

ПРИМЕНЕНИЕ ИСКУССТВЕННОГО ИНТЕЛЛЕКТА В ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

Калмухамедова Альбина Бакыткельдиевна

студент, кафедра пожарной безопасности Уфимского государственного технического авиационного университета, РФ, г. Уфа

Цыпышева Марина Викторовна

студент, кафедра пожарной безопасности Уфимского государственного технического авиационного университета, РФ, г. Уфа

Миниахметов Рамазан Маратович

студент, кафедра вычислительной техники и защиты информации Уфимского государственного технического авиационного университета, РФ, г. Уфа

Искусственный интеллект и связанные с ним термины машинное обучение и нейросети сегодня активно используют для продвижения нового поколения информационных систем. Специфика информационной безопасности, в отличие от остальных информационных технологий, в том, что обучение на старых данных неэффективно. Если дело касается распознавания лиц, планирования товарных запасов или машинного перевода текстов — то обучение на старых паттернах — основа успеха таких алгоритмов машинного обучения. Чем больше правильно распознанных лиц, правильно переведённых текстов, правильно спланированных запасов — тем лучше алгоритмы будут работать в будущем — объект изучения не будет сильно меняться и можно всё больше углубляться в детали — ведь нельзя ожидать, что у людей появится третий глаз или в языке радикально изменится морфология или синтаксис.

Основные задачи, которые требуется решать методами искусственного интеллекта в сфере обеспечения информационной безопасности:

- быстрое распознавание угроз;
- борьба с самообучающимся вредоносным ПО;
- анализ, недоступный не интеллектуальной системе защиты;
- построение мощной системы защиты на основе самообучения;
- обслуживание средств управления идентификацией и доступом к ресурсам и средств администрирования доступа;
- совершенствование современного антивирусного ПО, средств обнаружения атак, брандмауэров.

Для решения таких задач используются методы искусственного интеллекта:

- Продукционные (экспертные) системы;
- Байесовские сети;

- Искусственная нейронная сеть;
- Метод опорных векторов;

Продукционные (экспертные) системы основаны на продукциях — правилах вида «ЕСЛИ ТО», вырабатывающихся экспертами на основе опыта. Любая продукционная система состоит из трех основных компонентов:

- база знаний;
- рабочая память;
- механизм вывода.

База знаний содержит продукции, описывающие предметную область. В рабочей памяти хранится множество фактов, соответствующих ситуации, которые могут изменяться по мере применения правил. Механизм вывода служит для реализации логического вывода путем просмотра правил и фактов, нахождения соответствия между ними и изменения рабочей памяти.

Байесовские сети представляют собой модели событий и процессов на основе теории вероятностей и теории графов. Каждый узел является событием, описываемым случайной величиной. Если переменные (узлы) не соединены связями, то их считают условно независимыми. Все вершины, связанные с «родительскими» определяются таблицей условных вероятностей или функцией условных вероятностей. Для вершин «без родителей» вероятности ее состояний являются безусловными.

Искусственная нейронная сеть является упрощенной моделью мозга и представляет набор нейронов, соединенных между собой. Нейронные сети позволяют решать практические задачи, связанные с распознаванием и классификацией образов. Нейронные сети могут автоматически приобретать знания при обучении и обладают способностью к обобщению.

Метод опорных векторов — математический метод получения функции, решающей задачу классификации. Пусть два множества точек можно разделить плоскостью. Тогда таких плоскостей будет бесконечное множество. Выберем в качестве оптимальной плоскость, равноудаленную от ближайших точек-векторов обоих классов. Эти точки-вектора называются опорными. Поиск оптимальной плоскости приводит к задаче квадратичного программирования при множестве линейных ограничений неравенств.

Список литературы:

1. Котельников Е.В., Колеватов В.Ю. Методы искусственного интеллекта в задачах обеспечения безопасности компьютерных сетей : Статья. — 2010.
2. Павлов С. Н. Системы искусственного интеллекта : Учебное пособие. — 2011.
3. Подольский В.Е., Коробкова И.Л. Методы искусственного интеллекта для синтеза проектных решений : Учебное пособие. — 2010.
4. Зайцев О. Нейросети в системах безопасности [Текст] // ИТ-Спец. – 2007. – № 6. – С. 54-59.