А. К. Доронин, В. А. Липницкий
(*УО «БГУИР», Минск*)

ПРИМЕНЕНИЕ МЕТОДОВ МАШИННОГО ОБУЧЕНИЯ С ПОДКРЕПЛЕНИЕМ К ЗАДАЧЕ ОБНАРУЖЕНИЯ УЯЗВИМОСТЕЙ ТИПА SQL-ИНЪЕКЦИЯ

Обучение с подкреплением является подразделом машинного обучения, изучающим, как агент должен действовать в окружении, чтобы максимизировать некоторый долговременный выигрыш. Формально простейшая модель обучения с подкреплением состоит из:

- множества состояний окружения S;
- множества действий агента A;
- множества скалярных «выигрышей».

Агент принимает решение выбрать действие из множества A, получает ответ от среды (выигрыш), затем делает вывод и повторяет процесс игры с учётом вывода.

При помощи обучения с подкреплением были разработаны модели, позволившие машинному интеллекту неоднократно обыграть чемпионов по игре го и играм Atari [1].

Основная забота диспетчера локальной компьютерной сети – противостояние разного рода попыткам несанкционированного вмешательства, которые кратко можно назвать уязвимостями. Одной из наиболее серьёзных уязвимостей веб-приложений на протяжении многих лет остаётся внедрение операторов SQL, или SQL-инъекция. При-

менительно к задачам защиты информации перспективной может оказаться разработка интеллектуального сканера уязвимостей типа SQL-инъекция на основе методов машинного обучения с подкреплением. Множеством действий агента может выступать использование комбинаций различных ключевых слов языка SQL и различных техник отправки веб-запросов, а множеством выигрышей – минимальный набор действий для получения истинного ответа о наличии уязвимости. Имеется проблема сложности обучения сети – необходимо, чтобы среда возвращала «истинный» ответ о наличии той или иной уязвимости, кроме полученного предполагаемого ответа от сканера.

Литература

1 Playing Atari with Deep Reinforcement Learn [Electronic resource] / University of Toronto. – 2017. – Mode of access: https://www.cs. tronto.edu/~vmnih/docs/dqn.pdf. – Date of access: 06.01.2018.