Methodology of Software Risk Assessment

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

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.
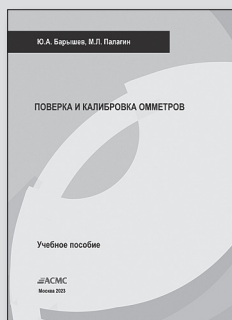
So, the most promising is the approach described in the international standard GOST R ISO/IEC 27000. According to the general criteria, a list of assets to be protected and their corresponding protection profiles are compiled. Risk level assessment is carried out in accordance with GOST R ISO/IEC 27005–2010, 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. RF Federal Law of 26.06.2008 N 102-FZ On ensuring uniformity of measurements.
2. R 50.2.077–2014 SSM. Tests of measuring instruments for the purpose of type approval. Software security check, Moscow, 2014, 24 P.
3. GOST R 8.654–2015 SSM. Software requirements for measuring instruments, Moscow, 2015, 12 P.
4. RF Ministry of Industry and Trade Order of 28.08.2020 N 2905 On approval of the procedure for testing standard samples or measuring instruments for the purpose of type approval, the procedure for approving the type of standard samples or type of measuring instruments, making changes to information about them, the procedure for issuing certificates of approval of the type of standard samples or type of measuring instruments, the form of certificates of approval of the type of standard samples or type.
5. Lazareva I.V., Pan'kov A.N. Overview of software risk assessment methods, *Kompetentnost' / Competency (Russia)*, 2023, no. 7, pp. 13–17.