



СПбГЭТУ «ЛЭТИ»
ПЕРВЫЙ ЭЛЕКТРОТЕХНИЧЕСКИЙ



А.Е. Сулавко

Машинное обучение в приложениях биометрии

Заключение

Конспект лекции

СПбГЭТУ «ЛЭТИ», 2022 г.



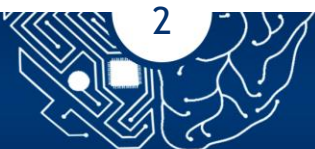


ЗАКЛЮЧЕНИЕ

В данном курсе были рассмотрены основные подходы к использованию машинного обучения в приложениях биометрии, каждый из которых, в конечном счете, заключается в решении задачи классификации биометрических образов (с разделением на классы «Свой»/«Чужой»). Среди изученных подходов:

- статистический подход, по сей день, успешно применяющийся в задачах биометрической аутентификации и представляющий собой «классику» реализации подобных задач;
- нейросетевой подход, относительно новый по сравнению со статистическими методами, однако демонстрирующий высокую надежность и эффективность, в особенности, в лице биометрико-криптографического подхода. К наиболее перспективной области развития нейросетевого подхода в биометрии можно отнести способы применения глубокого обучения и аппарата многослойных нейронных сетей для задач извлечения признаков из биометрических образов.
- подход ансамблирования моделей, заключающийся в объединении нескольких алгоритмов машинного обучения с целью получения лучшей эффективности в решении задачи классификации биометрических образов. Данный подход является наиболее перспективным как с точки зрения машинного обучения, так и с точки зрения биометрии, так как позволяет создавать максимально устойчивые к атакам системы, используя преимущество сразу нескольких алгоритмов.

Несмотря на все перечисленные выше способы реализации машинного обучения в биометрии, очевидным остается тот факт, что биометрические системы продолжают и дальше развиваться, в частности, с применением технологий искусственного интеллекта и машинного обучения. В таком случае, отдельной областью исследований представляются вопросы защиты используемого в биометрии искусственного интеллекта от разного рода атак, направленных на компрометацию данных и зондирования моделей. Такие атаки, как атака «одного бита» («на решающий бит»), «ключ под ковриком», состязательные атаки (в том числе атаки «извлечения знаний») в той или иной степени актуальны для наиболее ответственных приложений (каковыми являются биометрические системы), неправильная работа которых может





повлечь за собой материальный ущерб, нарушение информационной безопасности, угрозу жизни и здоровью граждан.

На сегодняшний день нет стандартов (как международных, так и российских), которые бы регламентировали технические аспекты защиты искусственного интеллекта от угрозы реализации всех перечисленных атак, а также особенности построения искусственного интеллекта, изначально устойчивого к этим атакам.

Искусственный интеллект должен проходить процедуру аутентификации. Для его авторизации необходимо использовать криптографический ключ или случайный длинный пароль, который должен храниться безопасно в защищенной памяти ИИ (ключ должен «помнить» только ИИ). В особо ответственных приложениях должна быть предусмотрена возможность смены ключа (пароля), используемого для авторизации ИИ. Для подобной перенастройки нужна процедура быстрого автоматического обучения блока защиты, отвечающего за связывание ключа с другими знаниями ИИ (контроль над возникновением переобучения должен быть автоматическим). Защищенное исполнение искусственного интеллекта в задачах классификации концептуально может быть построено по принципу преобразователя распознаваемых (классифицируемых) образов в длинный криптографический ключ, который можно ассоциировать с определённым управляющим воздействием. Только объект управления должен иметь представление о том, как применять возникающий на выходе ИИ ключ.

Как было рассмотрено в третьей главе данного курса, подобный подход частично реализуется НПБК, обученном по ГОСТ Р 52633.5-2011. На сегодняшний день существуют отличные от данного подхода реализации НПБК на базе разных типов нейронов, архитектур нейронных сетей и их ансамблей. Однако по-прежнему ряд вопросов, связанных с безопасностью ИИ в биометрии остаются открытыми, что, несомненно, представляет собой еще одну перспективную область исследований.

