1 INTRODUCTION TO INFORMATION SECURITY

Information security is related to cyber security in the processes of processing, storage, use, distribution and their final disposal. Nowadays, the Internet contains a huge amount of information of various nature and importance. This includes, for example, information from organisations and companies (production and technical knowledge, financial data, customer information), but also information that an individual publishes about himself or herself through online services and interactions with them. Some of this information is non-public, but a lot of information is publicly published and available.

The current trend is the predominance of digital information processing of organizations and businesses through information and communication technologies (ICT). According to a survey by AirSlate (2024), 75% of organizations are already processing all their documents digitally, or minimizing the use of paper. Digital processing of information has increased the efficiency of its processing, on the negative side is the possible vulnerability of the organization to its theft or destruction. In general, the increasing dependence on information and communication technologies means increased risks for society - the number of incidents such as theft and data leaks, online fraud and the spread of malicious code is clearly increasing. The consequence of data theft/damage may be the loss of reputation and trust of customers, disruption of the organization's activities or public services (e.g. failure of the traffic management system, e-health services, e-government, university information system). Therefore, from the point of view of security, an important factor in the operation of organizations is the reliable functioning of the built information and communication infrastructure, which, due to its existence in virtual cyberspace, often goes beyond the borders of the state.

The Internet is a publicly available worldwide network of interconnected computer networks with continuous mutual communication and a lot of processed information stored in personal computers, laptops, mobile phones, cloud storage, where this information is exposed to possible security threats. ***The security of each computer's stored information is determined by the level of security of the other computer to which it is connected.***

1.1 Definition of information security

In general, safety is a state without danger, i.e. protection from opponents. Information security focuses on the protection of information in any form. There are several definitions of information security, such as:

- ✓ Information security is a set of rules, procedures for the protection ***of information in printed and digital form*** against unauthorized access, use, publication, modification, inspection, recording or destruction.

- ✓ ***The international standard ISO/IEC 27002 (2005)*** defines information security as maintaining ***the confidentiality, integrity and availability of*** information. It's about protecting information from a range of threats to ensure business continuity, minimize business risk, and maximize ROI and business opportunities.
- ✓ ***SANS states*** that information security refers to ***processes and methodologies*** that are designed and implemented ***to protect printed, electronic or any other form of confidential, private and sensitive information and data*** from unauthorized access, use, misuse, disclosure, destruction, alteration or interruption.
- ✓ ***The European Parliament and the Council*** of the EU define the security of network and information systems as the ***ability of network and information systems*** to resist, with a certain degree of confidence, any action that compromises the availability, authenticity, integrity or confidentiality of data stored, transmitted or processed, or related services provided or accessible through those network and information systems.

1.2 Information security model

In terms of the basic definition of information security, the basic model of information security has been defined. The model is based on the characteristics of information that are important for security and their breach is critical. The model is referred to as ***the CIA triad*** or ***CIA triangle*** (Figure 1) and was the first industry standard for mainframe security.

Figure 1 Model of CIA

The model describes three basic characteristics of information:

- ✓ **Confidentiality** means that information ***is not accessible to unauthorized persons or systems***. Confidentiality ensures that only users who have the appropriate rights and authorizations have access to the information (sensitive data and information are only accessible to those who really need it).

- ✓ **Integrity** means that the information ***is in its original form and in its original state, is complete and undisturbed*** (has not been altered, manipulated or damaged). The integrity of information is an essential feature of information systems, because if users cannot verify the "authenticity" of the information, it has no value for them.
- ✓ **Availability** means ***ensuring timely and reliable access to information***, the ability to have information available when it is needed. It allows authorized users/computer systems to access and receive information without hindrance in the desired format and time.

1.3 Information and cyber security

In practice, the term information security is often confused with the term cybersecurity. Although in general both terms refer to information security, their content and "scope" are different.

Information security

- ✓ Information security is a broader category.
- ✓ Information security is a set of rules, procedures for protecting information in printed and digital form against unauthorized access, use, disclosure, modification, inspection, recording or destruction in order to ensure the confidentiality, integrity and availability of information. Information assets are not necessarily in cyberspace.
- ✓ It concerns processes and tools for the protection of sensitive information and information systems.
- ✓ It is a key part of cybersecurity.

Cybersecurity

- ✓ Cybersecurity ***is a subset of*** information security.
- ✓ Cybersecurity is a set of rules, procedures ***for the protection of information in electronic and digital form***, which are found in computers, storage devices and networks (i.e. in cyberspace).
- ✓ ***The goal is to protect cyberspace*** - to protect networks, intranets, devices, servers, information and computer systems and infrastructure from attacks, unauthorized access or damage.

1.4 Information security of the organization

For organizations, information is important for their operation, without the right information, errors in key processes can occur. At present, the electronic form of information processing through computer systems prevails in organizations, where the processing itself provides comprehensive software solutions - an information system and supporting application programs. From the point of view of information security***, an***

organization's information system is a comprehensive set of people, procedures and procedures, technical means (hardware, software, networks) and data that ensure the required functionality and provide information for a defined purpose (Figure 2). These components enable the automatic collection, transfer, storage, transformation, update and presentation of information for the needs of the organization. ***Each IS component also has its own security requirements.***

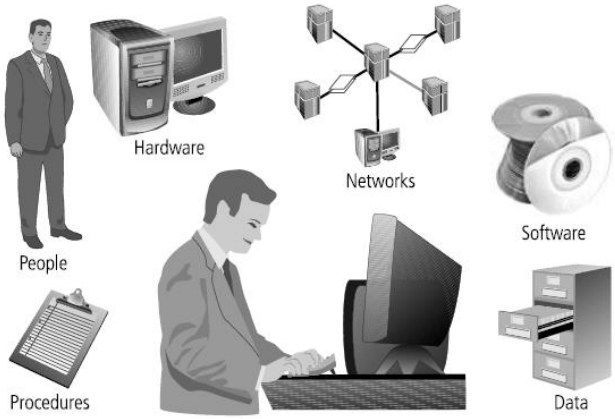

Figure 2 IS Components

1.4.1 Classification of Information Security Components from the Organization's Perspective

The goal of information security of an organization is the protection of information assets processed by the information system at all levels of processing. From the organization's point of view, it is ***a multifaceted system with multiple levels of information security***. The form of information processing is decisive for the classification of individual components - in classic, paper or electronic form. In the traditional, paper-based form of information processing, security is focused on physical security and defining permissions and access for the people who work with it (i.e. procedural and personnel security). In the case of the electronic form of information processing by ICT means, security is extended by additional security requirements: hardware, software, networks and communication channels. According to the above, the components of information security can be defined as follows:

- ✓ ***Physical security*** - protection ***of hardware*** from damage (servers, PCs, mobile phones, network infrastructure, data storage systems: disk arrays, cloud, power supplies, backup power supplies), but in general also the protection of buildings, premises from unauthorized access and misuse.
- ✓ ***Network and communication security*** - protection ***of the computer network and communication infrastructure*** (local computer network and connections to public networks, Wifi network, cabling, other connections and content). By connecting an organization's local computer network to the Internet, its information resources become a potential source of attack.
- ✓ ***Application security*** - software protection (operating systems, application software, system and development tools) is considered to be the most

demanding part of the security of the information system and applications (for the use of errors, weaknesses, holes in software programming).

- ✓ ***Information security*** is focused on the protection ***of information and data*** (documents, databases, system documentation and manuals, archived information, security-related files - files of passwords, IP addresses, e-mail addresses, outputs in paper form). Due to the number and variety of types and formats of information, it requires their classification according to their importance to the organization and defined security procedures.
- ✓ ***Personnel security*** is focused on the protection of ***an individual, a group of authorized persons*** and their access to information resources (business managers, administrative staff, administrators, users). In the literature, people are considered to be the weakest link in information security for various reasons (lack of education in ICT technologies, damage or loss of information, social engineering and manipulation).
- ✓ ***Procedural and operational security*** is focused on ***the procedures*** for the processing and use of information assets. A lack of knowledge of the procedures and procedures used by end-users may lead to a threat to IS. Operational security is focused on protecting the details of a specific activity or series of activities.

An enterprise-level information security management system belongs to the overall corporate governance. The initial written document is ***the Security Policy***, it defines a summary of security requirements and measures for information security at the physical, computer, communication, personnel and administrative levels. From the company's point of view, the security policy should answer the basic questions:

- ✓ What needs to be protected?
- ✓ Why is it necessary to protect it?
- ✓ How are we going to protect it?
- ✓ What to do in case of failure of measures?

In practice, the security policy of the organization of the solution is in the form of internal regulations - directives for individual areas of information security (e.g. the Cyber Security Directive, the Camera System Directive, the Personal Data Protection Directive). The condition is that all employees, users with access to corporate information resources, are familiar with the above documents. It is the duty of the organization to ensure permanent education of employees in the field of information security.

1.5 Digital security

Today's world is characterized by a huge increase in digitalization in all areas of our lives - more and more services and transactions are moving online. Traditional services are transformed into a digital form and "moved" to the online environment. An individual's access to these services requires the creation of a digital identity that is analogous to their physical identity in the real world. Services are becoming more accessible, providing individuals with time- and geographically unlimited access to information and other opportunities for personal development, education, communication and social interaction, collaboration. The disadvantage of an individual's virtual identity is the negative manifestations associated with its possible misuse, manipulation, but also manifestations such as cyberbullying and the loss of direct social communication of people.

1.5.1 Definition of digital security

The term digital security **is associated with the protection of the individual in the digital space**. As this is a new concept in connection with the security of an individual in the online environment, there is no general definition, here are several definitions:

- ✓ Digital security ***is the protection of digital identity and includes a set of best practices and tools used to protect personal data and online identity in the online space.***
- ✓ Digital security refers to ***measures and tools used to protect online identities, data and other digital assets*** from unauthorised access and malicious attacks. It includes a range of procedures aimed at ensuring the security of personal and professional information in the digital space.
- ✓ Digital security refers to protecting an individual's digital devices, data, and privacy from unauthorized access, misuse, and damage.

Knowing the components and components of an individual's digital security means being informed about the potential threats of its breach. Threat prevention and protection of digital identity requires an individual to take a proactive approach to their digital security and to have practical control and use of tools and procedures to secure it. Examples of such tools are: web services, antivirus software, biometric and secure personal devices, password management programs, parental controls, etc. It should be emphasized that this is a permanent process, as we "appear" in the online space through the online services we use, mobile applications on a daily basis. Therefore, educating the end user and taking a proactive approach to protecting their online identity, adopting best practices and practices for securing their online activities is crucial.

1.5.2 Digital security and cybersecurity

In practice, the terms digital security and cybersecurity are often used interchangeably, but they have different scopes and focuses.

Digital security

- ✓ Digital security ***is a narrower category – it focuses on the end user.***
- ✓ ***It is a subset of*** cybersecurity.
- ✓ It is a set of measures, procedures and tools to ***protect an individual's online identity, data and digital assets*** from unauthorised access, misuse in ***order to ensure the protection of their personal information, privacy and online presence***.
- ✓ It refers ***to tools and techniques*** designed ***to protect personal devices and information*** from unauthorized access and malicious attacks.

Cybersecurity

- ✓ Cybersecurity has ***a broader focus and includes the protection of networks, computer systems and the data contained therein***. It includes securing the information and communication infrastructure against a wide range of cyber threats, unauthorized access or data leakage, protection against malware.
- ✓ It uses ***more complex tools and techniques*** that are used ***to protect an organization's information and communication infrastructure*** and ensure the security of data and the systems that store and transmit it.

1.5.3 Digital identity

Digital identities are necessary to ensure people's trust in online service providers and vice versa and their interactions with each other online. These identities are closely linked to the true identity of the individual/organization. There are multiple definitions of digital identity:

- ✓ Digital identity is usually defined as a one-to-one relationship between a person and their digital presence. A digital presence can consist of multiple accounts, credentials, and privileges associated with an individual.
- ✓ Digital identity is ***all digital information that is used to prove an individual's identity online*** and that allows users to interact and transact in the virtual world. This information ***is non-transferable and reusable***.
- ✓ A digital identity ***is an online representation of a person, organization, or entity. It consists of all linked digital data and information***, such as name, email address, social media profiles, and online behavior.

An individual's digital identity contains sensitive/personal information, such as:

- ✓ Personal data (name and surname, date and place of birth, driver's license, occupation, place of work, social security number, e-mail, IP address, medical records).
- ✓ User credentials (logins/profiles, passwords, biometrics).
- ✓ Records of online behavior and interactions (publicly published posts, comments, photos, videos, browsing history, search queries).

This information can be stolen and misused to commit fraud against its owner or to commit fraud on behalf of the owner. There are two basic ways to reveal digital identity information:

- ✓ Knowingly disclosed information is any publicly available/disclosed information by an individual or platform (service) used by them. The User himself, voluntarily and knowingly, provides his/her personal or login data to third parties. Examples are: registering on websites/social networks, filling in online forms and questionnaires, sharing information on social networks, using public Wi-Fi networks, clicking on suspicious links.
- ✓ Unknowingly disclosed information is the result of undesirable activities aimed at unauthorized acquisition of a digital identity (weak passwords, careless behavior on the Internet, social engineering, gullibility, loss/theft of a device).

Examples of digital identity misuse:

- ✓ Identity theft: unauthorized access to personal data, for example to obtain false identity documents, opening fraudulent accounts.
- ✓ Violation of the privacy of an individual: the provision of personal data of the service provider to third parties without the consent of the identity owner, or the leakage of information as a result of a hacker attack (for example, mass theft of the identities of users of social networks, services, applications).
- ✓ Phishing attacks: stealing financial information.
- ✓ Cyberbullying, harassment, intimidation.
- ✓ Monitoring the movement of people using geolocation data of devices (mobile phone, Smart watch).
- ✓ Social engineering: spoofed emails (in the name of an employer, bank) in order to obtain sensitive information or click on malicious links.

1.5.4 Digital Footprint

Many online services and activities typically require verification of an individual's digital identity, but many collect information automatically (often without the individual's knowledge). There is a huge amount ***of publicly available*** personal, work data of individuals/organizations on the Internet. By using online services and their online activities***, an individual creates a digital footprint***. A digital footprint is recorded whenever a user uses an online service or performs any traceable

online activity. Therefore, it plays a significant role in creating a user's online reputation.

Digital Footprint Definitions:

- ✓ A digital footprint is ***a data footprint created by a user's online activities*** and the traces they intentionally or unintentionally leave behind.
- ✓ A digital footprint (also known as a digital shadow) ***is a traceable piece of information and activity*** that a user leaves on the internet.

Characteristics of a digital footprint:

- ✓ A digital footprint is ***a permanent and indelible part of an individual's online existence***.
- ✓ The digital footprint ***grows steadily*** with every online activity of the user or the tracking of the user's activities by websites/applications.
- ✓ It is ***created passively*** through online activities.

Types of Digital Footprint:

- ✓ **Active** (influenceable) - data is knowingly published by the user or is the result of targeted online activities of the user (e.g. conscious use of services, voluntarily published information: blogs, forums, social networks, e-mail, data storage, cloud).
- ✓ **Passive** (uninfluenced) - data is collected without the user's knowledge or consent by automatically used devices or services (e.g. information from a computer system, connection to computer networks and the Internet).

1.5.5 Legislation of the Slovak Republic in the field of information, cyber and digital security

According to experts, the legislation in the field of information, cyber and digital security is not sufficient and does not cover all areas of IT security. Another problem is the constant and rapid development of new IT services, technological solutions, applications and their immediate implementation into practice, which is associated with the growth in the number of users of these solutions. Users often use them without verifying their security aspects of their use (e.g. mobile applications, e-shops, AI-enabled tools, etc.).

Changes in legislative norms, or new legislative norms in recent years, are a response to the society-wide impact of online fraud (e.g. phishing, smishing, deepfake) or manifestations against individuals (cyberbullying). Below are the applicable legislative standards that apply to the field of IT law and information, cyber and digital security.

The basic legal document is the Constitutional Act No. 460/1992 Coll., **the Constitution of the Slovak Republic**, which states:

- ✓ Article 19(3) of the Constitution of the Slovak Republic: Everyone has the right to protection against unjustified interference in private and family life.
- ✓ Article. 22 of the Constitution of the Slovak Republic: The secrecy of letters, the secrecy of transported messages and other documents, and the protection of personal data are guaranteed.

Other legislation:

- ✓ Act No. 40/1964 Civil Code
- ✓ Act No. 513/1991 Commercial Code
- ✓ Act No. 311/2001 Labour Code
- ✓ Act No. 300/2005 Coll. Criminal Code
- ✓ Act No. 301/2005 Coll. Code of Criminal Procedure
- ✓ Act No. 211/2000 on free access to information
- ✓ Act No. 215/2004 on the Protection of Classified Information
- ✓ Act No. 22/2004 on Electronic Commerce
- ✓ Act No. 45/2011 on Critical Infrastructure
- ✓ Act No. 351/2011 on electronic communications
- ✓ Act No. 185/2015 Copyright Act
- ✓ Act No. 214/2008 Amendment to the Act on Electronic Signatures

Laws directly related to information, cyber and digital security:

- ✓ Act No. 18/2018 on the protection of personal data (GDPR Directive)
- ✓ Act No. 69/2018 on Cyber Security
- ✓ Act No. 95/2019 on Information Technologies in Public Administration
- ✓ Act No. 236/2021 on dangerous electronic harassment (cyberbullying)
- ✓ Regulation (EU) 2022/2554 on the digital operational resilience of the financial sector (Digital Operational Resilience Act DORA in force from 17 January 2025)