**CYBERSECURITY**

**Security risks of information and their classification. Industry of cybersecurity. Cybersecurity and control of the Internet. Malicious applications. Measures and means of information protection. Standards and specifications in information security field. The acts of the Republic of Kazakhstan governing legal relations in the sphere of information security. Digital signature. Encoding.**

**Cybersecurity. Security risks of information and their classification.**

Today we live in the one of the most transformational time in human history, where everything is connected. And this connected information network take an integral part in our daily lives. All organizations, such as governmental, medical, financial, and education institutions, use this network to operate effectively. Everyday all this organizations collect, process, store and share vast amount of digital information. As more digital information is gathered and shared, the protection of this information is becoming even more vital to our national security and economic stability.

Cybersecurity is the effort to protect computers, servers, mobile devices, electronic systems, networks and all data there from malicious attacks. All countries today need cybersecurity professionals to help protect their citizens and infrastructure.

With the development of information and communication technologies and increasing accessibility to the Internet, organizations become vulnerable to various types of threats. Threats come from different sources, like cyber attacks or employee’s activities. All people or organizations who want to protect their data or assets need to know risks that influence to and identify their impact to determine what they need to do to prevent attacks by selecting appropriate countermeasures.

Risks classification is important for organizations, as it is an important step towards implementation of information security. A risk can be caused by internal and external entities.

Internal risks occur when someone has access to the network with either an account on a server or physical access to the network. It can be result of employee action or failure of an organization process.

External risks come from people or organizations outside of a company. They don’t have authorized access to the computer system or network. Natural disasters like earthquakes, floods and fires also belong to external risks. External attacks occur through connected networks, physical intrusion or partner network.

Risk classification is based on information system security can be distinguished into following types:

1. Errors and omissions – is type of security threat that usually caused by human mistakes.

2. Fraud and theft–is type of security threat that can be performed using different modern forms of fraud and theft.

3. Employee sabotage–is type of security threat when person from the company expose information system resources.

4. Loss of physical infrastructure–is type of security threat that can be caused byloss of electricity supply, loss of communications, flood, fire, earthquake, strikes, etc.

5. Hackers–is type of security threat when people on an unauthorized way try to approach and use the system resources.

6. Malware – is type of security threat that encompass different types of computer viruses, Trojan horses, worms, logical bombs, and other form of “unwanted” software.

7. Threats to personal privacy – is type of threat when lots of personal data could be misused in many different ways.

**Cybersecurity and control of the Internet**

Today social networking changes the role of the Internet. In the early days, we could control our online behaviors, and had the ability to be who we chose to be. We could pick and decide which characteristics were shared with others. Nowadays, as the internet began to grow each day it is difficult to control it. Our offline identity is directly connected with our online actions. History of our internet browser, web searches and web pages visits, email and social media activities carry certain indications of our personality.

Your online identity is who you are in cyberspace. It is how you present yourself to others online. And you need to be accurate with personal information online. Your username shouldn’t lead strangers to think you are an easy target for cybercrimes or unwanted attention.

All information about you can be considered to be your data. It includes all pictures and messages that you exchange with your family, friends or collogues. Information such as medical, educational, financial, employment information, can be also used to identity you online. There are a lot of information about us, and there are different laws that protect our privacy and data, but we don’t know where all our data is.

**Malicious applications (Malware)**

Malware is a malicious software that can be used to steal data. It can take the form of executable code, scripts, active content and other software. The code is described as computer viruses, worms, Trojan horses, adware, bot, ransomwareand etc.

*Computer virus*–A virus is a malicious executable code that is attached to other executable files, often legitimate programs.

*Worms* – Worms are malicious code that replicate themselves by independently exploiting vulnerabilities in networks. They usually slow down networks.

*Trojan horses* – A Trojan horse is a malware that carries out malicious operations under the guise of a desired operation.

*Adware*–Adware is a malware that generates online advertisement in the user interface of the software.

*Bot* – Bot is a malware designed to automatically perform action, usually online.

*Ransomware* – Ransomware is malware designed to hold a computer system or the data it contains captive until a payment is made.

*Denial-of-Services (DoS)* attack is a type of network attack. It shut down a network and make it inaccessible to its intended users. There are two general methods of DoS attacks: flooding services or crashing services.

Flooding services – it occurs when the attacked system is overwhelmed by large amounts of traffic that the server is unable to handle.

Crashing services – it occurs when cybercriminals transmit bugs that exploit flaws in the targeted system.

*Distributed Denial-of-Services (DDoS)* attack is similar to DoS attack but originates from multiple, coordinates sources. It occurs when multiple systems organize a synchronized DoS attack to a single target.

*Phishing* is a cybercrime in which a target or targets are contacted by email, telephone or text message by someone. For example an email sent by retail store asking you to click a link to claim a prize. The link may go to a fake site asking for personal information, or it may install a virus.

How you can tell your system is infected with malware? Below some few signs of malware infection:

* Computer is slowing down
* Files are modifies or deleted
* Crashes
* Presence of unknown files, programs or desktop icons
* Running of unknown processes
* Browser errors
* Increasing of internet traffic
* Emails is being sent without your knowledge

**Measures and means of information protection**

To protect information and personal data you need to follow simple important ways:

* Turn your computer’s firewall on. Firewall is a layer of security that designed what traffic is and isn’t allowed to enter your computer on a network. Generally, they let good traffic through, while keeping hackers, malware, and other unsavory traffic out.
* Use antivirus. Antivirus software is designed to scan your computer and delete them. Methods by which viruses spread is through emails – opening the attachment in the email, visiting an infected website, clicking on an executable file, or viewing an infected advertisement.
* Manage your operating system and browser. Hackers are always trying to take advantage of vulnerabilities in your operating systems and your web browsers. And to protect your data you need to update your operating systems, including your web browsers, try to install the latest versions of software.
* Protect all your devices. Your computer devices, whether are PCs, laptops, tablets, smartphones, should be password protected to prevent unauthorized access. Andnever use unique password for all your devices.
* Encrypt your data. Encryption is the process of converting the information form an easily readable and understandable format into form where an unauthorized party cannot read it. There are encryption tools on the market that are to encrypt files, folders and even entire drivers.

The following should be considered when selecting encryption tools:

1. Purpose of encryption e.g. files, emails, and etc.
2. Operational requirements
3. Handling of temporary files
4. Ease of deployment
5. Ease of use
6. Key management and recovery

You can encrypt your data using Encrypting File System (EFS) in all Windows versions, follow next stepts:

1. Select one or more files or folders.
2. Right-click the selected data >Properties.
3. Click Advanced…
4. Select the Encrypt contents to secure data check box.
5. Files and folders that have been encrypted with EFS are displayed in green, as shown in the figure.

Nowadays, popular online services like Google, Facebook, Twitter use two-factor authentication to add an extra layer of security for account logins. Besides the username and password, or personal identification number (PIN) or pattern, two factor authentication requires a second token, such as a:

* Physical object - credit card, ATM card, phone, or fob
* Biometric scan - fingerprint, palm print, as well as facial or voice recognition

Firewall is a network security system that monitors and controls incoming and outgoing network traffic based on predetermined security rules. It can be installed on computer with the purpose of protecting that computer (host-based firewall), or it can be a network device that protects a network of computers and all of the host devices on that network.

Types of firewall:

* Network or packet layer firewall filtering based on network addresses, ports, or protocols
* Application layer firewall filtering based on application, program or services
* Proxy server firewall filtering client-side requests for the connection
* Network address translation firewall involves a large private network using addresses in a private range
* Host-based firewall filtering of ports and system service calls on a single computer operating system

Virtual private network (VPN) is a service that lets you access the web safely and privately by routing your connection through a server and hiding your online actions. This service encrypts your data, and the online destination sees your data as coming from the VPN, not from your computer and your location.

**Standards and specifications in information security field**

Generally speaking a standard, whether it is an accountability standard, a technical standard or an information security standard, it represents a set of requirements that a product or a system must achieve. The need for standards in the field of information security has been recognized over long time, and evolved significantly in recent years. First published the famous Orange Book “Trusted Computer Evaluation Criteria” of the United States Department of Defense. Other important standards of these years include: «Guiding documents of the State Technical Commission of Russian Federation», «The Information Technology Security Evaluation Criteria (ITSEC)», «Standards for Security Categorization of Federal Information and Information Systems», «Canadian Trusted Computer Product Evaluation Criteria».

In recent years, a new generation of standards has emerged in different countries dedicated to the practical issues of managing information security of a company. The firsts are international standards of information security management ISO15408, ISO17799 and etc.

Standards ISO / IEC17799: 2002 is one of the most well-known standards in the field of information security. They consider the following issues of ensuring the information security of organizations and enterprises:

* the need to ensure information security
* basic concepts and definitions of information security
* company information security policy
* classification and management of corporate information resources
* personnel management and information security
* physical security
* administration of information system security
* access management
* security requirements for IS in the case of development, operation and maintenance

Among the various IT security standards that currently exist in Kazakhstan, we should highlight regulatory documents on the criteria for assessing the security of computer equipment and documents regulating information security. These include regulatory documents on cryptographic protection of information processing systems and information systems. Below is a list of some of these standards:

* СТРК 34.026-2006 Protection of Information. Terms and definitions.
* СТРК 34.022-2006 Protection of information. Requirements for the design, installation, commissioning, operation and security of information systems.
* CT PK 34.023-2006 Information technology. Methods for assessing the compliance of information systems with safety requirements.
* CT PK ГОСТ Р 50739-2006 Computing facilities. Protecting information from unauthorized access. General technical requirements
* CT PK ИСО/МЭК 14888-3-2006 Information technology. Methods of information security. Digital signatures with the application. Part 3. Certificate Based Mechanisms

**The acts of the Republic of Kazakhstan governing legal relations in the sphere of information security. Digital signature. Encoding.**

Communication in the messenger, online payments, electronic services – all this becomes part of the daily affairs of a modern person. Digitalization, which has intensively entered the life of Kazakhstanis with the adoption of the state program “Digital Kazakhstan”, creates a new model of the economy, in which not only basic industries and business are digitized, but also the entire life of society.

For example, the eGov.kz e-government portal works to ensure that citizens have quick access to government services. These are services, such as submitting applications, obtaining certificates, licenses, registration and other operations. All this operation can be signed with your digital signature.

Digital signature is type of electronic signature based on public key infrastructure (PKI) standards, allows users to sign documents in compliance with country regulations. Digital signature is often used to implement electronic signature, which includes any electronic data that carries the intent of a signature. In 2003, January 7 Kazakhstan government accepted the law on Electronic document and electronic digital signature.