XIV Международная конференция

«Стратегия качества в промышленности и образовании»

4 -7 июня 2018 г., Варна, Болгария

МАТЕРИАЛЫ

(в 2-х томах)

ТОМ 1

XIV International Conference

«Strategy of Quality in Industry and Education»

June 4-7 2018, Varna, Bulgaria

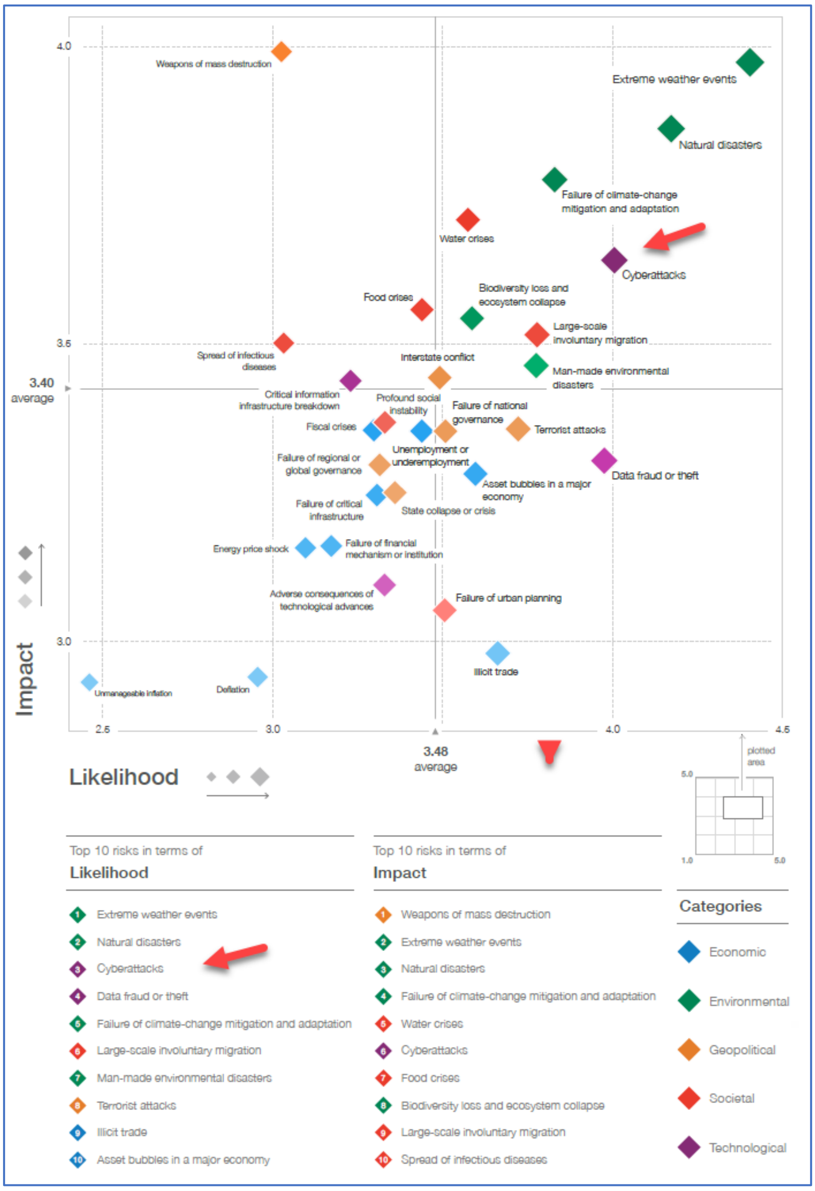
PROCEEDINGS

VOLUME 1

STRATEGY OF THE HIGHER EDUCATIONS OF UKRAINE IN TRAINING OF EXPERTS ON INFORMATIONAL AND CYBER SECURITY

Professor, Doctor of Science Y.V. Borsukovskii
State University of Telecommunications, Kyiv, Ukraine
Project Manager V.Y. Borsukovska
PJSC «Ukrsotsbank», Kyiv, Ukraine
Professor, Doctor of Technical Science V.L. Buriachok
Borys Grinchenko Kyiv University, Kyiv, Ukraine

In October 2017 the European Council again called the attention and assigned the task to enhance the cyber security actions within EU countries. The provided regulations underline the necessity in joint actions to combat cybercrimes. Cybercrimes and malware "… is the most global threat for our societies and economies. Due to the cyber-attacks we lose more than 400 bln Euro throughout the world. And this strictly underline the emergency in use of existent instruments in EU to increase the stability in cyberspace and react to the massive cyber incidents…" – reports the European Council [3].



Picture 1 - Global landscape of threats 2018

In 2018 the Davos Forum again in global topic "Creating a Shared Future in a Fractured World" discussed the combating the world`s cyber threats. Global landscape of threats presented to the Forum is provided on Picture 1 [4].

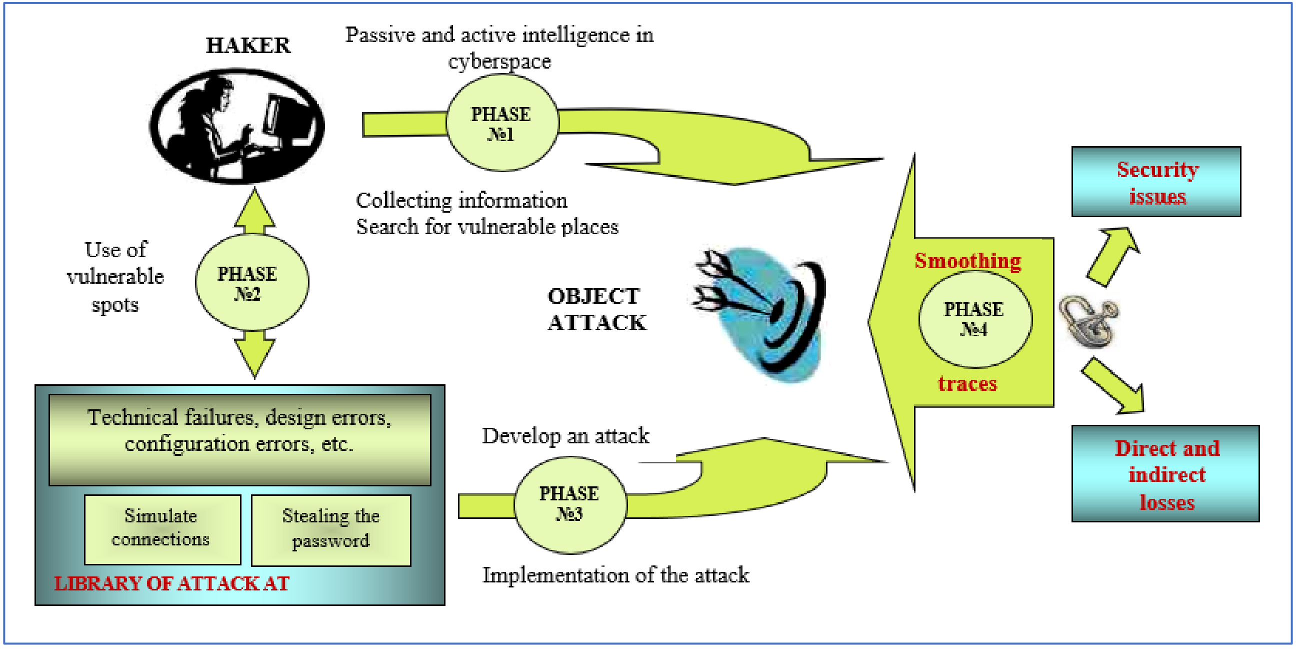
R-Vision Company on the basis of analysis of vendor`s forecasts for informational security (IS) had concluded the TOP-10 threats in informational sphere for [12], especially:

- use of machine learning and artificial intellect – applied for automated search of threats, increase of attacks accuracy, execution of sophisticated fishing attacks;

- further development of ransomware – such programs remains a key component in 2018landscape of threats, its families will increase, and hacker’s focus will move to mobile devices;
- IoT vulnerabilities will be used more often, considering the numerous devices are produces without any security rules and any industry standards;
- Hacking of mass media and social networks accounts to share the false information – shall mean the impact to stock market quotes, manipulation with public opinion, negative impact to the reputation, propaganda via hacked channels, etc.;
- Increase in attacks to manufacturing facilities – spin up in preparation and realization of complex cyberattacks in manufacturing facilities by means of cyber espionage and expert knowledges of Computer-Assisted Management of Technical Processes and industry specifics;
- Attack of ghost and light viruses – ghost malware does not write to hard drive the files and execute all its actions in memory, and during the system restart the virus is vanished, but it already damaged the system, and detect, trace or stop such an attack is extremely hard;
- Attacks on mobile applications. The main targets are Android and iOS platforms – increase in attacks frequency and improvement of prevention technologies will cause the appearance of more complicated APT-malwares for mobile platforms;
- Attacks on the cloud infrastructure and storages – leak of date from public cloud storages which may lead to access for private keys, passwords, private information and even intellectual property;
- Exploitation of vulnerabilities in mobile networks, as well Wi-Fi and Bluetooth protocols. Mobile network vulnerabilities are those of critical nature. For example, using mobile networks the self-driving cars exchange the data on speed, car`s geolocation on roads and other data. So, the DDoS-attack on such a car can ruin its driving and at last have the disastrous result;
- Revival of hardware attacks. Such attacks are directed on Intel Management Engine vulnerabilities. If the hackers could manage to use them, so on the other level will be used the target attacks, as well the crypto lockers, when the issue is not just limited with data blocking, but also with destroy of system board.

As one may see, the list of threats for world`s society varies much: starting from uncontrolled inflation up to extreme weather conditions, from any infections up to cyberattacks, from terrorism to collapse of government. Global trends which may cause the serious problems – shall include the climate changes, increasing cyber dependency of mankind, essential separation due to incomes level, and increasing polarization of the society [6].

World Economic Forum experts consider the world to face the exact crucial period when the focus of the world`s critical energy is directed especially to incitement of hatred. Mass cases of fraud with data and/or its theft cause not only the economic damage, but also cause geopolitical intensity and loss of confidence in Internet that automatically may lead to essential social unrest with unpredicted consequences [6]. Besides, the development and dissemination of perspective informational systems and technologies promote the new forms of cyber-attacks which expose the governmental and corporate resources to threats with which they are not ready deal with. In that due to statistics, the most widespread are considered the DDoS-attacks, and the most dangerous are considered the ART-attacks. The general scheme for the mentioned attacks is provided on the Picture 2 [9, 10].



Picture 2 – General scheme for hacker attack

As well, the one more joint and directed vector of attack was named by the Alexandr Liamin, Director General, Qrator Labs: “The main difference between 2016 and 2017 is that the criminals had turned their attention from hacking separate devices to attacks on cloud and IoT platforms. Internet of things provides criminals with access to the thousands of working machines at once, and frequently such intrusions remain unnoticed. Economic efficiency – is the reason we await for increase in frequency of similar attacks to the whole clouds and platforms in 2018” [11].

World Economic Forum defined the cybercrimes to be the most crucial global risks, and the cyber-attacks may cause the critical threat to the economics, states and societies which have the deficiencies in cooperation and lack of efficient system of informational and cyber protection. Cyber-attacks vectors analysis shows that the cyber-space has the strict tendency to a kind of hybrid war. The main precondition for such a tendency shall be the increasing interest of governmental structures in receiving of information which can be used by opposing parties in world`s competitor and political fights [7, 8]. Due to experts estimations the annual losses of world economy under the cybercrime may reach the 500 bln USD, considering the annual GDP of the Switzerland in 2017 is equal to 659 bln USD.

Obvious, that the cyber-attacks problems stay beyond the forces and organizations which trying to combat it separately. Only cooperation, information exchange and general standards will enforce the world community to counteract to these electronic crimes [5].

Considering world tendencies on cybersecurity, in January 2018 the World

Economic Forum had taken a decision for creation of Global Cyber Security Centre to ensure further development of the safe and secure cyberspace [5]. The Centre is aimed to create the first international platform for governments, companies, experts and law-enforcement agencies for cooperation and elimination of cyber securities problems. "…If we want to prevent a digital dark age, we need to work harder to make sure the benefits and potential of the Fourth Industrial Revolution are secure and safe for society. The new Global Centre for Cybersecurity is designed as the first platform to tackle today's cyber-risks in a truly global manner," said Alois Zwinggi, Managing Director at the World Economic Forum and Head of the Global Centre for Cybersecurity [5]. The main tasks of this Centre shall be the consolidation of existing cybersecurity initiatives of the World Economic Forum, establishment of an independent library of cyber best practices, help to the partners to enhance knowledge on cybersecurity, work towards an appropriate and agile regulatory framework on cybersecurity, serves as a laboratory and early-warning think tank for future cybersecurity scenarios. Global Centre for Cybersecurity will support primarily the governments and sectoral companies – Forum participants – to ensure the safe protection of the cyberspace using the approach providing the engagement of other parties of interest [4].

The general analysis of trends in cybersecurity demonstrates that the number of attacks on the state and private organizations in the world are permanently increasing and the attacks became more and more sophisticated. As well, it is harder to identify the attacks initiators. Such situation requires the dynamic adaptation of the informational and cyber security systems to the current and fast changed threats, and to the requirements, tasks and scope of the modern economy and business. In its turn, this requires the definition of the priority directions for training of specialists in informational and cybersecurity according to the provided landscape of global risks within informational sphere:

Threat model should consider the fact that in case of target attack the criminals will get 100% success. Taking current axiom the relevant changes should be implemented to the infrastructure of IT and informational and cyber security, and with high level of probability – to some business processes which could be critical in case of successful cyber-attack.

According to the defined risks, IT and informational and cyber security infrastructure should be developed on the basis of multi echelon organizational and technical levels of security using the best world practices, recommendations and methodology PCI, NIST, ISO and HIPAA.

Today, the experts define the following key directions which should be covered by the priority attention in training of cybersecurity specialists [2, 9, 10]:

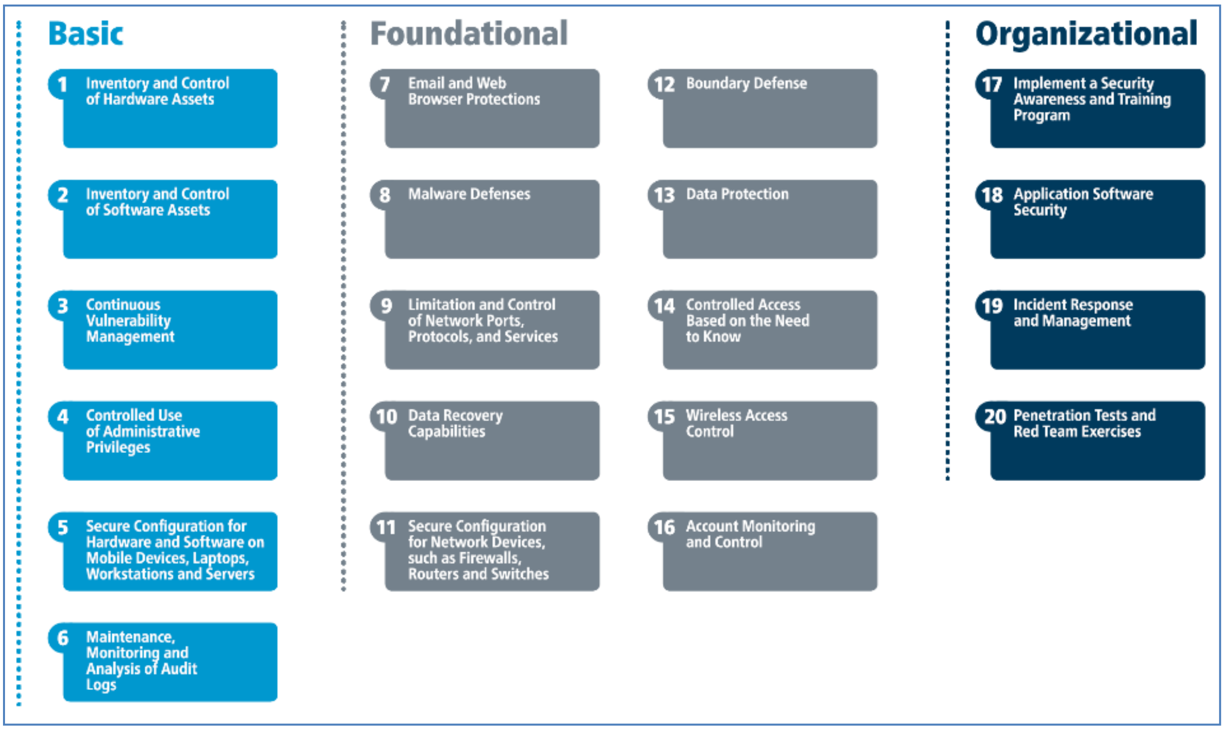
- analysis of current attacks and modern requirements to IT-technologies;
- authentication, encryption and development of the white list of applications:
- analysis and comparison of decisions taken with an existent methodologies and handbooks;
- approaches for use of products to ensure informational and cyber security;
- testing for vulnerabilities and evaluation of correspondence to the acting security

standards;

- use of world community recommendations in development of sectoral system of informational security.

Here we completely rely on CIS recommendations [1, 2] for establishment of separate training profiles for training of specialists in protection of informational state and corporate systems. These profiles should include the approaches and method for comprehensive verification of IT-infrastructure elements, configuration, access rights, privileges, log systems, actions and measures to react to the incidents, and principles of verification initiation.

In CIS Controls Version 7 [1, 2] these elements are divided to the three controls, that consider the current landscape of cyber threats (picture 3) – Basic, Foundational and Organizational.



Basic

1 Inventory and Control of Hardware Assets

2 Inventory and Control of Software Assets

3 Continuous Vulnerability Management

4 Controlled Use of Administrative Privileges

5 Secure Configuration for Hardware and Software on Mobile Devices, Laptops, Workstations and Servers

6 Maintenance, Monitoring and Analysis of Audit Logs

Foundational

7 Email and Web Browser Protections

8 Malware Defenses

9 Limitation and Control of Network Ports, Protocols, and Services

10 Data Recovery Capabilities

11 Secure Configuration for Network Devices, such as Firewalls, Routers and Switches

12 Boundary Defense

13 Data Protection

14 Controlled Access Based on the Need to Know

15 Wireless Access Control

16 Account Monitoring and Control

Organizational

17 Implement a Security Awareness and Training Program

18 Application Software Security

19 Incident Response and Management

20 Penetration Tests and Red Team Exercises

Picture 3 – CIS Controls

Basic Controls include the key directions to ensure the informational security of the state and private organizations:

- inventory and control of authorized and non-authorized hardware assets;
- inventory and control of authorized and non-authorized software assets;
- actions for vulnerabilities management;
- use of administrative privileges;
- secure configurations for mobile devices, laptops, working stations and servers;
- maintenance, monitoring and analysis of audit logs.

Foundational Controls include recommendations essential for use of best practices to ensure the merit and use of advanced cybersecurity technologies:

- email and web browser protection;

- malware protection;
- limitation and control of network ports;
- data recovery capabilities;
- secure configuration for network devices (firewalls, routers, commutators);
- boundary defense;
- data protection;
- controlled access;
- wireless access control;
- accounts control.

Organizational Controls include recommendations for organizational processes and administrative actions related to informational security, in order to increase the awareness of personnel and conduction of penetration testing. Especially:

- personnel awareness control;
- application software control;
- incidents response;
- penetration tests.

Priorities for training of the specialists in higher educational institutions should be defined under the risk-oriented models on the basis of permanent evaluation of current and advanced threats in the state and corporate sectors. Do we have enough financial and material resources to counteract or at least minimize the threats which constantly increase and dynamically changes? And this question has the negative reply. How find the way out? Just exclusively with the continuous risk assessment and sound management of the existent financial and technical resources, according to the adopted policies on informational and cybersecurity.

Considering our country is in need of modern training programs of experts in informational and cybersecurity which can adapt rapidly to the current risks and threats, so the higher educational institutions should develop their own ambitious tasks and develop the basic profiles in form of:

competencies (social and personal, instrumental, general scientific and professional);

production functions (research, design, organization, management, technologic, control, forecasting and technical) and relevant common tasks;

skills which should have the graduates and actually form the basis for their practical work in directions to organize and ensure the informational and cyber security.

Training programs should have the applicable content with the relevant financing (governmental or corporate orders for the relevant designs, and scientific grants) and be interactive – promptly consider the new risks in informational and cyber security.

Conclusions:

1) Modern problems with globalization and high efficiency of advanced IT technologies increase the possibility to implement the current informational and cyber threats and could encourage, as a consequence, the general world collapse.

2) Cyberattacks is an instrument for the speed achievement of required results as in economic, so in political spheres as well.

3) The necessity for all the nations of the globe to secure the informational resources, information and communication technologies and informational and telecommunication systems, as well the protection of own critical infrastructure from modern cyber threats require the engagement of higher educational institutions of Ukraine in processing and solving of emerging problems in sectors of crucial importance and sectors of national economy and defense potential by means of:

bringing of acting system of national standards of information protection in line with modern international requirements;

definition of training strategies to ensure the informational and cyber security – first of all, understanding that informational and cyber security should be based on awareness (intelligence-driven security), second – use of business partnership at the state and at the international level, third – implementation to the training the practical method on execution of comprehensive expertise of IT and informational security infrastructure according to the existent threats;

development of coordinated educational standards on informational (cyber) security at all educational levels;

establishment of the National Research and Development Centre on informational and Cyber Security and entrusting it with task for development and implementation of the new technologies on informational and cyber security in the state, corporate and scientific sectors;

processing of the issues for development in our country of the complex system for training and retraining of informational (cyber) security personnel with the necessary level and qualification according to the current world threats.

Reference

1. Center for Internet Security: [Electronic resource]. – Access mode: https://www.cisecurity.org/cis-controls-version-7-whats-old-whats-new/
2. Center for Internet Security: [Electronic resource]. – Access mode: https://www.cisecurity.org/controls/
3. Information Resistance: [Electronic resource]. – Access mode: http://sprotyv.info/ru/news/kiev/es-utverdil-mery-po-usileniyu-svoey-kiberbezopasnosti
4. World Economic Forum. Reports 2018: [Electronic resource]. – Access mode: www3.weforum.org/docs/WEF_GRR18_Report.pdf
5. UKRINFORM – Davos announced the establishment of the Global Cyber Security Center: [Electronic resource]. – Access mode: https://www.ukrinform.ru/rubric-technology/2389711-v-davose-obavili-o-sozdanii-globalnogo-centra-kiberbezopasnosti.html
6. Euronews - Davos 2018: Global Threats Response: [Electronic resource]. – Access mode: http://ru.euronews.com/2018/01/24/davos-2018-what-are-humanitarian-organisations-bringing-to-the-world-economic
7. US Treasury lost 3 terabytes of data on hacker attack: [Electronic resource]. – Access mode: http://biz.censor.net.ua/n3017228
8. Russia steps up cyber-attacks on UK. – The Sunday Times, February 2017: [Electronic resource]. – Access mode:

http://www.thetimes.co.uk/edition/news/russia-steps-up-cyber-attacks-on-uk-rl262pnlb

9. V.L. Buriachok. Recommendations on development and implementation of “Cybersecurity” training profile in Ukraine / Buriachok V.L., Bogush V.M. / Scientific Journal “Information Security” National Aviation University. - Vol. 20,2 (2014). - P. 126-131
10. Y.V. Borsukovskii. Role and place of the higher educational institutions in development of the informational and cyber security system of Ukraine / Borsukovskii Y.V., Buriachok V.L./ Modern Information Protection. - 2017. - №1. – P. 34-40
11. Qrator Labs defined important trends on Informational Security market: Electronic resource]. – Access mode: https://www.anti-malware.ru/news/2018-03-19-1447/25756
12. 2018 Informational Security Forecasts: [Electronic resource]. – Access mode: https://rvision.pro/blog-posts/prognozy-po-informatsionnoj-bezopasnosti-na-2018-god/

АНОТАЦІЇ / АННОТАЦИИ / ANNOTATION

UA

Борсуковський Ю.В., Борсуковська В.Ю., Бурячок В.Л. Стратегія вищих навчальних закладів України в підготовці фахівців з інформаційної та кібернетичної безпеки

В даній статті проведено детальний аналіз актуального ландшафту кіберзагроз та напрямки забезпечення інформаційної безпеки зі сторони світової спільноти. Наведені категорії CIS Control щодо напрямків пріоритетного забезпечення інформаційної безпеки державних і приватних організацій. Проаналізовані і сформовані рекомендації та вимоги щодо визначення пріоритетів підготовки фахівців у вищих навчальних закладах. Сформульовані базові напрямки залучення вищих навчальних закладів України до опрацювання та вирішення нагальних проблем критично важливих галузей і секторів національної економіки та обороноздатності.

Ключові слова: загрози, ризики, категорії, кібербезпека

RU

Борсуковский Ю.В., Борсуковская В.Ю., Бурячок В.Л. Стратегия высших учебных заведений Украины в подготовке специалистов по информационной и кибернетической безопасности

В данной статье проведен детальный анализ актуального ландшафта киберугроз и направления обеспечения информационной безопасности со стороны мирового сообщества. Приведенные категории CIS Control по направлениям приоритетного обеспечения информационной безопасности государственных и частных организаций. Проанализированы и сформированы рекомендации и требования по определению приоритетов подготовки специалистов в высших учебных заведениях. Сформулированы базовые направления привлечения высших учебных заведений Украины к обработке и решению насущных проблем критически важных отраслей и секторов национальной экономики, а также обороноспособности.

Ключевые слова: угрозы, риски, категории, кибербезопасность

UK

Borsukovskii Y., Borsukovska V., Buriachok V. Strategy of the higher educations of Ukraine in training of experts on informational and cyber security

The article provides the detailed analysis of current landscape of cyber threats and directions to ensure the informational security by the world society. Article presents CIS Controls on informational security for governmental and private organizations. It analyses and provides recommendations and requirements in definition of the priorities for training specialists in higher educational institutions. The article provides the basic directions for engagement of the higher educational institutions of Ukraine for processing and solving of current problems of the sectors of crucial importance and sectors of national economy and defense potential.

Keywords: threats, risks, categories, cybersecurity