ISSN 2518-1467 (Online),
ISSN 1991-3494 (Print)

ҚАЗАҚСТАН РЕСПУБЛИКАСЫ
ҰЛТТЫҚ ҒЫЛЫМ АКАДЕМИЯСЫНЫҢ

ХАБАРШЫСЫ

ВЕСТНИК

НАЦИОНАЛЬНОЙ АКАДЕМИИ НАУК
РЕСПУБЛИКИ КАЗАХСТАН

THE BULLETIN

OF THE NATIONAL ACADEMY OF SCIENCES
OF THE REPUBLIC OF KAZAKHSTAN

1944 ЖЫЛДАН ШЫҒА БАСТАҒАН
ИЗДАЕТСЯ С 1944 ГОДА
PUBLISHED SINCE 1944

1

АЛМАТЫ
АЛМАТЫ
ALMATY

2018

JANUARY
ЯНВАРЬ
ҚАҢТАР

Clarivate Analytics

NAS RK is pleased to announce that Bulletin of NAS RK scientific journal has been accepted for indexing in the Emerging Sources Citation Index, a new edition of Web of Science. Content in this index is under consideration by Clarivate Analytics to be accepted in the Science Citation Index Expanded, the Social Sciences Citation Index, and the Arts & Humanities Citation Index. The quality and depth of content Web of Science offers to researchers, authors, publishers, and institutions sets it apart from other research databases. The inclusion of Bulletin of NAS RK in the Emerging Sources Citation Index demonstrates our dedication to providing the most relevant and influential multidiscipline content to our community.

Қазақстан Республикасы Ұлттық ғылым академиясы "ҚР ҰҒА Хабаршысы" ғылыми журналының Web of Science-тің жаңаланған нұсқасы Emerging Sources Citation Index-те индекстелуге қабылданғанын хабарлайды. Бұл индекстелу барысында Clarivate Analytics компаниясы журналды одан әрі the Science Citation Index Expanded, the Social Sciences Citation Index және the Arts & Humanities Citation Index-ке қабылдау мәселесін қарастыруда. Web of Science зерттеушілер, авторлар, баспашылар мен мекемелерге контент тереңдігі мен сапасын ұсынады. ҚР ҰҒА Хабаршысының Emerging Sources Citation Index-ке енуі біздің қоғамдастық үшін ең өзекті және беделді мультидисциплинарлы контентке адалдығымызды білдіреді.

НАН РК сообщает, что научный журнал «Вестник НАН РК» был принят для индексирования в Emerging Sources Citation Index, обновленной версии Web of Science. Содержание в этом индексировании находится в стадии рассмотрения компанией Clarivate Analytics для дальнейшего принятия журнала в the Science Citation Index Expanded, the Social Sciences Citation Index и the Arts & Humanities Citation Index. Web of Science предлагает качество и глубину контента для исследователей, авторов, издателей и учреждений. Включение Вестника НАН РК в Emerging Sources Citation Index демонстрирует нашу приверженность к наиболее актуальному и влиятельному мультидисциплинарному контенту для нашего сообщества.

«Қазақстан Республикасы Ұлттық ғылым академиясының Хабаршысы».
ISSN 2518-1467 (Online),
ISSN 1991-3494 (Print)
Меншіктенуші: «Қазақстан Республикасының Ұлттық ғылым академиясы»РҚБ (Алматы қ.)
Қазақстан республикасының Мәдениет пен ақпарат министрлігінің Ақпарат және мұрағат комитетінде 01.06.2006 ж. берілген **№5551-Ж** мерзімдік басылым тіркеуіне қойылу туралы куәлік

Мерзімділігі: жылына 6 рет.
Тиражы: 2000 дана.

Редакцияның мекенжайы: 050010, Алматы қ., Шевченко көш., 28, 219 бөл., 220, тел.: 272-13-19, 272-13-18,
www: nauka-nanrk.kz, bulletin-science.kz

Типографияның мекенжайы: «Аруна» ЖК, Алматы қ., Муратбаева көш., 75.

«Вестник Национальной академии наук Республики Казахстан».
ISSN 2518-1467 (Online),
ISSN 1991-3494 (Print)
Собственник: РОО «Национальная академия наук Республики Казахстан» (г. Алматы)
Свидетельство о постановке на учет периодического печатного издания в Комитете информации и архивов Министерства культуры и информации Республики Казахстан **№5551-Ж**, выданное 01.06.2006 г.

Периодичность: 6 раз в год
Тираж: 2000 экземпляров

Адрес редакции: 050010, г. Алматы, ул. Шевченко, 28, ком. 219, 220, тел. 272-13-19, 272-13-18.
www: nauka-nanrk.kz, bulletin-science.kz

Адрес типографии: ИП «Аруна», г. Алматы, ул. Муратбаева, 75

Bulletin of the National Academy of Sciences of the Republic of Kazakhstan.
ISSN 2518-1467 (Online),
ISSN 1991-3494 (Print)
Owner: RPA "National Academy of Sciences of the Republic of Kazakhstan" (Almaty)
The certificate of registration of a periodic printed publication in the Committee of Information and Archives of the Ministry of Culture and Information of the Republic of Kazakhstan N 5551-Ж, issued 01.06.2006

Periodicity: 6 times a year
Circulation: 2000 copies

Editorial address: 28, Shevchenko str., of. 219, 220, Almaty, 050010, tel. 272-13-19, 272-13-18,
http://nauka-nanrk.kz /, http://bulletin-science.kz

Address of printing house: ST "Aruna", 75, Muratbayev str, Almaty

BULLETIN OF NATIONAL ACADEMY OF SCIENCES
OF THE REPUBLIC OF KAZAKHSTAN
ISSN 1991-3494
Volume 1, Number 371 (2018), 94 – 101

UDC 342.003.347/1

N. V. Kushzhanov, U. Zh. Aliyev

Turan-Astana University, Astana, Kazakhstan.
E-mail: kushzhan@bk.ru aliyevu@mail.ru

DIGITAL SPACE: CHANGES IN SOCIETY AND SECURITY AWARENESS

Abstract. Digital transformation of world permits all areas in our life from economy to policy, society and culture. The recent scandal with community service center and data protection showed how much sensitive we are in front of cyber-attacks and vulnerable when it comes to our personal security. The security awareness is necessary skill in present life, it's important for our job, social interactions and etc. EAUE stepped in new stage of interaction its formation of Digital Space, where no borders or limitation of information and resources. Cybersecurity as a national strategy and plan needs to deliver not only better security in government and business services, but a fundamental shift in the safety of the electronic environment in which they operate. Over the last 20 years, the IT community has failed to deliver a data utility that has the level of trust common in other utilities. What can the IT community do to turn around the current obstacles to developing an effective digital society? The purpose of this research paper is to discuss the security challenges that are associated with the digital age. The topic of cyber security is one that should be talked about more often in today's society. This paper points out the importance of cyber security awareness and protection. It touches on the major ideas of why our community and corporations are currently in a predicament. Lastly, the paper ends with proposed solutions on what can be done to address cyber security challenges in digital life.

Keywords: security; mobile devices; security awareness; cyber threats, digitalization, digital space.

Introduction. Mobile devices (i.e., cellphones, laptops, tablets) have become an indispensable part of our everyday life, since they fulfill the increasing users' desire for Internet connectivity and access to information, social and private networks at any time and place. Owing to the proliferation of "smart" devices and the escalating dependency on them with respect to the execution of everyday tasks, they have evolved from a communication medium to a multifunctional equipment. The reduced cost, in combination with the increasing computational and storage capacity of mobile devices, allow them to accommodate critical functionalities with significant security and safety related impact such as e-banking, control systems and Internet of things architectures. Such devices do not simply store information related to their owners, but also receive data on people and infrastructure related in some way to them. As a result, they can retrieve, store and modify extensive quantities of diverse and potentially sensitive information.

Furthermore, the users are accustomed to the notion of continuous connectivity, even across networks with potentially unknown configurations. Such transmissions are likely to be vulnerable to unauthorized access and, consequently, they constitute a security risk. In many cases, these risks materialize as direct criminal attacks, such as privacy intrusions or unauthorized disruptions of communication. Moreover, they can expose the users to more complex types of malicious activity, such as identity theft, blackmailing, active data collection, or defamation. In light of the increasing risks due to the aforementioned use of mobile devices, it is important that users are aware of the risks they are exposed to and, more importantly, that they are informed about how to protect themselves.

The exponential spread and scale-up of digital technologies and services has profound global implications, creating opportunities for sustainable development and inclusive growth, but at the same time new threats and challenges. Digitalization has an important role to play in a wide range of areas including gender, good governance, transparency and accountability, the fight against corruption, job creation and private sector development, access to micro-finance, improving access to public services - notably energy, protecting the environment and addressing climate change, providing humanitarian aid, promoting education, health or agriculture. As such, digital solutions can help combat poverty, contribute to better targeting and the linking of humanitarian and development activities, and help to manage migration and address shortcomings in a number of EU partner countries where identification and civil registries, digital entrepreneurship and Small and Medium Enterprises (SME's), e-Services, e-Government, mobile financing or blockchain secured transactions can reduce inequalities and increase prosperity. Digitalization acts as an accelerator and enabler of many, perhaps all of the SDGs. The 2030 Agenda for Sustainable Development sets specific targets in this respect.

Security awareness is the knowledge and attitude members of an organization possess regarding the protection of the physical, and especially *informational*, assets of that organization. Many organizations require formal security awareness training for all workers when they join the organization and periodically thereafter, usually annually.

The ability to evolve a digital society and to gain the many promised benefits depends in large part on a widespread confidence in the fabric of cyberspace. The denial-of-service attacks against Paypal and Amazon.com (2010), CNN (2008), Twitter (2009), the Australian Parliament (2010) and US oil firms (2011) may or may not have been successful in damaging the target, and indeed may have been used for publicity by Internet security companies, but they have increased public concern over security in cyberspace. The more serious intrusion attacks against Sony Corp. (in which credit card details of thousands of gamers were released) and RSA (in which highly sensitive information relating to its secure two-factor authentication device was compromised) demonstrate that the Internet is increasingly a very dangerous place to operate.

So what has changed on the Internet? The answer, of course, is everything – business activities, information technology, the communications environment and the threat landscape. Today, vendors and attackers have become embroiled in a cyber arms race, and users are the losers. There are regular reports of government and business systems being infiltrated and data breaches in government departments. Consumers' computers, wireless modems and, increasingly, cell phones are being subverted, and even the basic fabric of cyberspace is under attack, with nations demonstrating their ability to take control of the Internet.

In the last five years, there have been a number of fundamental shifts in technology and its use that require equally fundamental shifts in attitudes towards security. Information technology has evolved from purely a means of systems automation into an essential characteristic of society: cyberspace. The kind of quality, reliability and availability that has traditionally been associated only with power and water utilities is now essential for the technology used to deliver government and business services running in cyberspace.

Technology is changing rapidly, and another fundamental shift is occurring with the emergence of cloud computing. Cloud computing enables individuals and organizations to access application services and data from anywhere via a web interface; it is essentially an application service provider model of delivery with attitude. The economies possible through use of cloud, rather than internal IT solutions, will inevitably see the majority of businesses and, increasingly, governments running in the cloud within the next five years. This substantially changes the ways in which organizations can affect and manage both their IT function and security in their systems.

Today's security standards were developed in a world in which computers were subject to fraud and other criminal activities by individuals inside and, in some cases, outside the organization. However, this has changed in the last five years with the rapid increase in organized cybercrime through the emergence of robot networks (botnets), which enable criminal activity to be conducted on an unprecedented global scale and can also be used as force multipliers to deliver massive denial-of-service attacks on targeted businesses – at a level at which nations are increasingly at risk of being cut off from the global Internet.

Unfortunately, the capability of national police forces to stop global cybercrime is developing much more slowly than the technical abilities of cybercriminals. Cybercrime is now arguably a bigger issue than illegal drugs. The adoption of the Council of Europe Convention on Cybercrime is setting the scene for a global response to cybercrime, and there are signs that police forces globally are working together. However, much more needs to be done to develop the concept of a global jurisdiction before an adequately agile response to cybercrime can be developed.

Understanding the Threat Source. Clearly, understanding the source of any threat and the likelihood of the threat being a danger to an organisation's business interests is a critical first step in building a cybersecurity strategy. Steven Bucci describes the threat actors as shown in figure.

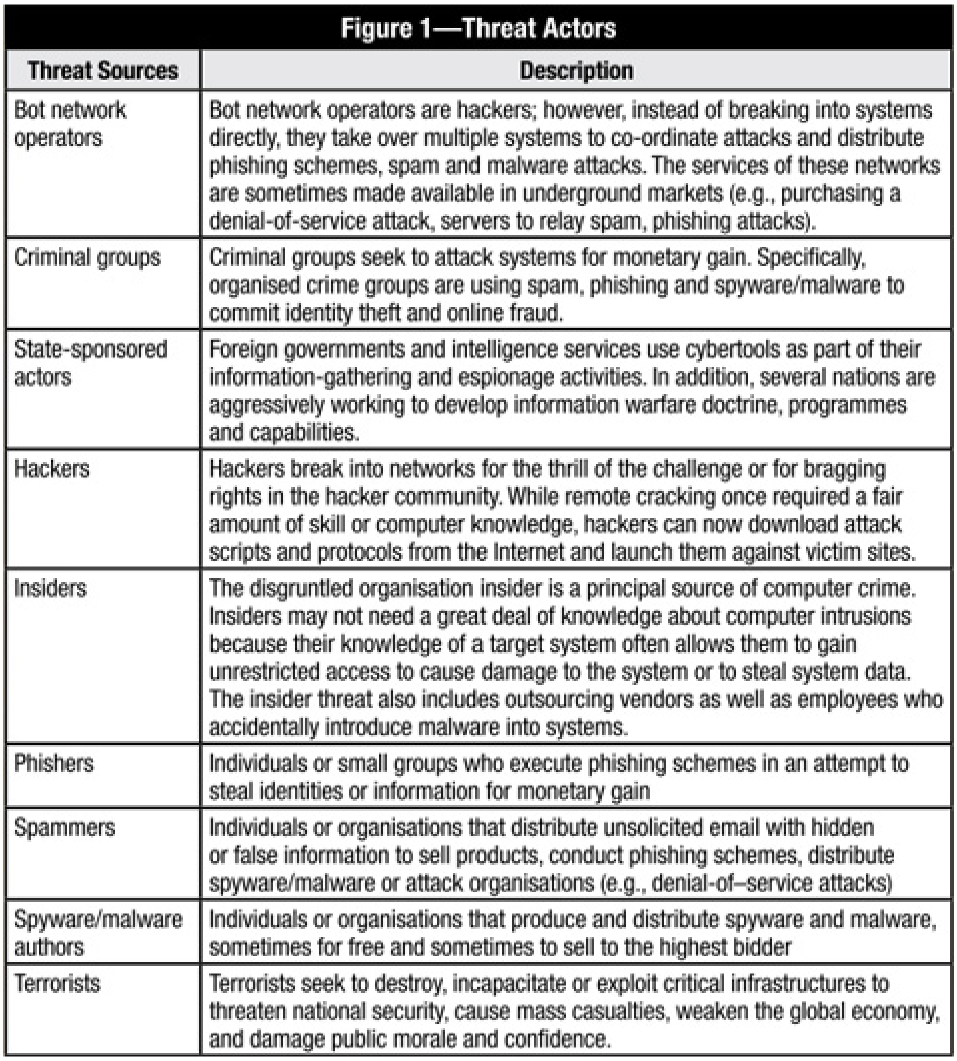

Figure 1—Threat Actors

Threat Sources	Description
Bot network operators	Bot network operators are hackers; however, instead of breaking into systems directly, they take over multiple systems to co-ordinate attacks and distribute phishing schemes, spam and malware attacks. The services of these networks are sometimes made available in underground markets (e.g., purchasing a denial-of-service attack, servers to relay spam, phishing attacks).
Criminal groups	Criminal groups seek to attack systems for monetary gain. Specifically, organised crime groups are using spam, phishing and spyware/malware to commit identity theft and online fraud.
State-sponsored actors	Foreign governments and intelligence services use cybertools as part of their information-gathering and espionage activities. In addition, several nations are aggressively working to develop information warfare doctrine, programmes and capabilities.
Hackers	Hackers break into networks for the thrill of the challenge or for bragging rights in the hacker community. While remote cracking once required a fair amount of skill or computer knowledge, hackers can now download attack scripts and protocols from the Internet and launch them against victim sites.
Insiders	The disgruntled organisation insider is a principal source of computer crime. Insiders may not need a great deal of knowledge about computer intrusions because their knowledge of a target system often allows them to gain unrestricted access to cause damage to the system or to steal system data. The insider threat also includes outsourcing vendors as well as employees who accidentally introduce malware into systems.
Phishers	Individuals or small groups who execute phishing schemes in an attempt to steal identities or information for monetary gain
Spammers	Individuals or organisations that distribute unsolicited email with hidden or false information to sell products, conduct phishing schemes, distribute spyware/malware or attack organisations (e.g., denial-of–service attacks)
Spyware/malware authors	Individuals or organisations that produce and distribute spyware and malware, sometimes for free and sometimes to sell to the highest bidder
Terrorists	Terrorists seek to destroy, incapacitate or exploit critical infrastructures to threaten national security, cause mass casualties, weaken the global economy, and damage public morale and confidence.

Steven Bucci"s model of treat factors

Steven Bucci shows that while cyberthreats are changing from individual hackers through organized crime and terrorist-based attacks to national- or state-sponsored cyberattacks, the level of danger is correspondingly increasing. Thus, while individuals may cause mayhem, it has been largely unsustainable and fairly contained. Now an attack may result in widespread destruction and an ongoing undermining of state sovereignty.

There is no single solution or panacea to the issues of cybersecurity, nor should there be. Each organization should assess what its needs are, how it intends to conduct its business activities and what the risks are to that process. There is a plethora of highly capable solutions that can then be implemented and, more important, maintained.

Consumers in cyberspace, be they government, industry or society, continue to be more mobile, more demanding and less tolerant of failure. While there is an increased awareness of threats, often the increased adoption of security comes only after data breaches and system failures.

What is cyber security and why should we care? Cyber security has become a new concept in the last decade. With technology advancing every day our society is becoming more connected than we have ever been before. While these advances are making our daily lives easier they are also adding extra risks to our personal information. Most people do not think about their identities getting stolen when they make an online purchase, check their email, or use social media. However, each time that you put your personal information on the Internet you are at risk of that information getting stolen. This is especially true for students, who spend so much time online doing school activities. Every time that they login to do school work, they are putting themselves at risk. There are many simple ways that these risks can be reduced, but it starts with cyber security awareness.

Cyber Security. The internet is not a secured space. It is an area where currently there are not many regulations. It is where anyone can put up, take down, or gather as much information as they want (Hall, 2012). It is open for anyone to place any information that they want online. Cyber security is becoming an increasingly talked about topic. With more and more people making their personal information available online than ever before, it is becoming a hacker's paradise. There are multiple different schemes that have been happening recently that are associated with Internet usage. Some of these scams involve hackers cracking passwords to get access to personal information and criminals using phishing techniques to gather information that they can use to steal individual's identities. Lastly, some schemes include phishing techniques used to con people out of money (Jansson & von Solms, 2013).

However, most individuals do not know about all of these scams and are unaware when they are happening to them. Because of this, people do not know how to protect themselves and how to stop being a target. It is important that we, as a nation, focus on making these individuals aware of the potential risks associated with the Internet. Cyber security needs to be more common knowledge and education needs to be more readily available. It is important for us to help educate individuals on what they can do to stop and prevent potential cyber security attacks. It is also especially important that our students to be able to recognize potential threats. Therefore, cyber security, awareness, and education needs to be taught at the higher education level.

Awareness. We log into our email account, bank account, or social media account and we do not even think about the process. These are the types of activities that hacker's make a living off of. The majority of people are not only unaware that cyber threats are real, but are also unaware of what to do about them. Most people just hope or assume that identity theft and phishing attacks are not going to happen to them. Ignorance is bliss after all. But, making society aware that even the smallest tasks can pose potential threats is crucial for their safety.

Awareness is the first step in reducing the number of identity thefts and personal information threats. The majority of individuals understand that by having their personal information online that they are taking a risk of that information being compromised. However, they do not possess the knowledge to know how to protect themselves. These people also understand that they should not include very sensitive information online, such as their social security numbers. Yet, they do not realize that even accessing your email could be just as detrimental to their safety.

Individuals believe that if they have a unique password then they are protecting themselves enough that they do not have to worry about cyber security threats (McCrohan, Engel, & Harvey, 2010). While this is a good first step, and it is strongly recommended to create unique passwords, it still simply is not enough to keep information private. Most hackers have the technology and knowledge to know how to decrypt these passwords or bypass them completely. Each day that our technology is improving is another day that hackers are figuring out how to crack that technology. "There is no argument whatsoever that the proliferation of devices and information are empowering. Technology is today far more democratically available than it was yesterday and less than it will be tomorrow" (Geer, 2015).

Likewise, much of the population believes that installing virus protection or spy software onto their computers is enough. They think that this software is going to save them from ever being hacked or having their information stolen (McCrohan, Engel, & Harvey, 2010). This is also simply not true. We need to change this way of thinking by helping society recognize the signs of the potential threats and risks. We then need to hand them the information that they need to keep themselves safe and protected. Some of the signs that users need to be aware of that usually indicate a phishing attempt are: words being misspelled, a certain degree of urgency or "deadlines", fake names and web links, and a request for personal information (Lungu & Tăbuşcă, 2010).

Mobile Awareness. Cyber security threats are not only common with computers. These threats are becoming increasingly popular on mobile devices. This is something that everyone, including students need to become aware of as well. With just as much information, if not more, on our cell phones as on our computers, hackers are starting to utilize the same technics that they do for computer phishing as they are now using for mobile device phishing. This threat is also something that students also need to recognize and become aware of. Behaviors need to change with both computer and mobile device usage. Just because your phone is almost always in your possession does not mean that the information in it is secured.

Education needs to become more available for both computer security and mobile device security as well. Many corporations are at risk because their employees are not knowledgeable on internet protection. This problem is one that needs to be addressed at the higher education level with college students (Patten & Harris, 2013). Many of the same security threats that are associated with computers are also associated with mobile devices. However, mobile devices pose more threats and challenges when it comes to protecting your information. This is because your cell phone usually holds more personal data than your computer does. Also, with mobile devices constantly moving in and out of Wi-Fi networks, many of which are unsecured, it makes stealing data easier for hackers. Another problem with mobile device security is the amount of malware being downloaded from App downloads. Malware on mobile devices is now higher than it is for PCs (Patten & Harris, 2013).

Creating a Safer Future. Teaching cyber security awareness and protection to students is not only important for their personal safety, but it is also setting us up for a safer future. Many of the threats that companies face could have been prevented if their employees were more educated on the subject of cyber security. “The state cyber-security in the United States is suffering from a lack of attention from industry and academia” (Pappalardo, 2004). This is leaving large corporations unprotected because their employees are not trained in this field. This is also leaving many of their client’s personal information unsafe and unsecured. It is the responsibility of The Department of Education to address attention to this major issue.

In fact, this issue is becoming “a matter of local and global importance” (U.S. Schools Not Preparing Kids for Digital Age, 2013). The workplace is filled with challenges associated with the digital age. Students in the United States are coming out of college not prepared to handles these challenges. This is making it difficult for employers who are looking for an IT professional that can help them with their cyber security needs. Since employers are not able to find these professionals who are both trained in general IT and security, it is leaving the employers and their company vulnerable. “Not only must students know how to stay safer online at school and at home, but they also must be equipped to deal with the workplace challenges of the digital age” (U.S. Schools Not Preparing Kids for Digital Age, 2013).

Technology is continuing to change and therefore curriculum needs to be changing along with it. “Cybersecurity is perhaps the most difficult intellectual profession on the planet” (Geer, 2015). Employers are realizing that they need more employees that have technology and security knowledge, but are finding it difficult to find students with the right combination of knowledge and expertise (Patten & Harris, 2013). They are finding that students are usually trained in specific areas of IT, but not with knowledge of cyber security practices. Colleges and Universities should be steering students towards degrees and careers that focus on cyber security and IT practices for the future safety of US organizations (Peterson, 2014).

Proposed Solutions. So what is to be done about this ever increasing dilemma? Well, there are a few options. The first option is to make everyone aware of the problem and get them excited about learning about cyber security. President Obama has taken the first step in making this come to life. He has declared that October will be National Cyber Security Awareness Month (Homeland Security, 2016). NCSAM is all about getting both the public and private sectors aware that the internet affect’s all of our daily lives, whether we realize it or not. The month is filled with events that are aimed at making the community aware of the threats associated with the internet. In addition to NCSAM, January 28th has been declared National Data Privacy Day (StaySafeOnline.org). On this day the National Cyber Security Alliance holds an event to promote cyber security awareness. They encourage users to STOP. THINK. CONNECT. All of these events are a great way to get information out to the public. However, for it to sink in for users and to make a difference we need this information to be important all year long, not just in October or on January 28th. These events are great for awareness and for getting the public excited about cyber security, but the end goal is for this information to be important year round.

The second option to solving this problem is starting cyber security education at younger ages. This topic should be just as important as history and gym. We need to start education in the middle school and high school levels. If we education students when they are younger, then there is a chance that we can get them excited about cyber security. We can create passion in students and they will then continue with that passion into college and their future careers. "Kids and teens have embraced the digital world with great intensity, spending as many as eight hours a day online by some estimates" (U.S. Schools Not Preparing Kids for Digital Age, 2013). This option will work because kids are already interested in the digital world, now we need to get them interested in how to protect themselves. We need to create a generation of cyber security enthusiasts.

The third option is to better educate our teachers. A major reason that our students are not educated on the affects cyber security is because our teachers are not educated on the subject either. "Yet, few …educators are teaching topics that would prepare students to be cyber-capable employees or cybersecurity-aware college students" (U.S. Schools Not Preparing Kids for Digital Age, 2013). The only way that we can expect student's behavior to change is if we teach them the proper way to handle these situations. Therefore, students who are now enrolled in teaching programs should be required to take cyber security courses. And current teachers should focus on online safety and cyber security awareness when taking continuing education courses and professional development training.

Lastly, the fourth option is for the academic community and corporations to team up (Pappalardo, 2004). We need to know what these corporations are looking for in an IT professional when they come out of college. We need to know what their company's needs are. Then the academic community will be able to come up with curriculum that meets and exceeds those needs. We need to start producing college graduates that possess the knowledge, skills, and capabilities to handle the new challenges that are associated with the digital age and cyber security.

Conclusion. Cyber security awareness is more important now than it has ever been before. Threats to personal information is increasing and identities are getting stolen every day. Making individuals aware of this is the first step. The second step is giving individuals the tools and knowledge that they need to protect themselves.

Being security aware means you understand that there is the potential for some people to deliberately or accidentally steal, damage, or misuse the data that is stored within a company's computer systems and throughout its organization. Therefore, it would be prudent to support the assets of the institution (information, physical, and personal) by trying to stop that from happening.

According to the European Network and Information Security Agency, 'Awareness of the risks and available safeguards is the first line of defense for the security of information systems and networks. With technology advancing every day our society is becoming more connected than we have ever been before. While these advances are making our daily lives easier they are also adding extra risks to our personal information. Most people do not think about their identities getting stolen when they make an online purchase, check their email, or use social media. However, each time that you put your personal information on the Internet you are at risk of that information getting stolen. This is especially true for young generation, who spend so much time online doing school activities. Every time that they login to do some work; they are putting themselves at risk. There are many simple ways that these risks can be reduced, but it starts with cyber security awareness.

The Internet and social media have become powerful channels for learning about public policy issues, exhorting friends and family to vote and supporting one's favorite causes or candidates. Over the last 20 years, there has been immense growth in the number of computing and network services, enabling transactions to be undertaken by the smallest businesses across a global marketplace. At the same time, there has been a growing community of individuals who have sought to exploit the vulnerabilities of network devices, computer systems and applications.

IT systems have proved over the last 20 years to be less than perfect, requiring compensating controls to address problems when they arise. Vendors continually release tactical patches and upgrades to fix problems, but hackers with knowledge, skills and capability have developed and released exploits and easy-to-use tools to enable even the least technical users to become adversaries. Security is not an adjunct or add-on to cyberspace; it is a fundamental aspect that must be considered alongside all other core functions to ensure that the business can meet its strategic objectives. Academics need to include cybersecurity as a core component of computer and information science to deliver a workforce properly prepared for its role in the digital society. The organization's leaders need to ensure that security architectures are developed to reflect the needs of the business, that the people it employs are certified professionals and tradespeople, and that the technology products and services that it uses are fit for purpose. For its part, government can usefully set the necessary standards and lead by example.

New governance models need to be developed that provide a consistent and effective basis for trust in a business process co-sourcing environment, and should ensure the existence of testing, monitoring and business continuity. Security technology continues to be complex and unwieldy, and not well aligned with consumer needs. Having to remember multiple IDs and complex passwords is a major inconvenience and a cause of many security issues. Posting personal information to public sites continues to be a contributing factor to identity theft. Firewalls protect what information is left behind inside the corporate electronic perimeter, but do little to protect the vast amount of business-sensitive information outside. Intrusion detection systems detect yesterday's problems, but not tomorrow's problems. Security models, architectures and technologies need to reflect these concerns.

Multiple activities within the business do not mean that there should be multiple security architectures to support them. Having a single, consistent and persistent approach that is proven and flexible is much easier to maintain. However, this does require a good understanding of the business objectives, the operational market and the risks the business faces. Hence, the security model must recognize that protection of services and information in itself is not enough; the company must be able to recover from failure and continue to operate at a level expected by its operating partners and customers. And, it must be able to demonstrate that capability on a continuous basis.

REFERENCES

[1] Lella A. Lipsman A. The US Mobile App Report. 2014. Available online: http://www.comscore.com/Insights/Presentationsand-Whitepapers/2014/The-US-Mobile-App-Report (accessed on 8 April 2015).

[2] Chin E., Felt A.P., Sekar V., Wagner D. Measuring user confidence in smartphone security and privacy. In Proceedings of the Eighth Symposium on Usable Privacy and Security, Washington, DC, USA, 11–13 July 2012. [Google Scholar]

[3] Felt A.P., Ha E., Egelman S., Haney A., Chin E., Wagner D. Android permissions: User attention, comprehension, and behavior. In Proceedings of the Eighth Symposium on Usable Privacy and Security, Washington, DC, USA, 11–13 July 2012. [Google Scholar]

[4] Mylonas A., Kastania A., Gritzalis D. Delegate the smartphone user? Security awareness in smartphone platforms. Comput. Secur. **2013**, 34, 47–66. [Google Scholar] [CrossRef]

[5] Ophoff J., Robinson M. Exploring end-user smartphone security awareness within a South African context. In Proceedings of the 2014 Information Security for South Africa, Johannesburg, South Africa, 13–14 August 2014. [Google Scholar]

[6] Parker F., Ophoff J., Van Belle J.P., Karia R. Security awareness and adoption of security controls by smartphone users. In Proceedings of the 2015 Second International Conference on Information Security and Cyber Forensics (InfoSec), Cape Town, South Africa, 15–17 November 2015. [Google Scholar]

[7] Markelj B., Bernik I. Safe use of mobile devices arises from knowing the threats. J. Inf. Secur. Appl. **2015**, 20, 84–89. [Google Scholar] [CrossRef]

[8] Markelj B., Zgaga S. Comprehension of cyber threats and their consequences in Slovenia. Comput. Law Secur. Rev.**2016**, 32, 513–525. [Google Scholar] [CrossRef]

[9] Sheila, M.; Faizal, M.; Shahrin, S. Dimension of mobile security model: Mobile user security threats and awareness. Int. J. Mob. Learn. Organ. **2015**, 9, 66–85. [Google Scholar] [CrossRef]

[10] Ariu D., Bosco F., Ferraris V., Perri P., Spolti G., Stirparo P., Vaciago G., Zanero S. Security of the Digital Natives. 2014. Available online: https://ssrn.com/abstract=2442037 (accessed on 13 October 2016).

[11] Norman G. Likert scales, levels of measurement and the "laws" of statistics. Adv. Health Sci. Educ. **2010**, 15, 625–632. [Google Scholar] [CrossRef] [PubMed111ryt5]

[12] Lampson Butler W. 'Computer Security in the Real World', IEEE Computer, 6 June 2004, http://research.microsoft.com/en-us/um/people/blampson/69-SecurityRealIEEE/69-SecurityRealIEEEpub.pdf

[13] Williams Alex 'RSA Breach: An Attack That Used a Social Media Boobytrap?', ReadWrite Enterprise, 18 March 2011, www.readwriteweb.com/enterprise/2011/03/rsa-breach-an-attack-that-used

[14] Greenberg Andy. 'When Cyber Terrorism Becomes State Censorship', Forbes.com. US Department of Defense, Cyber Strategy, www.defense.gov/home/features/2011/0411_cyberstrategy/

[15] Bucci Steven. 'The Confluence of Cyber Crime and Terrorism', The Heritage Foundation, 12 June 2009, www.heritage.org/Research/Lecture/The-Confluence-of-Cyber-Crime-and-Terrorism

[16] The Jericho Forum Vision, www.opengroup.org/jericho/Gasser, Morrie; Andy Goldstein; Charlie Kaufman; Butler Lampson; 'The Digital Distributed System Security Architecture', 1989, http://research.microsoft.com/en-us/um/people/blampson/41-DigitalDSSA/41-DigitalDSSAAsPub.pdf

[17] Geer D. (2015). Six Key Areas of Investment for the Science of Cyber Security. Futurist, 49(1), 10-15.

[18] Hall C. (2012). Security of the Internet and the Known Unknowns. Communications of the ACM, 55(6), 35-37. doi:10.1145/2184319.2184332

[19] Homeland Security. (2016, March 24). Retrieved March 24, 2016, from https://www.dhs.gov/national-cyber-security-awareness-month

[20] Jansson K., von Solms R. (2013). Phishing for phishing awareness. Behaviour & Information Technology, 32(6), 584-593. doi:10.1080/0144929X.2011.632650

[21] Lungu I., Tăbuşcă A. (2010). Optimizing Anti-Phishing Solutions Based on User Awareness, Education and the Use of the Latest Web Security Solutions.Informatica

[22] Economica, 14(2), 27-36.

[23] McCrohan K.F., Engel K., Harvey J.W. (2010). Influence of Awareness and Training on Cyber Security. Journal Of Internet Commerce, 9(1), 23-41. doi:10.1080/15332861.2010.487415

[24] National Cyber Security Alliance | StaySafeOnline.org. (n.d.). Retrieved April 11, 2016, from https://staysafeonline.org/

[25] Pappalardo J. (2004). Cyber-security Hampered by Lack of Attention. National Defense,89(610)

Н. В. Күшжан, О. Ж. Әлиев

«Тұран-Астана» университеті, Астана, Қазақстан

САНДЫҚ КЕҢІСТІК: ҚОҒАМДАҒЫ ӨЗГЕРІСТЕР ЖӘНЕ ҚАУІПСІЗДІК МӘСЕЛЕЛЕРІ

Аннотация. Әлемдегі сандық жаңару өмірімізде экономикадан бастап саясатқа дейінгі аймақты, қоғам мен мәдениетті қамтиды. Жақын арада халыққа қызмет көрсету орталығындағы жеке мәліметтердің жоғалу жағдайы біздің кибершабуылға әлсіздігімізді көрсетті, бұл жерде қауіпсіздік мәселесі де бар. Қауіпсіздік шараларын білу және түсіну – өзіміздің жұмысымыз үшін, әлеуметтік қарым-қатынастар үшін қажет дағды. ЕАЭС өзара қарым-қатынастың жаңа кезеңіне аяқ басты, бұл – ақпарат пен ресурстарда шектеу болмайтын Сандық Кеңістіктің қалыптасуы. Киберқауіпсіздік ұлттық стратегия сияқты дамуы керек, ол іскерлік қызмет көрсету нарығында қауіпсіздікті қамтамасыз етіп қоймай, IT қоршаған ортадағы қауіпсіздікті түпкілікті өзгерту жоспарын да қамтиды. Бұл ғылыми-зерттеу жұмыстарының мақсаты – сандық ғасырмен байланысты қауіпсіздік мәселелерін талқылау. Киберқауіпсіздік тақырыбы бүгінгі қоғамда жиі айтылатын мәселе. Аталған мақала қоғамдағы қауіпсіздік мәселесін тұтастай қарастырады. Біз сандық өмірде киберқауіпсіздікті қамтамасыз ететін нақты шешімдерді ұсындық

Түйін сөздер: қауіпсіздік, мобильді құрылғылар, қауіпсіздік мәселелері, кибер қауіптер, сандық кеңістік, сандық трансформациясы.

Н. В. Кушжанов, У. Ж. Алиев

Университет «Туран-Астана», Астана, Казахстан

ЦИФРОВОЕ ПРОСТРАНСТВО: ИЗМЕНЕНИЯ В ОБЩЕСТВЕ И ВОПРОСЫ БЕЗОПАСНОСТИ

Аннотация. Цифровое преобразование мира охватывает все области нашей жизни – от экономики до политики, общества и культуры. Недавний скандал с ЦОН и утечкой личных данных показал, насколько уязвимы мы перед кибератаками, когда дело доходит до нашей личной безопасности. Знание и понимание мер безопасности – необходимый навык в существующей жизни, это важно для нашей работы, социальных взаимодействий и т.д. ЕАЭС вступил в новый этап взаимодействия, это – формирование Цифрового Пространства, где не существуют границ или ограничений информации и ресурсов. Кибербезопасность должна развиваться как национальная стратегия и план, в рамках, которых должна обеспечить не только лучшую безопасность в правительстве и рынке деловых услугах, но и фундаментальное изменение в безопасности IT окружающей среды, в которой они работают. Цель этой научно-исследовательской работы состоит в том, чтобы обсудить проблемы безопасности, которые связаны с цифровым веком. Тема кибербезопасности – это та проблема, о которой нужно говорить чаще в сегодняшнем обществе. Данная статья рассматривает проблемы безопасности общества в целом. Мы попытались предложить определенные решения того, что может быть сделано, для того, чтобы обеспечить кибербезопасность в цифровой жизни.

Ключевые слова: безопасность; мобильные устройства; вопросы безопасности; кибер угрозы, цифровая трансформация, цифровое пространство.

Publication Ethics and Publication Malpractice
in the journals of the National Academy of Sciences of the Republic of Kazakhstan

For information on Ethics in publishing and Ethical guidelines for journal publication see http://www.elsevier.com/publishingethics and http://www.elsevier.com/journal-authors/ethics.

Submission of an article to the National Academy of Sciences of the Republic of Kazakhstan implies that the described work has not been published previously (except in the form of an abstract or as part of a published lecture or academic thesis or as an electronic preprint, see http://www.elsevier.com/postingpolicy), that it is not under consideration for publication elsewhere, that its publication is approved by all authors and tacitly or explicitly by the responsible authorities where the work was carried out, and that, if accepted, it will not be published elsewhere in the same form, in English or in any other language, including electronically without the written consent of the copyright-holder. In particular, translations into English of papers already published in another language are not accepted.

No other forms of scientific misconduct are allowed, such as plagiarism, falsification, fraudulent data, incorrect interpretation of other works, incorrect citations, etc. The National Academy of Sciences of the Republic of Kazakhstan follows the Code of Conduct of the Committee on Publication Ethics (COPE), and follows the COPE Flowcharts for Resolving Cases of Suspected Misconduct (http://publicationethics.org/files/u2/New_Code.pdf). To verify originality, your article may be checked by the Cross Check originality detection service http://www.elsevier.com/editors/plagdetect.

The authors are obliged to participate in peer review process and be ready to provide corrections, clarifications, retractions and apologies when needed. All authors of a paper should have significantly contributed to the research.

The reviewers should provide objective judgments and should point out relevant published works which are not yet cited. Reviewed articles should be treated confidentially. The reviewers will be chosen in such a way that there is no conflict of interests with respect to the research, the authors and/or the research funders.

The editors have complete responsibility and authority to reject or accept a paper, and they will only accept a paper when reasonably certain. They will preserve anonymity of reviewers and promote publication of corrections, clarifications, retractions and apologies when needed. The acceptance of a paper automatically implies the copyright transfer to the National Academy of Sciences of the Republic of Kazakhstan.

The Editorial Board of the National Academy of Sciences of the Republic of Kazakhstan will monitor and safeguard publishing ethics.

Правила оформления статьи для публикации в журнале смотреть на сайте:

www:nauka-nanrk.kz

ISSN 2518-1467 (Online), ISSN 1991-3494 (Print)

http://www.bulletin-science.kz/index.php/ru/

Редакторы *М. С. Ахметова, Т. М. Апендиев, Д. С. Аленов*
Верстка на компьютере *Д. Н. Калкабековой*

Подписано в печать 16.02.2018.
Формат 60x881/8. Бумага офсетная. Печать – ризограф.
14,2 п.л. Тираж 2000. Заказ 1.

Национальная академия наук РК
050010, Алматы, ул. Шевченко, 28, т. 272-13-18, 272-13-19