Z.E. Kenzhebayeva, G.Zh. Isabayeva, Zh.K. Zhunusova
JSC «Financial Academy»,
janka_tav@mail.ru, gulya_ij@mail.ru, jannahasimova@mail.ru

CYBER SECURITY

Abstract. Cybersecurity today is a serious aspect in the protection of not only personal information, but above all, the activities of banks, enterprises and individuals engaged in or holding funds in the cryptocurrency. The world community is concerned about the growing cyber threat, as information is a valuable asset of any organization, and therefore the creation of cyber security is necessary by creating groups of highly qualified specialists to strengthen national security from external and internal threats. Kazakhstan has also taken steps in the field of information security in the field of information, but the low level of competitiveness of the Republic of Kazakhstan in one of the most promising areas in the IT industry to develop solutions in the field of information security does not allow to counter these threats. Addressing the issue of national security in the field of cyber technologies, the authors see not only the adoption of the best practices of some countries, but also examine the issue of purchasing foreign software.

Keywords: Cybersecurity, national security, cyber technology, threats, cyber defense, information security.

INTRODUCTION

Awareness of growing cyber threats, in both military and civilian areas, led to the decision to create a special group of nearly a hundred experts, who a year later presented recommendations for relative innovations at the national level to prepare for future cyber war threats.

On October 6, 2016, by the Decree of the President of the Republic of Kazakhstan, the Ministry of Defense and Aerospace Industry of the Republic of Kazakhstan was established. One of the main activities of this ministry is the implementation of state policy in the field of information security in the field of information and communications (cyber security). By the same Decree, the Government of the Republic of Kazakhstan is charged with ensuring the creation of the Committee on Information Security, which in fact will now serve as the authorized body (regulator) for the development of state policy in the field of national information security.

MAIN PART

The innovations concerned not only the development of specific technologies, but also the creation of the necessary infrastructure, including the cooperation of industrial and academic circles with national security structures, educational programs within the school system of instruction, the creation of academic centers of excellence, critical national systems and many other projects. [2]

Organizations are actively developing their business relying on IT infrastructure as the foundation of business processes, but do not pay enough attention to IT security. In the first three months of 2017 alone, more than 500 Kazakhstanis were hacked in Kazakhstan.

Sites, including government sites. There was a massive attack on the IT infrastructure of Kazakhstan's financial institutions, which led to the restriction of banks, including disabling Internet banking and e-mail, for several weeks. Today, the most valuable asset of any organization is information, and the basis of all business processes is information and communication technologies. Under these conditions, competently constructed protection of company data is one of the key conditions for ensuring its competitiveness and development. Insufficient security of information can lead to significant consequences for a business, up to its complete stop.

The German government is creating a national cyber security agency. It will be called the Agency for Innovation and Cybersecurity. It is assumed that the agency will monitor the activities of companies engaged in developments in the field of cyber technologies, and, investing in them, get access to innovations before they reach the market.

According to the analysis of the German Defense Ministry, in order to ensure its own security, Germany should invest about 50 million euros in research in this area in the next two years.
In early March 2016, it became known about a major withdrawal of funds by hackers from the accounts of the Central Bank of Bangladesh. Hackers tried to withdraw $951 million from correspondent accounts at the Federal Reserve Bank of New York. Most of the operations were blocked, but $81 million was transferred to accounts in the Philippines. Later it was reported that the reason for the success of hackers could be a vulnerability in the international interbank system of information transfer SWIFT.

In April 2016, hackers acquired the personal data of about 50 million citizens of Turkey and put them in open access. The 6.6 GB file was posted online and contained personal information, including Turkish politicians.

Any resource on the territory of Kazakhstan is controllable: data on its owner, placed on the information resource and actions taken, will not be difficult to collect.

Worldwide, measures are being taken to combat cybercrime. The Netherlands has established a National Cyber Security Center as part of a public-private partnership to increase information sharing and cooperation in the country. Israel provides substantial tax breaks to companies that have their offices in the national cyber park in Beer Sheva as a mechanism to encourage research and development. Russia is developing a remedy in the event of a cyber-crisis. These are just a few examples of the growing maturity of states in specific areas of cyber security.

Russia’s losses from cyber attacks in 2017 amounted to about 600 billion rubles., Prime Minister Dmitry Medvedev said this, speaking at the international forum “Open Innovations - 2018” in Moscow.

Based on the continuation and development of the spirit of the ancient Silk Road, “One Belt and One Road” calls for the development of new mechanisms for regional economic partnerships, stimulating the economic prosperity of the countries involved, strengthening cultural exchanges and ties in all areas between different civilizations, and promoting peace and sustainable development.

Along with the topics on the global challenges facing the SCO countries, the key issues of the digitization of the Silk Road of the 21st century and the new format of organizing international business cooperation, special attention will be paid to the protection of the capital of Kazakhstan, Astana, from cyber threats. Therefore, it was decided that the panel session “Challenges of the digital economy will be the longest. Cybersecurity”.

In this regard, in the framework of the Fundamental Research Projects of the MES RK 1546 / GF2: “The legal framework for combating offenses in the global communication networks”, we considered it necessary to consider the relationship between such concepts as “information security” and “cybersecurity”, as well as “information security "And" cyber defense "in the legislation of the Republic of Kazakhstan.

On the territory of the former Soviet space, to understand cyber security ("cyber security"), as a rule, they use the broader concept of information security, which means the state of protection of the vital interests of an individual, society, state in the information sphere from external and internal threats, ensuring its formation, use and development.

At the same time, in Western democracies, the term “cybersecurity” is used to understand the reliability, stability and inviolability of computer networks, whatever information on them is distributed (with the exception of child pornography and similar criminal content).

Table 1 - 10 Top-countries by share of attacked industrial systems

<table>
<thead>
<tr>
<th>Place on the list</th>
<th>A country</th>
<th>Share of attacked systems,%</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.</td>
<td>Vietnam</td>
<td>66,1</td>
</tr>
<tr>
<td>2.</td>
<td>Algeria</td>
<td>65,7</td>
</tr>
<tr>
<td>3.</td>
<td>Morocco</td>
<td>60,4</td>
</tr>
<tr>
<td>4.</td>
<td>Tunisia</td>
<td>60,2</td>
</tr>
<tr>
<td>5.</td>
<td>Indonesia</td>
<td>55,7</td>
</tr>
<tr>
<td>6.</td>
<td>Bangladesh</td>
<td>54,2</td>
</tr>
<tr>
<td>7.</td>
<td>Kazakhstan</td>
<td>54,1</td>
</tr>
<tr>
<td>8.</td>
<td>Iran</td>
<td>53,9</td>
</tr>
<tr>
<td>9.</td>
<td>China</td>
<td>53,3</td>
</tr>
<tr>
<td>10.</td>
<td>Peru</td>
<td>53,1</td>
</tr>
</tbody>
</table>

Source "Kaspersky Lab"

In general terms, Cybershield quite fully covers cybersecurity issues at the state level; now it is up to practical implementation of the concept. Thus, in general, while positively assessing the emergence of
such a document, some of the experts surveyed expressed concerns about domestic software development and their advantage for government orders. The general meaning of what was said was reduced to “it is good if such protectionist policies give impetus to the development of domestic software, and it is bad if the Kazakhstani product is simply pushed through at tenders, despite its low quality”.

The national legislation of Kazakhstan lacks the concepts of “cyber security” and “cyber defense”, in which we enter the Top - 10 countries subject to cyber-attack, that is, 7th place with an indicator of 54.1%, for example, in the current legislation only the concepts “information security” and “information security”.

The Law of the Republic of Kazakhstan “On Informatization” does not contain as such a definition of the term “information security”, but paragraph 11 of Article 1 of this Law refers to the national operator in the field of informatization, which is a “legal entity created by the decision of the Government of the Republic of Kazakhstan, to which the owner, in the person of the state, is entrusted with the task of integrating and ensuring the security of state information systems and state electronic information resources.”

True domestic developers, who need time and money to develop domestic means of protecting information and other software and hardware products, are at a disadvantage, since it is not possible to provide finished products within the prescribed period under the law on public procurement. Therefore, it is necessary to take certain measures, including legislative, to stimulate domestic start-up companies for the production of products in the field of information protection.

Thus, by keeping the ratio of the studied terms in the legislation of the Republic of Kazakhstan, we can focus only on the terms “information security” and “information protection” that are in the legislation of Kazakhstan, and the terms “cybersecurity” and “cyber defense.”

The lack of conditions for the development of production (development, implementation) of domestic software and hardware information security. The low level of competitiveness of the Republic of Kazakhstan in one of the most promising areas in the IT industry to develop solutions in the field of information security.

However, how to implement a strategic program of import substitution in the absence of the necessary qualified national personnel? In Kazakhstan, there is no concentrated critical mass of scientists in the field of information security, that is, a scientific school in the field of information security is poorly developed. And, as a result, there is a passive training of specialists who become uncompetitive in the field of information security. This leads to another acute problem for Kazakhstan - the lack of a national standard for encryption and, in general, national (civil) cryptography in general.

Training specialists in the field of information security in foreign universities to provide state bodies with qualified personnel is costly and carries a heavy burden for the country’s budget. Therefore, the training of national personnel in this field should be carried out through the qualitative improvement of educational programs in national universities of the Republic of Kazakhstan and the development of a number of incentive measures for domestic scientists and faculty members. It is also necessary to consider the possibility of allocating a certain number of quotas in the framework of the Bolashak program for training personnel on the programs of magistracy, doctoral studies and scientific internships in the field of information security.

CONCLUSION

It is necessary to take into account the current trends in the field of information security - it is quantum cryptography. I note that quantum cryptography is a new trend in the field of information security. Recently, on August 1, China launched the world's first quantum communications satellite, not susceptible to hacking. That is, it would seem that the distant future in the field of information security has in fact already come.

Thus, information security can be expressed in two ways, firstly, it is an organizational element of the public administration system, and secondly, it is an indicator of the effective functioning of public administration. This is due to the fact that the realization of threats indicates the inefficiency of the functioning of the public administration system. In order to support domestic manufacturers, it is necessary to study the issue of legislative regulation of the procurement of foreign software in the field of information security.
REFERENCES

[9] Cybersecurity is a good resource // http://www.goodnewsfinland.ru/arhiv/mesyacev/c703aa4e/c877e38d0/

УДК: 004.942

Ж.Е. Кенжебаева, Г.Ж. Исабаева, Ж.К. Жунусова
АО «Финансовая Академия»

КИБЕРБЕЗОПАСНОСТЬ

Аннотация. Кибербезопасность на сегодняшний день является серьезным аспектом в деле защиты не только личной информации, но и прежде всего, деятельности банков, предприятий и лиц занимающихся или держащие средства в криптовалюте. Мировая общественность обеспокоена растущей кибернетической угрозой, так как ценным активом любой организации является информация, и связано с чем создание кибербезопасности необходимо путем создания групп высококвалифицированных специалистов с целью укрепления национальной безопасности от внешних и внутренних угроз. Казахстан так же предприял шаги в области информационной безопасности в сфере информатизации, однако низкий уровень конкурентно-способности Республики Казахстан в одном из самых перспективных направлений в ИТ-отрасли по разгрому борьбе решений в сфере информационной безопасности не позволяет противостоять данным угрозам. Решение вопроса национальной безопасности в области кибертехнологий, авторы видят не только перепрежения передового опыта некоторых стран, но и изучая вопрос закупа иностранного программного обеспечения.

Ключевые слова: Кибербезопасность, национальная безопасность, кибертехнологии, угрозы, киберзащита, информационная безопасность.

УДК: 004.942

Ж.Е. Кенжебаева, Г.Ж. Исабаева, Ж.К. Жунусова
АК “Кыргыз Академия”

КИБЕРКАУПСИЗДІКГІ

Аннотация. Киберкаунсыздейді бұғін күні жеке акпаратты гана емес, банктердің, жеке тұлғалардың және криптовалюталық акпаратты ұстан үшін кез келген қосылымдардың қызметін деген мақсатта аспақтың төрт түрлі таблица, сондықтан бұл ең кәсіби болып табылады. Ол қосылымының бөлігінің қоғамдықтардың құрылысына қатысты, өйткені ақпаратты қәдімдегі ұлы амалдарының құрылысы ең кәсіби болып табылады. Казақстан ақпаратты сулымдар асырлыққа келсе де, қоғамдық акпаратты қөз көбейткендету қамтамасыз ететін және қоғамға қолданыс үшін қабылдамаға келетін зерттеулер жөнінде ең кәсіби болып табылады. Казахстан Республикасының бекеелгі қабылдауынан қолданыс үшін қолданыс қамтамасыз ететін және қолданыс үшін қолданыс қамтамасыз ететін зерттеулер жөнінде ең кәсіби болып табылады.