Автоматизация в промышленности 2023. №12
www.avtprom.ru

DOI: 10.25728/avtprom.2023.12.11

Леонов Н.В. (ФГУП «ГосНИИПП»),
Буйневич М.В. (Санкт-Петербургский университет ГПС МЧС России)

Проблемные вопросы поиска уязвимостей в программном обеспечении промышленных ИТ-устройств

Рассмотрена проблема небезопасного программного обеспечения, использование которого приводит к реализации угроз информационной и кибербезопасности. В качестве одного из механизмов предотвращения возможных неблагоприятных последствий рассматривается поиск уязвимостей в коде программ промышленных IT-устройств. На основании авторского опыта и проанализированных публикаций выделены пять проблемных вопросов, возникающих из-за недостаточной исследованности предметной области и оказывающих существенное влияние на поиск таких уязвимостей в контексте сложности решения следующих задач: выбор способа поиска, обход защиты от анализа кода, представление уязвимостей, оценка эффективности поиска, учет неклассических эффектов и формализация. Для каждого проблемного вопроса указаны возможности применения искусственного интеллекта.

Ключевые слова: уязвимость, программное обеспечение, информационная и кибербезопасность, проблемные вопросы, промышленные устройства.

Леонов Николай Викторович *– канд. техн. наук, доцент, начальник лаборатории Государственного научно-исследовательского института прикладных проблем,*
Буйневич Михаил Викторович *– д-р техн. наук, проф., проф. кафедры прикладной математики и информационных технологий Санкт-Петербургского университета государственной противопожарной службы МЧС России.*

Список литературы

1. *1.* Несов В.С., Маликов О.Р. Автоматический поиск уязвимостей в больших программах // Информационное противодействие угрозам терроризма. 2006. № 7. С. 281-291.
2. Полухин П.В. Фаззинг – современная технология поиска уязвимостей в Веб-приложениях // Наука и современность. 2012. № 16-1. С. 313-318.
3. Щедрин Д.А. Применение методов машинного обучения и анализа статического кода интеллектуальных систем // Научно-исследовательский центр «Technical Innovations». 2023. № 16. С. 28-32.
4. Варновский Н.П., Захаров В.А., Кузюрин Н.Н., Шокуров А.В. Современное состояние исследований в области обфускации программ: определения стойкости обфускации // Труды ИСП РАН. 2014. Т. 26. № 3. С. 167-198.
5. Шариков П.И. Методика обфускации байт-кода Java-приложения с целью его защиты от атак декомпиляцией // Вестник СПбГУПТД. Сер. 1: Естественные и технические науки. 2022. № 1. С. 64-72.
6. Маркин Д.О., Макеев С.М. Система защиты терминальных программ от анализа на основе виртуализации исполняемого кода // Вопросы кибербезопасности. 2020. № 1 (35). С. 29-41.
7. Марков А.С., Фадин А.А. Статический сигнатурный анализ безопасности программ // Программная инженерия и информационная безопасность. 2013. № 1. С. 50-56.
8. Федорченко А.В., Чечулин А.А., Котенко И.В. Аналитический обзор открытых баз уязвимостей программно-аппаратного обеспечения // Проблемы информационной безопасности. Компьютерные системы. 2014. № 3. С. 131-135.
9. Артамонов В.С., Винниченко А.В. Формирование базы данных параметров уязвимостей информационно-телекоммуникационной системы // Радиолокация, навигация, связь: Тр XXVI международной научно-технической конференции. 2020. Т. 6. Воронеж. С. 372-382.

10. Соболевская Е.Ю., Шевченко И.Д., Алексеев С.Е. Алгоритм формирования базы уязвимостей и выбор архитектуры нейронной сети для их обработки // Моделирование, оптимизация и информационные технологии. 2022. Т. 10. № 3 (38). С. 26-27.
11. Левкин И.М. Комплексная оценка эффективности робототехнических систем добывания и обработки информации // Известия высших учебных заведений. Приборостроение. 2017. Т. 60. № 2. С. 110-116.
12. Репкин А.С. Модуль приоритезации ветвей условий для повышения эффективности автоматизированного поиска уязвимостей // Сборник избранных статей научной сессии ТУСУР. 2020. № 1-2. С. 110-113.
13. Буйневич М.В., Израилов К.Е. Антропоморфический подход к описанию взаимодействия уязвимостей в программном коде. Ч. 1. Типы взаимодействий/ Ч. 2. Метрика уязвимостей // Защита информации. Инсайд. 2019. № 5 (89)/ № 6 (90). С. 78-85/С. 61-65.
14. Максимова Е.А., Садовникова Н.П. Межсубъектное взаимодействие как источник деструктивных воздействий на субъекте критической информационной инфраструктуры // Прикаспийский журнал: управление и высокие технологии. 2021. № 2 (54). С. 71-80.
15. Максимова Е.А. Аксиоматика инфраструктурного деструктивизма субъекта критической информационной инфраструктуры // Информатизация и связь. 2022. № 1. С. 68-74.
16. Исахин Г.В. Формализация уязвимостей на языке OVAL // Вестник современных исследований. 2020. № 5-3 (35). С. 4-6.

Leonov N.V., Buinevich M.V. The challenges of vulnerabilities scanning in the software of industrial IT devices

The paper discusses the problem of insecure software, whose use results in the implementation of information and cybersecurity threats. The search for vulnerabilities in the software code of industrial IT devices is considered as a possible mechanism for preventing possible destructive consequences. Based on authors' experience and the analyzed publications, five challenges are identified, which are posed by the insufficient research of the subject area and have a significant impact on the search for such vulnerabilities in the context of the complexity of solving the following tasks: selection of the search method, bypassing protection from code analysis, vulnerability representation, evaluation of search efficiency, consideration of non-classical effects, and formalization. For each challenge, the possibilities of applying artificial intelligence are indicated.

Keywords: vulnerability, software, information and cybersecurity, problematic topics, industrial devices