Автоматизация в промышленности 2021. №11
www.avtprom.ru

DOI: 10.25728/avtprom.2021.11.09

М.В. Буйневич (СПб УГПС МЧС), К.Е. Израилов (СПбГУТ),
В.В. Матвеев (СПбГЭУ), В.В. Покусов (КАИБ)

Способ вариативной классификации уязвимостей в программном коде. Часть 1. Стратификация и категориальное деление

Решается задача вариативной классификации уязвимостей программного кода. В результате обзора релевантных научных работ были установлены границы предметных областей, а также плюсы и минусы известных подходов. Предложен способ классификации, основанный на пяти предпосылках: автоматизация, экспертное мнение, машинное обучение, необходимость и достаточность деления, работа с человеко-ориентированными данными. Указаны шаги по реализации способа, которые позволяют создавать подходящие классы и относить к ним найденные и гипотетические уязвимости.

В первой части статьи на примере программного обеспечения телекоммуникационных устройств описаны первые четыре шага способа, а именно: экспертная стратификация уязвимостей, категориальное деление множества уязвимостей на группы, составление набора классов и предварительное отнесение к ним уязвимостей.

Ключевые слова: программное обеспечение телекоммуникационных устройств, уязвимости программного кода, адаптивная классификация, категориальный анализ, машинное обучение.

Буйневич Михаил Викторович *– д-р техн. наук, проф., профессор кафедры прикладной математики и информационных технологий Санкт-Петербургского университета государственной противопожарной службы МЧС России,*

Израилов Константин Евгеньевич *– канд. техн. наук, доцент кафедры защищенных систем связи Санкт-Петербургского государственного университета телекоммуникаций им. проф. М.А. Бонч-Бруевича, старший научный сотрудник лаборатории проблем компьютерной безопасности Санкт-Петербургского Федерального исследовательского центра РАН,*

Матвеев Владимир Владимирович *- д-р техн. наук, проф., профессор кафедры экономической безопасности Санкт-Петербургского государственного экономического университета,*

Покусов Виктор Владимирович *- председатель Казахстанской ассоциации информационной безопасности, Алматы, Казахстан.*

Список литературы

1. *Розова С.С.* Классификационная проблема в современной науке. Новосибирск: Наука, 1986. 224 с.
2. *Виткова Л.А., Израилов К.Е., Чечулин А.А.* Классификация уязвимостей интерфейсов транспортной инфраструктуры умного города // Актуальные проблемы инфотелекоммуникаций в науке и образовании (АПИНО-2020). Тр. IX междунар. научно-технич. и методич. конф. С.-Петербург. 2020. С. 253-258.
3. *Понкин И.В., Редькина А.И.* Классификация как метод научного исследования, в частности в юридической науке // Вестник Пермского университета. Юридические науки. 2017. Вып. 37. С. 249-259.
4. *Джангазова К.А., Утамуратов О.А.* Классификация уязвимостей безопасности // Высшая школа. 2016. № 10. С. 123-124.
5. *Надеждин Е.Н., Шершакова Т.Л.* Задача классификации уязвимостей программного обеспечения в корпоративной информационной сети // Шуйская сессия студентов, аспирантов, педагогов, молодых ученых. Тр. X междунар. научной конф. 2017. С. 207.
6. *Надеждин Е.Н., Шершакова Т.Л.* Алгоритм нечеткой классификации уязвимостей прикладного программного обеспечения // Проблемы фундаментальной и прикладной информатики в управлении, автоматизации и мехатронике. Тр. междунар. научно-технич. конф. Курск. 2017. С. 109-113.
7. *Матяш Е.Д.* Классификация и разметка элементов текста на уровне предложения для выявления уязвимостей нулевого дня // Комплексная защита информации. Тр. XXII научно-практич. конф. Полоцк. 2017. С. 253-256

8. *Доронин А.К., Липницкий В.А.* Построение модели машинного обучения для задачи классификации степени критичности CVE-уязвимостей // Веснік Магілеўскага дзяржаўнага ўніверсітэта імя А.А. Куляшова. Серыя В. Прыродазнаўчыя навукі: матэматыка, фізіка, біялогія. 2020. № 1 (55). С. 51-63.
9. *Алексеев И.В., Зегжда П.Д.* Классификация уязвимостей сетевых протоколов на основе спецификаций // Проблемы информационной безопасности. Компьютерные системы. 2020. № 1. С. 24-32.
10. *Зиновьев А.В., Язиков Г.Е., Аборнев А.А.* Практическое применение метода машинного обучения «мешок слов» в модуле «1С (чат-бот)» для автоматизации работы сотрудников первой линии поддержки пользователей // Газовая промышленность. 2021. № 5 (816). С. 28-31.
11. *Израилов К.Е.* Обобщенная классификация уязвимостей интерфейсов транспортной инфраструктуры умного города // Информационные технологии. 2021. Т. 27. № 6. С. 330-336.
12. *Муханова А., Ревнивых А.В., Федотов А.М.* Классификация угроз и уязвимостей информационной безопасности в корпоративных системах // Вестник НГУ. Серия: Информационные технологии. 2013. Т. 11. № 2. С. 55-72.
13. *Сучков А.П.* Классификация уязвимостей интегрированных систем управления на ранних стадиях жизненного цикла // Системы и средства информатики. 2017. Т. 27. № 4. С. 132-143.
14. *Сидоров А.Г.* Способы классификации и системы оценки уязвимостей в аналитических системах сбора и анализа сведений об уязвимостях и угрозах ИБ // Фундаментальные и прикладные исследования молодых ученых: Тр. II междунар. научно-практич. конф. студентов, аспирантов и молодых ученых. Омск. 2018. С. 503-509.
15. Кубарев А.В. Подход к формализации уязвимостей информационных систем на основе их классификационных признаков // Вопросы кибербезопасности. 2013. № 2 (2). С. 29-33.
16. *Израилов К.Е.* Визуализация многопризнаковых уязвимостей программного кода с помощью метода главных компонент // Вестник СПбГУПТД. Серия 1: Естественные и технические науки. 2020. № 1. С. 3-8.
17. *Huang G., Li Y., Wang Q., Ren J., Cheng Y., Zhao X.* Automatic Classification Method for Software Vulnerability Based on Deep Neural Network // The Proceedings of IEEE Access. 2019. Vol. 7. PP. 28291-28298.
18. *Aota M., Kanehara H., Kubo M., Murata N., Sun B., Takahashi T.* Automation of Vulnerability Classification from its Description using Machine Learning // The Proceedings of Symposium on Computers and Communications (ISCC). IEEE, 2020. PP. 1-7.
19. *Shuai B., Li H., Li M., Zhang Q., Tang C.* Automatic classification for vulnerability based on machine learning // The Proceedings of International Conference on Information and Automation (ICIA). IEEE, 2013. PP. 312-318.
20. *Last D.* Using historical software vulnerability data to forecast future vulnerabilities // Resilience Week (RWS). 2015. PP. 1-7.
21. *Gonzalez D., H. Hastings and M. Mirakhorli.* Automated Characterization of Software Vulnerabilities // 2019 IEEE International Conference on Software Maintenance and Evolution (ICSME). 2019. PP. 135-139.
22. *Буйневич М.В., Израилов К.Е.* Категориальный синтез и технологический анализ вариантов безопасного импортозамещения программного обеспечения телекоммуникационных устройств // Информационные технологии и телекоммуникации. 2016. Т. 4. № 3. С. 95-106.
23. *Буйневич М.В., Щербаков О.В., Израилов К.Е.* Структурная модель машинного кода, специализированная для поиска уязвимостей в программном обеспечении автоматизированных систем управления // Проблемы управления рисками в техносфере. 2014. № 3 (31). С. 68-74.
24. *Richards T., Walters E.K., Moss J.E.B., Palmer T., Weems C.C.* Towards universal code generator generation» // The Proceedings of IEEE International Symposium on Parallel and Distributed Processing. 2008. PP. 2560-2567.
25. 25.Волков Д.С., Иванов А.В. Применение генетических алгоритмов для выбора ключа шифрования в системах связи ракетных комплексов // Актуальные проблемы авиации и космонавтики. 2016. Т. 1. № 12. С. 145-147

Buynevich M.V., Izrailov K.E., Matveev V.V., Pokusov V.V. A method for variative classification of vulnerabilities in program code. Part 1. Stratification and categorization.

The problem of variative classification of vulnerabilities in program code is solved. Based on an overview of related scholarly articles, the boundaries of subject areas were determined as well as the merits and drawbacks of known approaches. This implied a new classification technique based on five prerequisites: automation, expert judgements, machine leaning, necessity and sufficiency of division, and human-oriented data processing. Actions to implement the technique are proposed, which allow to develop suitable classes and sort the vulnerabilities both detected and possible. In the first part of the article, with an example of telecommunication device software, the first four steps are described, namely: expert stratification of vulnerabilities, categorization of the set of vulnerabilities, classification and preliminary sorting of vulnerabilities.

Keywords: telecommunication device software, vulnerabilities in program code, adaptive classification, categorical analysis, machine learning.