**УДК 004.056**

# АЛГОРИТМ ОЦЕНКИ ЭКСПЛУАТИРУЕМОСТИ ДЕФЕКТОВ БЕЗОПАСНОСТИ ПРОГРАММНОГО ОБЕСПЕЧЕНИЯ С ИСПОЛЬЗОВАНИЕМ СИМВОЛЬНОГО ВЫПОЛНЕНИЯ

**Челпанов А.Д.** (Университет ИТМО)
**Научный руководитель – к.т.н. Югансон А.Н.**
(Университет ИТМО)

Наличие эксплуатируемых дефектов безопасности в программном обеспечении влечет за собой репутационные и финансовые потери. Из-за потенциально большого количества дефектов в программных продуктах необходимо определять приоритет исправления каждого обнаруженного дефекта. В докладе рассмотрен алгоритм оценки эксплуатируемости дефектов программного обеспечения с использованием символьного анализа.

**Введение.** Существующие алгоритмы и системы оценки эксплуатируемости дефектов безопасности можно разделить на две группы: алгоритмы и системы автоматической генерации эксплойтов и интеллектуальные системы, основанные на технологии машинного обучения. К первой группе относятся решения автоматического создания эксплойтов по трассе машинных инструкций, которая создается при аварийном завершении программы. Интеллектуальные модели используют открытые базы уязвимостей, CVSS рейтинги уязвимостей и существующие эксплойты в качестве материала для машинного обучения.
В данной работе представляется алгоритм оценки эксплуатируемости программных дефектов безопасности с использованием символьного выполнения.

**Основная часть.** Под программным дефектом безопасности подразумевается перечень инструкций в программном обеспечении, исполнение которых может привести к нарушению конфиденциальности, целостности и/или доступности программного обеспечения.
Символьное выполнение – это техника анализа программного обеспечения, которая описывает состояние программы в виде логических формул, на основе разрешимости которых определяется текущее состояние программы. Динамическое символьное выполнение, в свою очередь, позволяет в конкретный момент времени соотнести текущее состояние программы и формулы, которым оно описывается. Это позволяет эффективнее определять ограничения, накладываемые на переменные, возникающих при ветвлениях программы.
Алгоритм оценки эксплуатируемости дефектов программного обеспечения с использованием символьного выполнения заключается в следующем. В качестве входной информации используется список дефектов безопасности, найденных с помощью статического анализатора. Каждому дефекту в списке соответствует тип CWE и его краткое описание.
Первоначально осуществляется поиск всех путей до обнаруженного дефекта, который реализуется с помощью статического анализа. Путь представляет из себя связный список адресов от точки входа в программу до дефекта.
Далее проводится динамическое символьное выполнение в соответствии с найденными маршрутами. Перед началом выполнения необходимо указать переменные, которые влияют на эксплуатируемость рассматриваемого дефекта, как символьные. Результатом данного этапа служит получение логических формул, которые относятся к указанным ранее символьным переменным.
Предлагается считать дефект безопасности эксплуатируемым, если полученные логические формулы не ограничивают его эксплуатацию.

**Выводы.** Предложенный алгоритм оценки эксплуатируемости дефектов безопасности программного обеспечения позволяет приоритезировать найденные дефекты безопасности для исправления эксплуатируемых в первую очередь. Дальнейшая работа будет направлена на апробацию и определение эффективности описанного алгоритма.