Таким образом, мы определили, что унифицированного метода, подходящего для оценки риска большинства средств измерений с программным обеспечением, не существует. В то же время нельзя не отметить наиболее перспективный подход, описанный в международном стандарте ГОСТ Р ИСО/МЭК 27000. Согласно общим критериям составляется перечень активов, подлежащих защите, и соответствующие профили защиты. Оценка уровня риска проводится по ГОСТ Р ИСО/МЭК 27005–2010, то есть анализируются все аспекты оценки рисков программного обеспечения в разных направлениях. Благодаря совмещению подходов указанных стандартов можно получить единый наиболее эффективный метод. ■

Статья поступила в редакцию 25.02.2023

Overview of Software Risk Assessment Methods

I.V. Lazareva[1], FSBI All-Russian Research Institute of Metrological Service (FSBI VNIIMS), i.lazareva@vniims.ru
A.N. Pan'kov[2, 3, 4], FSBI VNIIMS, FSAEI FVT Academy for Standardization, Metrology and Certification (Training), FSBEI HE MIREA — Russian Technological University, PhD (Tech.), apankov@vniims.ru

[1] Laboratory Assistant of Department, Moscow, Russia
[2] Head of Laboratory, Moscow, Russia
[3] Deputy Head of Department, Moscow, Russia
[4] Associate Professor of Department, Moscow, Russia

Citation: Lazareva I.V., Pan'kov A.N. Overview of Software Risk Assessment Methods, *Kompetentnost' / Competency (Russia)*, 2023, no. 7, pp. 13–17.
DOI: 10.24412/1993-8780-2023-7-13-17

key words

metrology, measuring instruments, risk assessment, software protection, information technology

Today, one of the main tasks of metrological service workers is to assess and minimize risks when using software in measuring instruments. A risk-based approach can help to solve it. The authors reviewed various risk assessment methods and came to the conclusion that some of the considered software risk assessment methods are narrowly focused and applicable only in their areas, or require additional information, for example, in the form of source code as for the van Dersen method.
So, the most promising is the approach described in the international standard GOST R ISO/IEC 27000. According to the general criteria, a list of assets to be protected and their corresponding protection profiles are compiled. Risk level assessment is carried out in accordance with GOST R ISO/IEC 27005–2010, that is, by analyzing all aspects of software risk assessment in different directions. By combining the approaches of these standards, you can get a single most effective method.

References

1. GOST R 8.839–2013 SSM. General requirements for software controlled measuring instruments, Moscow, 2014, 42 P.
2. GOST R ISO/IEC 27000–2012 Information technology (IT). Methods and means of ensuring security. Information security management systems. General overview and terminology, Moscow, 2014, 22 P.
3. GOST R ISO/IEC 27005–2010 Information technology (IT). Methods and means of ensuring security. Information security risk management, Moscow, 2011, 51 P.
4. WELMEC 5.3. Issue 1. Risk assessment guide for market surveillance: weigh and measuring instruments, 2011.
5. Directive 2014/32/EU of the European Parliament and of the Council of 26 February 2014 On measuring instruments, *Official Journal of the European Union L 96*, 2014.
6. OIML D 31 Edition 2008 (E) General requirements for software controlled measuring instruments.
7. R 50.2.077–2014 SSM. Tests of measuring instruments for the purpose of type approval. Software security check, Moscow, 2014, 24 P.
8. GOST R 8.654–2015 SSM. Software requirements for measuring instruments, Moscow, 2015, 12 P.