УДК 004.8

БЕЗОПАСНОСТЬ МАШИННОГО ОБУЧЕНИЯ В БАНКОВСКОЙ СФЕРЕ

Шишко А.В. (Университет ИТМО)
Научный руководитель – к.т.н., доцент Волошина Н.В.
(Университет ИТМО)

Аннотация. Проблема безопасности машинного обучения является значимой при применении технологии в банковской сфере. В данной работе был произведен анализ влияния машинного обучения на безопасность банковских систем, установлены взаимосвязи влияния отдельных параметров обучаемой выборки на конечную безопасность обученной модели.

Введение. В наше время системы с применением технологии машинного обучения проникли во все сферы человеческой деятельности, банковская сфера не стала исключением. Вычислительные мощности современных компьютеров привели нас к возможности повсеместно использовать инструменты для анализа данных на основе машинного обучения. Данные инструменты существенно расширяет возможности по обработке данных позволяя достичь ранее недостижимых результатов. Однако, как и для любой другой бурно развивающиеся технологии, вопросы безопасности рассматриваются далеко не в первую очередь. Банковская сфера является одной из наиболее важной сферой человеческой деятельности, поэтому, при применении новых инструментов и технологий вопрос безопасности является одним из наиболее важных для рассмотрения. В контексте данного исследования были рассмотрены проблемы влияния обучающей выборки на безопасность нейронной сети, а также возможные проблемы с реализацией атаки на сеть.

Основная часть. Безопасное использование любой технологии или инструмента подразумевает уверенность в безопасности каждого структурного блока. Для обеспечения безопасности необходимо рассмотреть все возможные риски при применении определенного инструмента или технологии особенно в банковской сфере. В машинном обучении для обучения нейронной сети используются большие наборы структурированной информации, так называемые датасеты. Эти наборы включают в себя различные выборки данных, взятых из разных, не всегда верифицированных источников. В настоящее время, при выборе датасета ученые и исследователи не рассматривают возможности злоумышленника подмешивать к необходимым данным специальные микровыборки для обучения нейронной сети реакции на специальные паттерны особым, отличным от нормального поведения образом. В банковской сфере данное допущение может привести к крупным потерям, например, если в выборку для обучения торгового бота подмешать данные для реакции на определенный набор повышений и падений акции можно заставить бота купить или продать крупный объём ценных бумаг по невыгодной цене, что приведет к катастрофическим финансовым потерям. Также следует учесть возможность предугадывать поведение нейронной сети при добавлении в обучающую выборку специальных паттернов, что может компрометировать возможную стратегию покупки или продажи ценных бумаг. В данной работе были рассмотрены механизмы воздействия на нейронную сеть, а также возможные способы защиты от нежелательного воздействия.

Выводы. Банковская сфера активно использует инструменты на базе машинного обучения, поэтому, необходимо обеспечить защиту нейронной сети от возможных злоумышленных вмешательств в ее обучение и исполнение.