Taylor & Francis
Taylor & Francis Group

Information Security Journal: A Global Perspective

ISSN: 1939-3555 (Print) 1939-3547 (Online) Journal homepage: http://www.tandfonline.com/loi/uiss20

Cyber crime risk awareness in Kyrgyz Republic

Rita Ismailova & Gulshat Muhametjanova

To cite this article: Rita Ismailova & Gulshat Muhametjanova (2016) Cyber crime risk awareness in Kyrgyz Republic, Information Security Journal: A Global Perspective, 25:1-3, 32-38, DOI: 10.1080/19393555.2015.1132800

To link to this article: https://doi.org/10.1080/19393555.2015.1132800

Published online: 21 Jan 2016.

INFORMATION SECURITY JOURNAL: A GLOBAL PERSPECTIVE
2016, VOL. 25, NOS. 1–3, 32–38
http://dx.doi.org/10.1080/19393555.2015.1132800

Taylor & Francis
Taylor & Francis Group

Cyber crime risk awareness in Kyrgyz Republic

Rita Ismailova and Gulshat Muhametjanova

Department of Computer Engineering, Faculty of Engineering, Kyrgyz-Turkish Manas University, Bishkek, Kyrgyz Republic

ABSTRACT

In this paper we present the information security awareness rate of students in Kyrgyz Republic, where there is a rapid pace of formation and development of the information society. The survey was conducted with a sample of 172 students from different departments of the university. Our research study showed that despite the huge number of reports about computer crimes in the web, the knowledge about cybercrime is quite low and students are mostly not aware of many aspects of computer crime. Analysis was done to determine dependence of information security awareness rate on computer literacy rate and the education field of students. We conclude that although information technology is of wide usage, the information security topics need to be taught to prevent them from becoming victims of cyber crime.

KEYWORDS

Cyber crime; computer literacy; information security awareness; Kyrgyz Republic

1. Introduction

The Internet has become a socio-technical system of systems (Laplante, Michael, & Voas, 2009). All aspects of human life are more or less dependent on software. With the growing role of this system, the number of crimes committed by means of computer technologies has also increased. Although many models for cyber crime investigations have been proposed (Ciardhuáin, 2004), a crime over cyber space is generally not perceived as a crime which is punishable.

In Howard and Longstaff (1998), a cyber attack has been defined as an "event that occurs on a computer or network that is intended to result in something that is not authorized to happen" (p. 11). In Gandhi et al. (2011), it has been defined as any act by an insider or an outsider that compromises the security expectations of an individual, organization, or nation. According to the environment (Hundley & Anderson, 1996), cyber attacks can affect data, processing, applications, and the network.

Although cyber attack can be defined, there is no generally accepted definition for cyber crime. According to the United Nations Office on Drugs and Crime, "a limited number of acts against the confidentiality, integrity and availability of computer data or systems represent the core of cybercrime" (p. 11); however, in general, any crime conducted via the Internet or some other computer network can be defined as a cyber crime.

Currently, due to developments in information technologies, many crimes have digital "traces." Thus, computerized crime has been evolved slowly, so there was time for development of countermeasures as well. Illegal activities held over cyber space are relatively new forms of crime. This type of crimes conducted via the Internet or some other computer network. Mainly it becomes possible due to low level of information security awareness among network users. As Korpela (2015) indicated, security starts at the end user security awareness can affect every aspect of an organization's security profile.

While the growth of cyber crime in developed countries was generally phased with the development of information technology, in the Kyrgyz Republic as well as in many other countries with similar backgrounds, it appeared suddenly. Internet penetration rate in Kyrgyz Republic is at 24.17%, and, according to Internet World Stats (2014), out of 158 countries it is ranked 112. In spite of the low Internet penetration rate in Kyrgyz Republic, young people, especially students in higher education

CONTACT Rita Ismailova rita.ismailova@manas.edu.kg, ritochkina@gmail.com Kyrgyz-Turkish Manas University, Chyngyz Aitmatov Campus (Jal), Faculty of Engineering, 521, Bishkek, Kyrgyz Republic.

institutions, are using the Internet frequently. However, Internet users were not ready for crimes that were brought by global network. Even among students, the Information Security Awareness (ISA) rate has never been studied. According to National Statistics Committee, in 2013, only 1.9% (i.e., 80 out of 4,198) of government agencies were connected to computer networks and 6.26% (263 out of 4,198) of government agencies and companies have websites (NSC, 2015). Thus, the traffic goes mostly abroad. In the report by (Kaspersky Lab, 2015), it is informed that the spear phishing email messages were used as a transmission vector, and victims were mostly Russian-speaking financial institutions. This increases the risk of becoming a victim for users in Kyrgyz Republic, since mostly Russian websites are in use, making it important to improve the information security awareness rate among Internet users. The aim of this work is to determine the level of knowledge of risks in the cyber space among students in the Kyrgyz Republic.

2. Related works

With the development of information technologies, the rate of illegal activities in cyber space has become a real threat. Despite the growth of computer literacy and Internet penetration rates, the level of information security awareness among users is still low. At the same time, however, cyber space crimes no longer require complex skills or techniques, mostly because of the top level hackers who develop and make available many hacking techniques or tools. Especially, the number of young people from developing countries involved in cyber crime has increased the rate of financial fraud in Internet (Holt, 2007). Since the baggage of knowledge needed for hacking becomes less, the information security awareness rate should be raised.

Siponen (2000) analyzed approaches in the area of information security awareness and education from the viewpoint of the theoretical framework and showed strengths and weaknesses. Many authors studied the ISA within organizations (e.g., Bulgurcu, Cavusoglu, & Benbasat, 2010) where employees' attitude, normative beliefs, and self-efficacy to comply were examined, while others (e.g., Claburn, 2005; Ernst & Young, 2008) rely on technology-based solutions.

Information security awareness rates of certain groups or population have not been studied well. Though Boyce and Jennings (2002) stated that security awareness comes along with users' understanding of security policies, procedures, and practices so users could make sound judgments if a potential security issue occurs when there is no further guidance. Thus, the problem of estimating a user's understanding rate becomes vital in information security.

In Fakeh, Zulhemay, Shahibi, Ali, and Zaini (2012), information security awareness amongst academic librarians was studied, which showed that the level of information security awareness was relatively high.

In Arfi and Agarwal (2014a), information security literacy among elders in India was examined. According to the authors, the residence type of elderly people has an effect on their level of knowledge. The authors (2014b) also showed that gender does not influence the knowledge about information security.

The same year, Lean-Ping and Chien-Fatt published their results about multi-dimension assessment of an individual's information security awareness level in (Ong & Chong, 2014). In the research by Yunos, Ahmad, and Mohd Sabri (2015), 22 experts from Critical National Information Infrastructure took part in an interview session about a proposed cyber terrorism conceptual framework and provided supportive guidelines as to whether an action by someone is within the framework of cyber terrorism.

As can be seen from the literature review, there a few works concerning the information security awareness level from human factor point of view. McClain et al. (2015) explained that it was hard to collect data since cyber operations at most organizations are considered to be sensitive, and it was easier to conduct research based on the security training exercises of college graduates and college students. Therefore, in the current research, we decided to evaluate the information security awareness rate among students.

3. Method

3.1. Participants

The study obtained a sample of students in the universities in Kyrgyz Republic. Questionnaires were distributed both online and in paper form. The response rate for online questionnaire was 27.83%. Printed questionnaires were distributed among instructors, with a return rate of 69%. Thus, the total sample comprised 172 students between 19 and 35 years old. In our sample, there are 32% male and 68% female students. The majority of participants are undergraduate students 16–23 years old (95.3%), and M.S. and Ph.D. students of age 26–35 (4.7%). Cumulative grade point average (CGPA) ranges from 0.90 to 4.00. Marital status includes 9 married (5.2%), 158 not married (91.9), and 5 who did not answer.

3.2. Materials

Respondents were asked the question about having a personal computer and, if the answer was "yes," whether the computer was connected to the Internet. Next, the computer literacy rate was examined using six questions, asking if the respondents have a good knowledge of main concepts of a computer, hardware, operating system, text editors, spread sheets, and presentation-making programs. Thus, before analyzing the information security awareness, the computer literacy level and Internet penetration rate were studied within a given sample. In Chen, Shaw, and Yang (2006), the authors conducted this study in the context of an actual organization and developed the online tests to measure the general security awareness level of users.

The ISA rate was analyzed according to 31 questions of a 3-point Likert type scale, with values 1 = disagree, 2 = partially agree, and 3 = agree on knowledge of cybercrimes (KoC); and seven 3-point Likert type questions on frequency of occurrence of different cyber crime events (FoC) (1 = never happens, 2 = happens sometimes, and 3 = happens often).

In addition, open ended questions on comparison of real crime and crime over Internet were asked.

3.3. Procedure

For this study responses from students were collected both in written form through direct questionnaires and online survey using Google forms. The questions were adopted from Arfi and Agarwal (2014a) and corrected taking into account the Kyrgyz Republic Penal Code.

4. Results

4.1. Demographic overview

According to the questionnaire results, the response rate of students with a personal computer is 73.8%, while an Internet penetration rate is only 54.1%; that is, almost half of the respondents do not have connection to the global web, which is the main threat to information security. As it is shown in Table 1, students distribution according to faculty show that most of the students were from the Faculty of Education (45.3%), followed by Faculty of Economics (39%) and Faculty of Engineering (15.7%).

4.2. Relationship between computer literacy and information security awareness rate

The next part of the questionnaire determines the general knowledge level of students in terms of computer usage, since it is essential for analyzing the level of threats in cyber space. Among respondents, 50.6% stated that they have strong knowledge of general computer concepts, 31.4% have strong knowledge of computer hardware, 43.6% said that they are good with operating systems, 62.8% are good text editors, 39.5% are good at spread sheets, and 57% have strong knowledge of presentation programs.

The answers to information security awareness questions showed that 47.1% of students have a high level of knowledge and 52.9% have an average level. None of the students had a low level of ISA. However, in the evaluation of cyber crime occurrence frequency, 4.1% of students showed

Table 1. Demographic profile of respondents.

Category	Subcategories	Percentages %	Frequency
Gender	Male	32	55
	Female	68	117
Age	16–20 years	70.9	122
	21–24 years	24.4	42
	25–29 years	1.2	2
	Over 30 years	2.9	5
Faculty	Engineering	15.7	27
	Education	45.3	78
	Economics	39.0	67
Have home computer	Yes	73.8	127
	No	26.2	45
Internet access	Yes	54.1	93
	No	45.9	79

Table 2. Level of ISA.

		Frequency	
N	Level of knowledge	f	%
1	Low	7	4.1
2	Medium	106	61.6
3	High	59	34.3

low knowledge results, 61.6% showed average, and only 34.3% showed high results (Table 2).

As a next step, the relationship between the computer literacy rate and ISA rate was analyzed. It was expected that the strong knowledge of computer concepts would imply a higher level of ISA knowledge. The One-Way ANOVA Test was conducted to see if the hypothesis is correct (Table 3).

Because most flexible and most conservative (Tabachnick & Fidell, 2001) we used Scheffee post-hoc comparisons (Table 4). According to results, the ISA rate of students whose computer literacy rate is low and medium do not differ with MD = –.16, SD = .08, p > .05, while students with low and high level of computer literacy show significant difference in terms of ISA knowledge with MD = –.22, SD = .08, p < .05. The ISA rate of students based on frequency of cyber crime occurrence questions (FoC) do not differ for all three groups of students.

This result suggests that especially students from group with high level of computer literacy and low level group do differ.

4.3. Relationship between students faculty and information security awareness rate

In this section, we analyze the relationship between education field and the level of digital risks knowledge of students. Students' distribution according to faculty is defined as Faculty of Education (45.3%), Faculty of Economics (39%), and Faculty of Engineering (15.7%).

Here, the relationship between students' faculty and ISA rate was analyzed. It was expected that the students from the Engineering faculty would be more aware of risks coming from the Internet. The One-Way ANOVA Test was conducted to see if the hypothesis is correct.

The ANOVA (Table 5) showed that there is a statistically significant difference between student's education field and ISA rate for all three areas of knowledge—general computer literacy rate (GCLR), question on knowledge of cyber crimes (KoC), and questions on frequency of occurrence of different cyber crime events (FoC). The degrees

Table 3. ANOVA of ISA rate in terms of GCL rate.

		Sum of squares	df	Mean square	F	Sig.
Knowledge of cyber crimes	Between groups	.713	2	.356	3.411	.035
	Within groups	17.655	169	.104		
	Total	18.367	171			
Frequency of cyber crimes	Between groups	1.243	2	.621	3.815	.024
	Within groups	27.523	169	.163		
	Total	28.766	171			

The ANOVA indicated significant difference between Computer Literacy Rate and ISA rate, for both general agree-disagree questions and frequency questions, F(2, 169) = 3.411, p = 0.035 and F(2,169) = 3.815, p = 0.024, respectively (Table 3). That is, there is a relationship between computer literacy and the ISA rate.

Table 4. Post hoc tests of ISA rate in terms of GCL rate.

Dependent variable		(I) General	(J) General	Mean difference (I-J)	Std. error	Sig.
Knowledge of cyber crimes	Scheffe	Low	Medium	–.16	.08	.144
			High	–.22*	.08	.036
		Medium	Low	.16	.08	.144
			High	–.05	.05	.546
		High	Low	.22*	.08	.036
			Medium	.06	.05	.546
Frequency of cyber crimes	Scheffe	Low	Medium	.20	.10	.149
			High	.04	.11	.926
		Medium	Low	–.20	.10	.149
			High	–.16	.07	.059
		High	Low	–.04	.11	.926
			Medium	.16	.07	.059

*The mean difference is significant at the 0.05 level.

Table 5. ANOVA of ISA rate in terms of students faculty.

		Sum of squares	df	Mean square	F	Sig.
General computer literacy rate	Between groups	9.72	2	4.865	21.500	.000
	Within groups	38.23	169	.226		
	Total	47.96	171			
Knowledge of cyber crimes	Between groups	.40	2	.201	1.894	.154
	Within groups	17.96	169	.106		
	Total	18.36	171			
Frequency of cyber crimes	Between groups	.11	2	.056	.329	.720
	Within groups	28.65	169	.170		
	Total	28.76	171			

Table 6. Post hoc tests of GCL rate in terms of students faculty.

Dependent variable		(I) faculty	(J) faculty	Mean difference (I-J)	Std. error	Sig.
General computer literacy rate	Scheffe	Economics	Engineering	−.44*	.11	.000
			Education	.25*	.08	.008
		Engineering	Economics	.44*	.11	.000
			Education	.69*	.11	.000
		Education	Economics	−.25*	.08	.008
			Engineering	−.69*	.11	.000

*The mean difference is significant at the 0.05 level.

of freedom are F(2, 169) = 21.50, F(2, 169) = 1.89, and F(2, 169) = .329, respectively. The significance is $p < 0.05$ for GCLR and $p > 0.05$ for two other areas showing the ISA rate (both KoC and FoC). That is, there is no direct relationship between student studying engineering and other students in terms of their awareness of risks coming from Internet. Nevertheless, the study field does impact students' general computer literacy level.

According to results, the GCLR of students from different faculties are significantly different, $p < .05$ for all compared pairs of faculties (Table 6). Thus, students from three faculties have dissimilar attainments level in information technology.

5. Discussion and conclusion

In this work, the information security awareness rate was studied among students in the Kyrgyz Republic. Since the "Internetization" in the Kyrgyz Republic is similar to this process in former Soviet republics, it can be assumed that the same pattern can be observed in those countries as well. However, national statistical committees on ICT development of the Commonwealth of Independent States (Ministry of National Economy of the Republic of Kazakhstan, Committee on Statistics, 2015a; Ministry of National Economy of the Republic of Kazakhstan, Committee on Statistics, 2015b; The State Committee of Republic of Uzbekistan on Statistics, 2015; The State Statistical Committee of the Republic of Azerbaijan, 2015) as well as a report on Global ICT Developments by International Telecommunication Union (ITU, 2014), (ITU, 2013) showed that in CI countries there is the least variation in ICT performance. However, there are only a few research studies conducted in the Kyrgyz Republic (and in ex-soviet territory) in terms of computer literacy and internet penetration rates and no study about students' knowledge in the field of cyber crime (Akin, 2013). According to Muhametjanova and Çagiltay (2012), in 2012 only 42.8% of students had a personal computer at home and only 28.1% had Internet access at home. In three years, these numbers have increased to 73.8% of students who have a personal computer, while the Internet penetration rate increased to 54.1%. These rates are important to evaluate the ISA rate since connection to the global web increases the rate of information security risks. Although Internet threats in the Kyrgyz Republic are the "lowest" level of cyber crime—hooliganism, hacktivism, and cyber fraud (Кутнаева, 2014)—the risks are growing. For example, in five month of 2015 there were seven attacks on government websites in the Kyrgyz Republic, while in all of 2014 there were four attacks (Ismailova, 2015). Therefore, it is important for the country in this stage of information and communication technology development to increase the security awareness of users.

According to the National Statistics Committee (2015), the Internet penetration rate is quite low; as a results, students are mostly not familiar with many aspects of computer crime. Moreover, as our research showed, many of them do not consider some cyber crime types as a crime at all. This might be partially explained by the fact that in the Kyrgyz Republic Penal Code, there is only one section concerning cyber crime (which shall be punished by a public apology or a fine of five hundred to one thousand payment indicators (approximately US $7,500–15,000) or restriction of freedom for up to three years, or imprisonment up to three years). In addition, answers to the open-ended question showed that people mostly do not consider a cyber crime as a crime at all. Respondents were asked to rate the crime: if personal data are stolen by breaking into a house and by breaking into an Internet account. According to their answers, the first one is definitely as a robber, while the hacker is just a "smart guy" and should be encouraged rather than punished.

Furthermore, the result showed that the more computer literate a student is, the higher level of knowledge in threats of cyber space he has. In addition, the analysis indicated that there is no difference between students studying engineering and other students in terms of their awareness of risks coming from Internet. Nevertheless, the study field does impact students' general computer literacy level. Thus, students from three faculties have dissimilar attainments level in information technology.

Although this research shed light on students' attitudes toward cyber crime and revealed problems in this field, the results were mostly predictable, given the "computerization" background of the Kyrgyz Republic. The most surprising and unexpected result is that hacking is not considered a crime but an advantageous skill. Thus, there are still many unanswered questions concerning information security awareness rates in the Kyrgyz Republic, and we believe further research studies are necessary. There is no doubt, however, that students must be taught about the existence of cyber crime and that cyber crimes are punishable.

ORCID

Rita Ismailova http://orcid.org/0000-0003-0308-2315

References

Akin, M. S. (2013). Computer and internet usage in higher education in developing countries: Case for Kyrgyz university students. *International Journal of Information Technology and Business Management*, *12*(1), 41–48.

Arfi, N., & Agarwal, S. (2014a). A study on level of knowledge regarding cybercrime among elderly residing in homes and old age homes. *International Journal for Research in Applied Science and Engineering Technology*, *2*(6), 30–34.

Arfi, N., & Agarwal, S. (2014b). Knowledge of cyber crime among elderly across gender. *International Journal for Advance Research in Engineering and Technology*, *2*(2), 7–9.

Boyce, J., & Jennings, D. (2002). *Information assurance: Managing organizational IT security risks*. London: Butterworth-Heinemann.

Bulgurcu, B., Cavusoglu, H., & Benbasat, I. (2010). Information security policy compliance: An empirical study of rationality-based beliefs and information security awareness. *MIS Quarterly*, *34*(3), 523–548.

Chen, C. C., Shaw, R. S., & Yang, S. C. (2006). Mitigating information security risks by increasing user security awareness: A case study of an information security awareness system. *Information Technology Learning and Performance Journal*, *24*(1), 1.

Ciardhuáin, S. Ó. (2004). An extended model of cybercrime investigations. *International Journal of Digital Evidence*, *3*(1), 1–22.

Claburn, T. (2005, 17 Januray). Machine wars: The battle between good and evil in cyberspace is increasingly fought with automated tools. *InformationWeek*, 54–63. Retrieved from http://www.informationweek.com/machine-wars/d/d-id/1029687?

Ernst & Young. (2008). *Moving Beyond Compliance: Ernst & Young's 2008 Global Information Security Survey*. Retrieved from http://www.ey.com/Publication/vwLUAssets/2008_Global_Information_Security_Survey_english/$FILE/2008_GISS_ingles.pdf

Fakeh, S. K. W., Zulhemay, M. N., Shahibi, M. S., Ali, J., & Zaini, M. K. (2012). Information security awareness amongst academic librarians. *Journal of Applied Sciences Research*, *8*(3), 1723–1735.

Gandhi, R., Sharma, A., Mahoney, W., Sousan, W., Zhu, Q., & Laplante, P. (2011). Dimensions of cyber-attacks: Cultural, social, economic, and political. *Technology and Society Magazine, IEEE*, *30*(1), 28–38. doi:10.1109/MTS.2011.940293

Holt, T. J. (2007). Subcultural evolution. Examining the influence of on-and off-line experiences on deviant subcultures. *Deviant Behavior*, *28*(2), 171–198. doi:10.1080/01639620601131065

Howard, J. D., & Longstaff, T. A. (1998). A common language for computer security incidents. *Sandia National Laboratories.*

Hundley, H. O., & Anderson, R. H. (1996). Emerging challenge: Security and safety in cyberspace. *Technology and Society Magazine, IEEE*, *14*(4), 19–28. doi:10.1109/44.476633

Internet World Stats. (2014). *Internet users by country (2014)*. Retrieved from http://www.internetlivestats.com

Ismailova, R. (2015). Website accessibility, usability and security: A survey of government websites in Kyrgyz Republic. *Universal Access in Information Society*, *16*(2), 1–8.

ITU. (2013). *Measuring the Information Society Report 2014*. Retrieved from http://www.itu.int/en/ITU-D/Statistics/Documents/publications/mis2014/MIS2014_without_Annex_4.pdf

ITU. (2014). *Measuring the Information Society Report 2015*. Retrieved from http://www.itu.int/en/ITU-D/Statistics/Documents/publications/misr2015/MISR2015-w5.pdf

Kaspersky Lab. (2015). Carbanak APT: The Great Bank Robbery. *Securelist*. Retrieved from https://securelist.com/files/2015/02/Carbanak_APT_eng.pdf

Korpela, K. (2015). Improving cyber security awareness and training programs with data analytics. *Information Security Journal: A Global Perspective*, *24*(1–3), 72–77.

Laplante, P., Michael, B., & Voas, J. (2009). Cyberpandemics: History, inevitability, response. *IEEE Security and Privacy*, *7*(1), 63–67. doi:10.1109/MSP.2009.4

McClain, J., Silva, A., Emmanuel, G., Anderson, B., Nauer, K., Abbott, R., & Forsythe, C. (2015). Human performance factors in cyber security forensic analysis. *Procedia Manufacturing*, *3*, 5301–5307. doi:10.1016/j.promfg.2015.07.621

Ministry of National Economy of the Republic of Kazakhstan, Committee on Statistics. (2015a). *Internet users per 100 inhabitants*. Retrieved from http://www.stat.gov.kz/getImg?id=ESTAT079459

Ministry of National Economy of the Republic of Kazakhstan, Committee on Statistics. (2015b). Доля пользователей сетью Интернет (2015b). *Percentage of internet users*. Retrieved from http://www.stat.gov.kz/getImg?id=ESTAT095594

Muhametjanova, G., & Çagiltay, K. (2012, July). Students' and instructors' perceptions on use of information and communication technologies during instruction in a Kyrgyzstan University. In *2012 IEEE 12th International Conference on Advanced Learning Technologies (ICALT)* (pp. 500–502). Piscataway, NJ: IEEE.

National Statistics Committee. (2015). *26.06.2015/Information and Communication Technologies in Kyrgyz Republic 2009–2013*. Retrieved from http://new.stat.kg/media/publicationarchive/30e40cc2-0587-4f0f-b7f0-d488351e30b3.doc

Ong, L., & Chong, C. (2014, January). Information Security Awareness: An Application of Psychological Factors–A Study in Malaysia. In *2014 International Conference on Computer, Communications and Information Technology (CCIT 2014)* (pp. 98–101). Paris, France: Atlantis Press.

Siponen, M. T. (2000). A conceptual foundation for organizational information security awareness. *Information Management & Computer Security*, *8*(1), 31–41. doi:10.1108/09685220010371394

Tabachnick, B. G., & Fidell, L. S. (2001). *Using multivariate statistics* (6th ed.). Boston, MA: Allyn & Bacon.

The State Committee of Republic of Uzbekistan on Statistics. (2015) Potential grows in ICT-sphere. *Report by Acrom Sultanov, Head of Information Service of Goskomstat*. Retrieved from http://old.stat.uz/en/press/6640/

The State Statistical Committee of the Republic of Azerbaijan. (2015). *Main macro indicators of information and communication*. Retrieved from http://www.stat.gov.az/source/communication/en/001_1en.xls

Yunos, Z., Ahmad, R., & Mohd Sabri, N. A. (2015). A qualitative analysis for evaluating a cyber terrorism framework in Malaysia. *Information Security Journal: A Global Perspective*, *24*(1–3), 15–23.

Кутнаева, Н. (2014). Сложности кибербезопасности в Центральной Азии (The complexities of cyber security in Central Asia). *per Concordiam*, *2*(5), 14–19.

Biographies

Rita Ismailova received B.S. in Applied Mathematics and Informatics from Kyrgyz State National University (Kyrgyz National University of Jusup Balasagyn), Bishkek, Kyrgyzstan, in 2001; M.S. in Applied Mathematics from Kyrgyz State National University (Kyrgyz National University of Jusup Balasagyn), Bishkek, Kyrgyzstan, in 2003; and Ph.D. in Cryptography from Middle East Technical University, Ankara, Turkey, in 2012. Current research interests include cryptography, information security, and electronic government.

Gulshat Muhametjanova received B.S. in Computer Engineering from Kyrgyz Turkish Manas University, Bishkek, Kyrgyzstan, in 2004 and a PhD on B.S. in Computer Education and Instructional Technologies from Middle East Technical University, Ankara, Turkey, in 2014. Current research interests include technology integration, e-learning, distance education, and social networking sites.