UDC 006.034 *DOI: 10.32362/2500-316X-2019-7-1-48-56*

ANTIVIRUS SOFTWARE AND INDUSTRIAL CYBER SECURITY SYSTEM CERTIFICATION IN RUSSIA

M.A. Nazarenko[@],
A.I. Gorobets,
D.V. Miskov,
V.V. Muravyev,
A.S. Novikov

MIREA – Russian Technological University, Moscow 119454, Russia
[@] Corresponding author e-mail: Nazarenko@mirea.ru

The article is dedicated to issues in certification of antivirus software and industrial cyber security systems. It was shown that certification time in Russia is much longer than in the USA, European Union and Germany. The life time and the development time of products of this field were analyzed in the article. Each variable was specified for new products and for new versions of existing products. Some statistical methods were used in the article: Cronbach's alfa, t-statistics, and median value similarity that are typical for the articles in quality management. As a result, it was found that certification time in Russia for industrial cyber security systems is significantly longer than in other analyzed countries, up to three-fold. Product development and life time are also longer. However, the most important result is that certification in Russia adds from 32.1 to 40 percent of time to the development of a new version or a new product, correspondingly, whereas in other investigated countries these numbers are about 17 percent. Reduction of certification time will increase new product development efficiency in the field of cyber security, which will improve positions of Russian products at the international market.

Keywords: cyber security, industrial cyber security system, antivirus software, certification, Russia.

СЕРТИФИКАЦИЯ АНТИВИРУСНОГО ПРОГРАММНОГО ОБЕСПЕЧЕНИЯ И СИСТЕМ КИБЕРБЕЗОПАСНОСТИ АСУ ТП В РОССИИ

М.А. Назаренко[@],
А.И. Горобец,
Д.В. Миськов,
В.В. Муравьев,
А.С. Новиков

МИРЭА – Российский технологический университет, Москва 119454, Россия
[@]Автор для переписки, e-mail: Nazarenko@mirea.ru

Статья посвящена вопросам сертификации антивирусного программного обеспечения и систем промышленной кибербезопасности. Показано, что время сертификации в России промышленной системы кибербезопасности (кибербезопасности АСУ ТП) значительно больше (до трех раз), чем в США, Европейском Союзе и Германии. В статье проанализированы продукты этих отраслей по времени жизни и времени разработки. Время разработки и использования продуктов также больше. Каждая переменная представлена для новых продуктов и для новых версий существующих продуктов. В статье использованы статистические методы: Альфа Кронбаха, Т-статистика и сравнение медианных значений. Перечисленные методы нередко используются в статьях по управлению качеством. Однако самый важный результат состоит в том, что в России сертификация добавляет от 32.1 до 40% ко времени на разработку новой версии или нового продукта, соответственно, в то время как в других странах – около 17%. Сокращение сроков сертификации приведет к повышению эффективности разработки новых продуктов в области кибербезопасности, что позволит улучшить позиции российской продукции на международном рынке.

Ключевые слова: кибербезопасность, промышленная система кибербезопасности, антивирусное программное обеспечение, сертификация, Россия.

Introduction

One of the most important issues in the modern world is cybersecurity. Vast majority of population in developed countries are using different devices for work and in their everyday life. As a result, there are about 3 devices per person in the age of 12–65 years old in developed countries including Russia [1]. Each of these devices can be probably attacked. As a result, they have been secured by relevant cyber secure systems and software. In this study, antivirus software means software products for personal computers, laptops and mobile phones, including smartphones, and industrial cyber security system means cyber security software and products for industrial objects, including SCADA, DCS and PLC. Undoubtedly, both of these software products are included into one class, whereas, according to the Russian legislation, there are substantially different procedures of registration and certification for these software products.

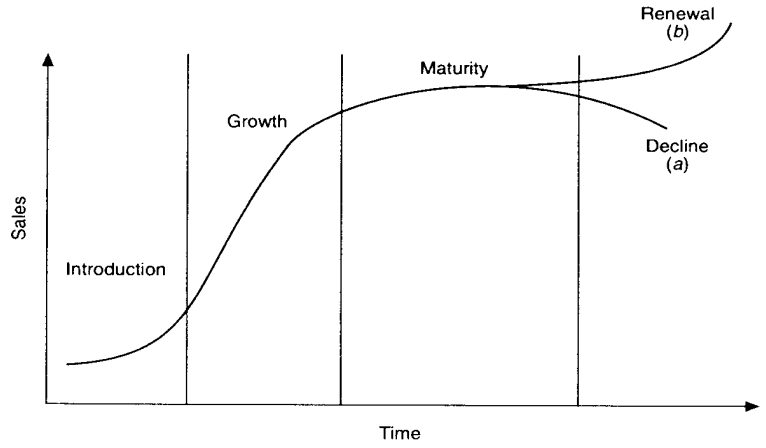
In the article, procedures of registration and certification of antivirus software and industrial cyber security systems in Russia will be analyzed. At present, a vast majority of the research in this field is dedicated to TQM accordance, including usability characteristics [2–6], specifics of this products' technical quality [7, 8], laws in this field and their meaningfulness [9–11]. Moreover, some studies in similar or close fields are dedicated to certification processes and such issues of standardization as reclamation activities [12]. In this article, studies dedicated to technical innovations, procedures and other development issues of antivirus software and industrial cyber security systems will be not covered due to the fact that they are far from standardization topicality.

In modern standardization theory, branch standards and certificates are instruments of government regulation. Usually, government certification and accreditation of IT products aims to archive several goals [13]:

- market regulation;
- consumers defense;

- risk minimization;
- social losses minimization;
- providing of key industries stable functioning.

Government certification is applied in key fields of public and scientific development. Cyber security is definitely one of them. Usually, certification and standardization are based on technical characteristics, applied methods, types of tasks and potential customers groups. Moreover, certification time is interdependent with the development cycle and life period of the product. In IT field it is usually dependent on several issues [13]. The first of them is information product update and new version presenting. Ordinary product life cycle includes introduction, growth, maturity and decline. However, an IT product with new versions and updates has the possibility of renewal (Fig.). Thus, certification should be significantly shorter in time than product life time. They should be more or less equal to the product introduction time. The second issue is time for new version development. Certification time should be significantly less than time required for developing a new version of the product [18].



IT product life cycle.

Antivirus software and industrial cyber security systems are similar in kind. Therefore, it is reasonable to assume that their certification and standardization should be similar too. However, certification of antivirus software and industrial cyber security systems have significant differences in Russia.

The aim of the article is to analyze the consistency of certification procedures for antivirus software and industrial cyber security systems with life time and development cycle of these products. It is assumed that current certification time in Russia is not efficient ant leads to market failures. Therefore, optimization and reduction of certification time can increase the efficiency of antivirus software and industrial cyber security systems.

Methods

The article compares development time for antivirus software and industrial cyber security systems, including the development of new versions of the products, with time for their certification. For valuable comparison, data from certification organizations of several countries are provided. The data cover time for discussible products certification. Moreover, information about product life time and development time is presented. The data are analyzed with the help

of several statistical methods typical for this research field [14]:

- Cronbach's alfa – for data internal reliability analysis;
- t-statistics – for data stability estimation;
- median value similarity.

Data about certification time are based on open information of national certification agencies, including Federal Service for Technical and Export Control (Russia), National Institute of Standards and Technology (USA), Cyber and Information Security (EU), Federal Office for Information Security (Germany).

Results

First of all, it is important to underline that antivirus software and industrial cyber security system certification are regulated differently in Russia. Antivirus software has no government certification. However, the industrial cyber security system has extremely strong standards. Whereas, in other countries, especially, in the USA, the difference between these two IT products is significantly less. In foreign countries the basic of regulation in this field is licensing and patterns. In Russia the key difference is the object of the defense. In foreign countries responsibility for the choice of industrial cyber security system is on the customer [9]. However, the government can restrict or even forbid the usage of some foreign products [10]. In Russia, the question is presented in an opposite way. Each cyber security system for an industrial object should be firstly certificated (not to be confused with licensed) by a government organization, and only then it can be purchased at the market [9]. Therefore, for providing comparable data, this study analyzes industrial cyber security system certification.

In table 1 key figures about efficiency and certification time for 4 cyber security agencies are presented: Federal Service for Technical and Export Control, National Institute of Standards and Technology, Cyber and Information Security, Federal Office for Information Security. For each agency data about average and median certification time in months, Cronbach's alfa and t-statistics are presented.

Table 1. Efficiency and certification time

Agency	*New version*				*New product*			
	Average	Cronbach's alfa	t-Statistics	Median	Average	Cronbach's alfa	t-Statistics	Median
Federal Service for Technical and Export Control	–	–	–	–	11	–	–	11
National Institute of Standards and Technology	1.8	0.89	3.87	1.9	4	0.91	3.2	4.1
Cyber and Information Security	2.1	0.74	4.94	2.0	3.5	0.84	2.81	3.4
Federal Office for Information Security	2.0	0.92	3.52	2.2	3.7	0.9	3.15	3.4

As shown in table 1, in the USA, European Union and Germany as a separated country certification and licensing procedures take rather similar time. In contrast, in Russia there are no cases of new product version certification and just one for new product. Therefore,

no statistical calculations are available for Federal Service for Technical and Export Control. For National Institute of Standards and Technology median values are usually a little bit higher than average. It means that distribution is shifted to the right. In other words, there are cases with significantly less than average certification time, whereas vast majority of the companies are forced to face a bit longer certification time. For Cyber and information security and Federal Office for Information Security the opposite statement is true. Moreover, it is important to add that in Cyber and Information Security certification time is slightly less than in Federal Office for Information Security, whereas is National Institute of Standards and Technology certification time for new products is more for new products and less for new versions.

According to the research question, data about product life cycle and product development time should be presented (Tables 2 and 3). The presented data are based on previous studies [12, 15].

Table 2. Product life time (consumption)

Country	*New version*				*New product*			
	Average	Cronbach's alfa	t-Statistics	Median	Average	Cronbach's alfa	t-Statistics	Median
Russia	18.5	0.71	4.32	19.0	25.1	0.68	5.48	27.8
USA	14.5	0.85	2.98	13.9	17.2	0.84	4.89	17.0
EU	15.2	0.87	5.14	14.3	18.1	0.79	4.31	18.4
Germany	14.7	0.79	3.71	14.1	17.4	0.82	5.15	17.6

Thus, according to the data in tables 2 and 3, product life cycle is significantly longer in Russia than in the USA and the European countries. It is true both for new products and new versions of existing products. For new versions the difference in life time period is about 4.9 months, and for new products even more: 10.1 months. New products here are understood to be products that have no other versions. Simultaneously, there are quite similar values for the USA, European Union and Germany. Thus, it can be concluded that Russia is far from this group of the countries in product life time.

Table 3. Product development time

Country	*New version*				*New product*			
	Average	Cronbach's alfa	t-Statistics	Median	Average	Cronbach's alfa	t-Statistics	Median
Russia	17.2	0.67	3.98	16.9	28.1	0.78	3.33	27.9
USA	11.2	0.71	4.65	11.4	24.4	0.89	5.15	23.8
EU	11.9	0.79	4.71	11.7	26.3	0.92	4.27	25.7
Germany	13.2	0.77	4.23	12.8	25.9	0.9	5.48	25.4

Characterizing product development time, it should be highlighted that time for new product development for Russia and other countries mentioned in the research is more or less equal. In Russia it is longer than in the USA by 4.1 months (14.7%), European Union by 2.2 (7.9%) and Germany by 2.5 (9%), whereas, for new version development the difference is significantly more. For comparison, it is 5.5 months (32.5%) longer than in the USA, 5.2 months (30.8%) longer than in European Union and 4.1 months (24.3%) longer than in Germany.

For tables 1–3 all analyzed variables were stable enough according to the t-statistics and reliable enough according to the Cronbach's alfa analysis. However, reliability for foreign countries is higher than for Russia due to the fact of a bigger sample.

According to tables 1–3 data about median values can be put into one massive to compare average certification time, life time and development time for new products and new product versions. Comparison data are presented in table 4.

Table 4. Certification time, product life and development time

Country	*New version*			*New product*		
	Russia	Product life	Development life	Certification	Product life	Development life
Russia	–	19.0	16.9	11	27.8	27.9
USA	1.9	13.9	11.4	4.1	17.0	23.8
EU	2.0	14.3	11.7	3.4	18.4	25.7
Germany	2.2	14.1	12.8	3.4	17.6	25.4

The data presented in table 4 show that certification time in Russia is about 40% of product life and development time for new products. In contrast, in the USA it is about 24% and 17.2% correspondingly, in European Union – 18.5% and 13.2%, in Germany – 19.3% and 13.3%. Thus, it can be concluded that in Russia the measured variables are significantly higher than in other investigated countries.

For Russia there are no data about certification time for new product versions. However, average coefficient of difference between certification time for a new product and a new product version is 1.8. This variable can be reasonably extended for the certification process in Russia. So, certification time in Russia should be about 6.1 months. This time is 32.1% of new product version life time and 36.1% of new product version development time. For the other investigated countries the following results were calculated: for the USA 13.7% and 16.7%, respectively, for European Union 14% and 17.1%, for Germany 15.6% and 17.2%. Thus, it should be concluded that in Russia average certification time for any process of product creation in the field of industrial cyber security systems is significantly longer in absolute and relative figures than in the USA and Europe.

Discussion

In the research data on product certification time, life and development time for industrial cyber security systems were analyzed. As a result, percentage of certification time in the key process of the IT products in cyber security was found. Previous studies do not cover such kind of statistics. Instead of this they analyze procedures [4–6] and TQM in the field of cyber security [12, 15], specifics of products' technical quality [7, 8], laws in this field and their meaningfulness [9–11].

The key result of the study is that the certification process in absolute and relative measure in Russia is significantly longer than in other investigated countries. This leads to additional slowdown of the new products development in cyber security field. At present, processes of software development in this field are longer than in the USA by 6 months or 1.5 times, and certification procedures take almost 3 times more. Moreover, certification time in the USA is just about 17% of development time both for a new product version and a new product development, whereas in Russia it is 32.1 and 40%, correspondingly.

Conclusion

Both antivirus software and industrial cyber security systems are important for Russia development and security as a country. Moreover, these products can be sold (and are even being sold at present) abroad. At present certification in this field is significantly longer than in other developed countries, which leads to a slowdown in the development of new products and their versions and creates situations where companies are not interested in proper certification of each version. In other words, the certification procedure as a whole for industrial cyber security systems is inefficient. For antivirus software there is no procedure at all, i.e., it is not efficient either. As a result of the article, it can be concluded that reduction of certification time for industrial cyber security system will increase the certification procedure efficiency in product development in this field in Russia.

Moreover, it is important to add that antivirus software and industrial cyber security system are international products. Many countries purchase products that have been created abroad. Therefore, simplification, especially certification process time reduction will lead to extension of Russian cyber security information products abroad.

References:

1. Kabali H.K., Rigoyen M.M., Nunez-Davis R., Budacki J.G., Mohanty S.H., Leister K.P., Bonner R.L. Jr. Exposure and use of mobile media devices by young children. *Pediatrics.* 2015; 136(6): 1044-1050. doi: 10.1542/peds.2015-2151.

2. Schoitsch E., Schmittner C., Ma Z., Gruber Th. The need for safety and cyber-security co-engineering and standardization for highly automated automotive vehicles. In: Advanced Microsystems for Automotive Applications. Schulze T., Müller B., Meyer G. (eds). Springer, 2015: 251-261.

3. Ni J.Z., Melnyk S., Flynn B.B., Ritchie W. Why be first if it doesn't pay? The case of early adopters of C-TPAT supply chain security certification. *Int. J. Operat. & Product. Management.* 2016; 36(10): 1161-1181.

4. Gcaza N., Von Solms R. A strategy for a cybersecurity culture: A South African perspective. *The Electronic Journal of Information Systems in Developing Countries.* 2017; 80(1): 1-17.

5. Mourtzis D., Vlachou E. Cloud-based cyber-physical systems and quality of services. *The TQM Journal.* 2016; 28(5): 704-733.

6. Raisinghani M.S. Can total quality management exist in cyber security: Is it present? Are we safe? In: Handbook of Research on Digital Crime, Cyberspace Security, and Information Assurance. IGI Global, 2015: 350-359.

7. Cherdantseva Y., Burnap P., Blyth A., Eden P., Jones K., Soulsby H., Stoddart K. A review of cyber security risk assessment methods for SCADA systems. *Computers & Security.* 2016; 56: 1-27.

8. Kent A.D. Cyber security data sources for dynamic network research. In: Dynamic Networks and Cyber-Security. Publisher WSPC, 2016: 37-65.

9. Efremova M.A. Criminal-legal ensuring of cyber security: Problems and ways of their solution. *Pravo i kiberbesopasnost'* (Law and Cyber Security). 2014; 2: 33-38. (in Russ.)

10. Ziborov O.V., Ivanov M.A., Chekunov I.G. The state of cyber security in modern

information society. *Voprosi kiberbesopasnosti* (Questions of Cyber Security). 2017; 52(20): 15-18. (in Russ.)

11. Kartskhiya A.A. Cyber security and intellectual property. Part 1. *Voprosi kiberbesopasnosti* (Questions of Cyber Security). 2014; 1(2): 61-66. (in Russ.)

12. Knowles W., Hutchison D., Prince D., Diss J.P. A survey of cyber security management in industrial control systems. *Int. J. Critical Infrastructure Protection.* 2015; 9: 52-80.

13. Gopalakrishnan S., Zhang H. The link between vendor certification and performance in IT outsourcing: A tale of two stories. *Academy of Management Proceed.* 2018; 1: 129-167.

14. Kantardjieva M. The relationship between total quality management (TQM) and strategic management. *J. Economics, Business and Management.* 2015; 3(5): 537-541.

15. Shin J. , Son H., Rahman K.U., Heo G. Development of a cyber security risk model using Bayesian networks. *Reliability Engineering & System Safety.* 2015; 134: 208-217.

Литература:

1. Kabali H.K., Rigoyen M.M., Nunez-Davis R., Budacki J.G., Mohanty S.H., Leister K.P., Bonner R.L. Jr. Exposure and use of mobile media devices by young children // Pediatrics. 2015. V. 136. № 6. P. 1044–1050. doi: 10.1542/peds.2015-2151

2. Schoitsch E., Schmittner C., Ma Z., Gruber Th. The need for safety and cyber-security co-engineering and standardization for highly automated automotive vehicles // In: Advanced Microsystems for Automotive Applications / Schulze T., Müller B., Meyer G. (eds). Springer, 2015. P. 251–261.

3. Ni J.Z., Melnyk S., Flynn B.B., Ritchie W. Why be first if it doesn't pay? The case of early adopters of C-TPAT supply chain security certification // Int. J. Operat. & Product. Management. 2016. V. 36. №. 10. P. 1161–1181.

4. Gcaza N., Von Solms R. A A strategy for a cybersecurity culture: A South African perspective // The Electronic Journal of Information Systems in Developing Countries. 2017. V. 80. №. 1. P. 1–17.

5. Mourtzis D., Vlachou E. Cloud-based cyber-physical systems and quality of services // The TQM Journal. 2016. V. 28. № 5. P. 704–733.

6. Raisinghani M.S. Can total quality management exist in cyber security: Is it present? Are we safe? // In: Handbook of Research on Digital Crime, Cyberspace Security, and Information Assurance. IGI Global, 2015. P. 350–359.

7. Cherdantseva Y., Burnap P., Blyth A., Eden P., Jones K., Soulsby H., Stoddart K. A review of cyber security risk assessment methods for SCADA systems // Computers & Security. 2016. V. 56. P. 1–27.

8. Kent A.D. Cyber security data sources for dynamic network research // In: Dynamic Networks and Cyber-Security. Publisher WSPC, 2016. P. 37–65.

9. Ефремова М.А. Уголовно-правовое обеспечение кибербезопасности: некоторые проблемы и пути их решения // Право и кибербезопасность. 2014. № 2. С. 33–38.

10. Зиборов О.В., Иванов М.А., Чекунов И.Г. Состояние кибербезопасности современного информационного общества // Вопросы кибербезопасности. 2017. № 52(20). С. 15–18.

11. Карцхия А.А. Кибербезопасность и интеллектуальная собственность. Часть 1 //

Вопросы кибербезопасности. 2014. № 1(2). С. 61–66.

12. Knowles W., Hutchison D., Prince D., Diss J.P. A survey of cyber security management in industrial control systems // Int. J. Critical Infrastructure Protection. 2015. V. 9. P. 52–80.

13. Gopalakrishnan S., Zhang H. The link between vendor certification and performance in IT outsourcing: A tale of two stories // Academy of Management Proceed. 2018. № 1. P. 129–167.

14. Kantardjieva M. The relationship between total quality management (TQM) and strategic management // J. Economics, Business and Management. 2015. V. 3. № 5. P. 537–541.

15. Shin J. , Son H., Rahman K.U., Heo G. Development of a cyber security risk model using Bayesian networks // Reliability Engineering & System Safety. 2015. V. 134. P. 208–217.

About the authors:

Maxim A. Nazarenko, Ph.D. (Physics and Mathematics), Head of the Chair of Quality Management and Certification, Institute of Radio Engineering and Telecommunication Systems, MIREA – Russian Technological University (78, Vernadskogo Pr., Moscow 119454, Russia).

Alexey I. Gorobets, Ph.D. (Engineering), Associate Professor of the Chair of Quality Management and Certification, Institute of Radio Engineering and Telecommunication Systems, MIREA – Russian Technological University (78, Vernadskogo Pr., Moscow 119454, Russia).

Dmitriy V. Miskov, Ph.D. (Engineering), Associate Professor of the Chair of Quality Management and Certification, Institute of Radio Engineering and Telecommunication Systems, MIREA – Russian Technological University (78, Vernadskogo Pr., Moscow 119454, Russia).

Vyacheslav V. Muravyev, Senior Lecturer of the Chair KB-9 "Applied and Business Informatics", Institute of Integrated Security and Special Instrumentation, MIREA – Russian Technological University (20, Stromynka St., Moscow 107076, Russia).

Alexandr S. Novikov, Ph.D. (Engineering), Associate Professor of the Chair of Quality Management and Certification, Institute of Radio Engineering and Telecommunication Systems, MIREA – Russian Technological University (78, Vernadskogo Pr., Moscow 119454, Russia).

Об авторах:

Назаренко Максим Анатольевич, кандидат физико-математических наук, заведующий кафедрой управления качеством и сертификации Института радиотехнических и телекоммуникационных систем ФГБОУ ВО «МИРЭА – Российский технологический университет» (119454, Россия, Москва, пр-т Вернадского, д. 78).

Горобец Алексей Иванович, кандидат технических наук, доцент кафедры управления качеством и сертификации Института радиотехнических и телекоммуникационных систем ФГБОУ ВО «МИРЭА – Российский технологический университет» (119454, Россия, Москва, пр-т Вернадского, д. 78).

Миськов Дмитрий Валентинович, кандидат технических наук, доцент кафедры управления качеством и сертификации Института радиотехнических и телекоммуникационных систем ФГБОУ ВО «МИРЭА – Российский технологический университет» (119454, Россия, Москва, пр-т Вернадского, д. 78).

Муравьев Вячеслав Викторович, старший преподаватель кафедры КБ-9 «Прикладная и бизнес-информатика» Института комплексной безопасности и специального приборостроения ФГБОУ ВО «МИРЭА – Российский технологический университет» (107076, Россия, Москва, ул. Стромынка, д. 20).

Новиков Александр Серафимович, кандидат технических наук, доцент кафедры управления качеством и сертификации Института радиотехнических и телекоммуникационных систем ФГБОУ ВО «МИРЭА – Российский технологический университет» (119454, Россия, Москва, пр-т Вернадского, д. 78).

For citation: Nazarenko M.A., Gorobets A.I., Miskov D.V., Muravyev V.V., Novikov A.S. Antivirus software and industrial cyber security system certification in Russia. *Rossiyskiy tekhnologicheskiy zhurnal* (Russian Technological Journal). 2019; 7(1): 48-56. (in Russ.). DOI: 10.32362/2500-316X-2019-7-1-48-56

Для цитирования: Назаренко М.А., Горобец А.И., Миськов Д.В., Муравьев В.В., Новиков А.С. Сертификация антивирусного программного обеспечения и систем кибербезопасности АСУ ТП в России // Российский технологический журнал. 2018. Т. 7. № 1. С. 48–56. DOI: 10.32362/2500-316X-2019-7-1-48-56