РОССИЙСКАЯ ФЕДЕРАЦИЯ

ФЕДЕРАЛЬНАЯ СЛУЖБА
ПО ИНТЕЛЛЕКТУАЛЬНОЙ СОБСТВЕННОСТИ

RU2022682843

ГОСУДАРСТВЕННАЯ РЕГИСТРАЦИЯ ПРОГРАММЫ ДЛЯ ЭВМ

Номер регистрации (свидетельства):
2022682843
Дата регистрации: **28.11.2022**
Номер и дата поступления заявки:
2022681967 18.11.2022
Дата публикации и номер бюллетеня:
28.11.2022 Бюл. № 12

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 реализации атаки уклонения в отношении модели обнаружения вторжений»

Реферат:
Программа предназначена для реализации атаки уклонения в отношении модели машинного обучения, применяемой в системе обнаружения компьютерных атак. Поиск состязательных примеров ведётся при наличии знания о модели и обучающей выборке. Для каждой сетевой сессии тестовой выборки применяется метод перебора значений выбранного признака с проверкой сохранения метки «атака» у модифицированной сессии и изменения ответа модели. В рамках подхода учитывается невозможность прямого произвольного изменения значений отдельных признаков сессий сетевого трафика со стороны атакующего. 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. IBM-совместимые ПК Linux.

Язык программирования: Python (Jupyter Notebook)

Объем программы для ЭВМ: 39 КБ