

Аннотация дисциплины Б.1.2.11 Дисциплина. Компьютерная вирусология

Дисциплина "Компьютерная вирусология" изучается обучающимися по основной профессиональной образовательной программе "Разработка программных систем и систем искусственного интеллекта" направления подготовки "09.03.04 Программная инженерия". Дисциплина изучается в 8 семестре. Общая трудоемкость дисциплины составляет 144/4 часов/з.ед. Самостоятельная работа заключается в выполнении работ, указанных в разделе 4.

В ходе изучения дисциплины осуществляется текущий контроль в форме технологии рейтингового контроля в соответствии с технологической карты дисциплины, размещенной на электронном курсе, а также промежуточный контроль в форме балльно-рейтинговый контроль.

Целью изучения дисциплины является формирование следующих компетенций:

1. ML-1 Способен применять знания об истории развития и трендах современного ИИ для формулирования корректных постановок задач и поиска перспективных способов решения проблем с помощью ИИ
2. ML-2 Способен применять фундаментальные принципы и методы машинного обучения включая подготовку данных оценку качества моделей и работу с признаками
3. ПК-4 Владение навыками использования операционных систем, сетевых технологий, средств разработки программного интерфейса, применения языков и методов формальных

В ходе изучения дисциплины последовательно рассматриваются темы:

1. Лекция №1. Вводная лекция. История становления курса. Понятие модели угроз. Классификация моделей угроз.
2. Лекция №2. Вредоносная программа: правовая квалификация. Основные термины и определения. Признаки вредоносности. Ситуационное моделирование.
3. Лекция №3. Классификация вредоносных программ и программных компонент. Алгоритмическая модель типового компьютерного вируса.
4. Лекция №4. Технологии обнаружения признаков вредоносности программ и программных компонент: случай скриптовых языков программирования, общий случай. Технологии ИИ в обнаружении признаков вредоносности программ: продукционные подходы, технологии БЯМ.
5. Лекция №5. Проблемы формального определения компьютерного вируса. Классификационные признаки компьютерных вирусов и особенности поведения инфицированных программ и программных систем. Основной классификационный признак в контексте теоретико-множественного формализма. Современное параопределение компьютерного вируса. ГОСТы и жизненный цикл вредоносных программ.
6. Лекция №6. Теоретико-алгоритмические проблемы обнаружения компьютерных вирусов: основные теоремы.
7. Лекция №7. Обнаружение вредоносных программ на практике. Технологии ИИ в обнаружении РПВ: методология. Ожидания от сильного ИИ. Проблема скрытых вычислений.
8. Лекция №8. Существование компьютерных вирусов в контексте базовых архитектур вычислительных систем. Субъектно-объектный формализм при анализе проблемы существования компьютерных вирусов.
9. Лекция №9. Понятие политики безопасности. Основные политики безопасности противодействия угрозе существования компьютерных вирусов.

Основными стратегическими образовательными технологиями являются: исследовательские, лекционные занятия, практические и лабораторные занятия, процедуры

самообучения, дискуссионные, доступ обеспечивается с помощью электронного курса и сервисов образовательного портала пгту на платформе lms moodle (elearning.vlgatech.net), интегрированного с федеральной платформой гис сцос online.edu.ru открытый образовательный портал (moored.net)..

В рамках указанных технологий применяются тактические образовательные технологии: классическая лекция, проблемная лекция, задания, игровое проектирование, информационные, лекция с обсуждением новых научных достижений в сфере ии по результатам конференции и публикаций и др.), семинары с ит-практиками, конкурсы, хакатоны, кейс-чемпионаты, мастер-классы, командные проектные задания и др..