РОССИЙСКАЯ ФЕДЕРАЦИЯ

ФЕДЕРАЛЬНАЯ СЛУЖБА
ПО ИНТЕЛЛЕКТУАЛЬНОЙ СОБСТВЕННОСТИ

RU2022685576

ГОСУДАРСТВЕННАЯ РЕГИСТРАЦИЯ ПРОГРАММЫ ДЛЯ ЭВМ

Номер регистрации (свидетельства):
2022685576
Дата регистрации: **26.12.2022**
Номер и дата поступления заявки:
2022684362 12.12.2022
Дата публикации и номер бюллетеня:
26.12.2022 Бюл. № 1
Контактные реквизиты:
+7-903-700-79-86, m.kalugin@ispras.ru

Автор(ы):
Булгакова Мария Ивановна (RU),
Гетьман Александр Игоревич (RU),
Горюнов Максим Николаевич (RU),
Мацкевич Андрей Георгиевич (RU),
Перминов Андрей Игоревич (RU),
Рыболовлев Дмитрий Александрович (RU)
Правообладатель(и):
Федеральное государственное бюджетное учреждение науки Институт системного программирования им. В.П. Иванникова Российской академии наук (RU)

Название программы для ЭВМ:
«Программа защиты от атаки уклонения в системе обнаружения вторжений»

Реферат:
Программа предназначена для защиты от атак уклонения в отношении модели машинного обучения в системе обнаружения компьютерных атак. Состязательные примеры генерируются перебором значений одного из признаков классификации для каждой сессии тестовой выборки с меткой "атака". При изменении ответа модели, пример считается состязательным. Для защиты в обучающую выборку добавляются найденные примеры с корректной разметкой. После обучения на них модель верно классифицирует состязательные примеры, то есть обеспечивается устойчивость классификатора к состязательным атакам. Программа разработана ИСП РАН в рамках мероприятия «Методы обнаружения и противодействия атакам с внедрением закладок и зловредного кода в модели машинного обучения» Программы центра ИИ «Разработка методов и технологий создания систем доверенного искусственного интеллекта» по направлению доверенный искусственный интеллект. Тип ЭВМ: IBM PC - совмест. ПК. ОС: Linux.

Язык программирования: Python (Jupyter Notebook)

Объем программы для ЭВМ: 46 КБ