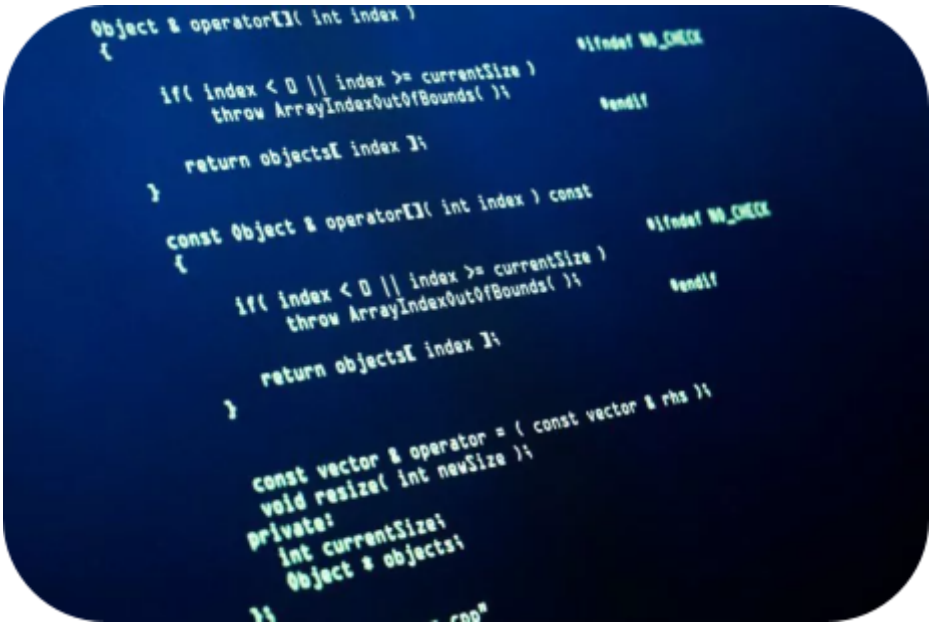
Выявление уязвимостей программного кода с помощью машинного обучения

Уязвимости в программном обеспечении — это далеко не только мелкие неудобства при работе с компьютерами и смартфонами; наличие уязвимостей иной раз может привести как к колоссальному материальному ущербу, так и к трагическим последствиям. А с учетом того, что цифровизация проникает всё глубже во все сферы человеческой жизнедеятельности, в том числе и критические, важность задачи разработки и совершенстования средств выявления уязвимостей в программном коде сложно переоценить.

Традиционно для выявления уязвимостей используются такие инструменты, как статические и динамические анализаторы. Эти инструменты анализируют исходный код программы и способны указать на строку в коде, где есть уязвимость, а также определить, какого рода эта уязвимость, например, неопределенное поведение, переполнение буфера, утечки памяти и пр.



Альтернативным подходом к выявлению уязвимостей является использование методов машинного обучения, в основе которых лежат не формальные наперед заданные правила, а «самостоятельное обучение» системы путем выявления сложных закономерностей на большом количестве примеров. Системы, основанные на методах машинного обучения, способны как составить конкуренцию, так и дополнить традиционные инструменты выявления уязвимостей в коде.

Отдельно среди методов машинного обучения стоит выделить большие языковые модели (англ. Large Language Models, LLMs). Широкому

кругу пользователей большие языковые модели известны прежде всего по вопросно-ответным системам общего профиля, таким как ChatGPT. Но также в последнее время активно разрабатываются и внедряются большие языковые модели для специализированного применения, в частности, разработаны большие языковые модели специально для выявления уязвимостей в коде, и научно-исследовательская работа в этом направлении активно продолжается.

Задачей проекта будет построение системы выявления уязвимостей программного кода на основе методов машинного обучения, в частности, на основе существующих больших языковых моделей. Ожидается, что система будет принимать на вход программный код на языке C и выдавать пользователю рекомендации, связанные с уязвимостями в этом коде, при этом будет требоваться, чтобы частота ошибок в выдаче рекомендаций не превышала определенный порог. Сама система будет разработана на языке Python.

Заинтересованные и проявившие свои способности участники проекта могут быть в дальнейшем приглашены на стажировку или работу в Группу Астра — компанию-производитель российской операционной системы Astra Linux.