— 304 с.

5. Малюк А.А. Введение в защиту информации в автома тизированных системах / А.А. Малюк, С.В. Пазизин, Н.С. Погожин.— Москва : Горячая линия — Телеком, 2001.— 148 с.

6. Федин, Ф. О. Информационная безопасность : учебное пособие / Ф. О. Федин, В. П. Офицеров, Ф. Ф. Федин. — Москва : Московский городской педагогический университет, 2011. — 260 с. — Текст : электронный // Цифровой образовательный ресурс IPR SMART : [сайт]. — URL: https://www.iprbookshop.ru/26486.html. — Режим доступа: для авторизир. пользователей

7.2 Дополнительная литература

1. Мельников В.В. Безопасность информации в автоматизированных системах / В.В. Мельников.— Москва : Финансы и статистика, 2003.— 368 с.

7. Гайдамакин Н.А. Разграничение доступа к информации в компьютерных системах / Н.А. Гайдамакин.— Екатеринбург : Изд-во Урал. ун-та, 2003.— 328 с.

8. Зегжда Д. П. Основы безопасности информационных систем / Д.П. Зегжда, А.М. Ивашко.— Москва : Горячая линяя — Телеком, 2000.— 452 с.

9. Барсуков В.С. Безопасность: технологии, средства, услуги/ В.С.Барсуков.— Москва : КУДИЦ-ОБРАЗ, 2001–496с.

10. Расторгуев С.П. Информационные войны / С.П. Расторгуев. — Москва : «Финансы и статистика», 1998.— 415 с

11. Хорев, П.Б. Методы и средства защиты информации в компьютерных системах : учеб.пособие для вузов / П.Б.Хорев .— 2-е изд.,стер. — М. : Академия, 2006 .— 256с. : ил. — (Высшее профессиональное образование:Информатика и вычислительная техника) .— Библиогр.в конце кн. — ISBN 978-5-7695-3288-2 /в пер./ : 180.40 (6 экз.).

12. Куприянов, А.И. Основы защиты информации : учеб.пособие / А.И.Куприянов,А.В.Сахаров,В.А.Шевцов .— 2-е изд.,стер. — М. : Академия, 2007 .— 256с. : ил. — (Высшее профессиональное образование:Радиоэлектроника) .— Библиогр.в конце кн. — ISBN 978-5-7695-4416-3 /в пер./ : 247.00 (10 экз.)

13. Мельников, В.П. Информационная безопасность и защита информации : учеб.пособие для вузов / В.П.Мельников,С.А.Клейменов,А.М.Петраков;под ред.С.А.Клейменова .— 3-е изд.,стер. — М. : Академия, 2008 .— 336с. — (Высшее профессиональное образование:Информатика и вычислительная техника) .— Библиогр.в конце кн. — ISBN 978-5-7695-4884-0 /в пер./ : 239.80 (5 экз.).

14. Остапенко, Г.А. Информационные операции и атаки в социотехнических системах : учеб.пособие для вузов / Г.А.Остапенко;под ред.В.И.Борисова .— М. : Горячая линия-Телеком, 2007 .— 134с. : ил. — (Учебное пособие для высших учебных заведений.Специальность) .— Библиогр.в конце кн. — ISBN 5-93517-288-7 : 102.85 (3 экз.).

8 Перечень ресурсов информационно-телекоммуникационной сети «Интернет», необходимых для освоения дисциплины (модуля)

1. https://e.lanbook.com/ - ЭБС «Лань», доступ авторизованный
2. https://urait.ru/ - Образовательная платформа «Юрайт», доступ авторизованный
3. https://www.iprbookshop.ru/ - Цифровой образовательный ресурс IPR SMART, доступ авторизованный
4. https://tsutula.bookonlime.ru/ - ЭБС ТулГУ «BookOnLime» учебные издания ТулГУ по всем дисциплинам, доступ авторизованный
5. https://www.studentlibrary.ru/ - ЭБС «Консультант студента», доступ авторизованный (указывается для строительных и медицинских специальностей!)
6. https://dlib.eastview.com/browse/udb/12 - Политематическая база данных периодических изданий East View, доступ авторизованный
7. https://cyberleninka.ru/ - Научная электронная библиотека «КиберЛенинка» , доступ свободный
8. https://www.elibrary.ru/ - Научная электронная библиотека eLibrary.ru, доступ свободный

9 Перечень информационных технологий, необходимых для осуществления образовательного процесса по дисциплине (модулю)

9.1 Перечень необходимого ежегодно обновляемого лицензионного и свободно распространяемого программного обеспечения, в том числе отечественного производства

1. Текстовый редактор Microsoft Word;
2. Программа для работы с электронными таблицами Microsoft Excel;
3. Программа подготовки презентаций Microsoft PowerPoint;
4. САПР КОМПАС-3D;
5. Пакет офисных приложений «МойОфис».

9.2 Перечень необходимых современных профессиональных баз данных и информационных справочных систем

1. Справочная правовая система «КонсультантПлюс».