DOI: 10.33498/louu-2021-11-234

Aytakin Nazim Ibrahimova

PhD in Law, Deputy Dean of Law Faculty
of Baku State University,
Professor at the Department of "Constitutional Law"
of Baku State University
(Baku, Azerbaijan)
ORCHID ID: https://orcid.org/0000-0002-3134-8486
aytakin_ibrahimli@yahoo.com

УДК 342.95

INFORMATION SECURITY AND INFLUENCING FACTORS

Abstract. By listing human needs, Maslow focused first on physiological needs and then security needs. People desire to feel safe in any environment. Consequently, the idea of maintaining a safe environment for people to live more comfortably and securely has been an invaluable reality throughout history. Every state needs laws that will continue to exist and ensure its internal security, and the power that will enforce them. Although it is the duty of states to ensure and maintain security, everyone must be educated about security and fulfil their responsibilities.

The article's purpose is to analyse of the key aspects of information security and influencing factors.

Information security ensures the protection of information from a wide range of threats in order to ensure the speed of work in the organization, reduce possible shortcomings in the work and increase the future return on investment. Information comes in many forms. Information may be stored on paper, in electronic form, delivered by mail or e-mail, or expressed in words between individuals. Information in any form must be protected in an appropriate form.

Keywords: information security; key aspects of information security; factors affecting security; classification of security.

Nowadays, it is important for the public and private sectors to continuously protect information, which is the most valuable asset of human beings, in terms of features such as confidentiality, integrity and accessibility. In addition to a number of physical and systematic measures, protection can be achieved by informing individuals about a number of information security hazards and risks, security policies or regulations, how to combat these threats, and how to minimize existing risks as much as possible. Information security targets to ensure sustainability, minimize losses in the event of unforeseen disasters, and protect the confidentiality, integrity, and accessibility of information in all circumstances.

© Aytakin Nazim Ibrahimova, 2021

Accessibility to information via the Internet in e-government makes government agencies more vulnerable to threats and attacks. For this reason, information security is especially significant issue for states.

The article's purpose is to analyse of the key aspects of information security and influencing factors.

Although the word "safety" means a feeling of trust and attachment without fear, hesitation or doubt, the word "security" means the continuation of law and order in society without violating it, and the situation in which people can live without fear[1].

The word security comes from the Latin word "secures" meaning safe, but the English equivalent of the word is "security". When we study the word security from its etymological perspective, we see that it comes from the root "without care"[2]. From this point of view, it can be concluded that security emerges as the result of insecurity, carelessness and defencelessness. For the human race, security is the ability to and scope within which an individual or a society to live in peace, to be protected against internal and external threats. A society that meets this need and is secure is a safe society, and a person can be called as a reliable person.

Security is one of the most important needs for living beings to live and express their feelings more comfortably since the day they came into being. In an article dated from 1943 and written by a psychologist Abraham Harold Maslow, the theory of the "pyramid of needs"[3] is given and it is stated the needs of certain categories of people and the priorities of those needs. This theory explains that by meeting the needs of living things, they go in search of higher needs, which create a hierarchy among themselves, and that the individual's personal development is determined by the category of needs that prevails at that moment. However, according to this theory, an individual cannot move to a higher level of needs without fully meeting the needs of a given category.

Information is personalized information that allows a person to fully and correctly perceive what is happening around them. Information manifests itself in the form of thinking, foresight, feelings, thoughts, lessons learned, projects implemented, and experiences obtained. Information, like other assets in an organization, is important to the organization and therefore should be best protected.

The role of information security in security management. Information security is considered in a deductive way and holistically. With a holistic approach, we can classify information security for organizations in the following way.

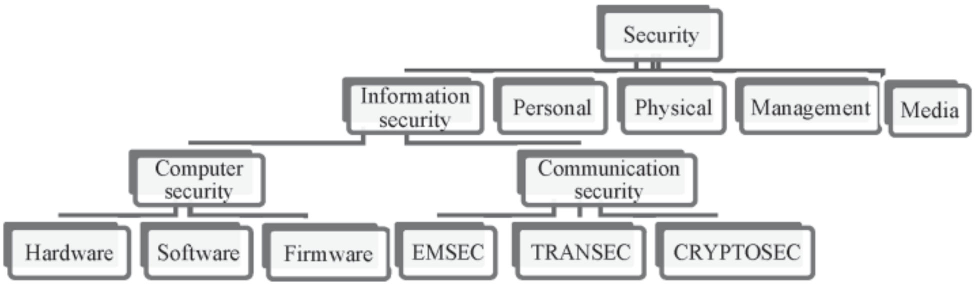
Classification of security areas[4]:

[1] 'Safety' *(Obastan – onlayn lüğətlər və ensiklopediyalar)* <https://obastan.com/axtar/?l=az&q=safety> (accessed: 14.11.2021).

[2] 'Security' *(Online Etymology Dictionary)*<https://www.etymonline.com/word/security#etymonline_v_30368> (accessed: 14.11.2021).

[3] A Maslow, 'A Theory of Human Motivation' (1943) 50 Psychological Review 370–96.

[4] ACO security Directive AD 70-1 SUPREME HEADQUARTERS ALLIED POWERS EUROPE, Belgium, 1 January 1997, Part V Chapter 1.



As in this classification, safety should be considered with all indicators. Security on a computer network most likely falls into the category of computer security (COMPUSEC). However, there is no clear certainty between the classifications. All classifications are interrelated. At the heart of all these relationships is the human factor. Human security is perhaps the most significant issue here.

Nowadays, companies and government agencies engaged in trade are very seriously focused on the use of information in order to continue their work with the increasing use of information and communication technologies. Along with this direction, the importance of information has increased, and it has become an urgent need not only to store and collect it securely, but also to send it from one place to another. This dependence on information has acquired a very important place among the beings possessed by the institution. Attacks on information will result in the destruction, deletion, loss of integrity or confidentiality of information, disruption of the information infrastructure, and disruption of operations.

Information security aims to protect information from unauthorized access, use, emergence, destruction, alteration and damage. Information security ensures the continuity of work in an organization which guarantees that information is protected from large-scale threats in order to reduce the potential for shortcomings in the work and increase future benefits. Information in any form must be adequately protected. Guaranteeing information security is possible by ensuring a sufficient level of confidentiality, integrity and usability of information[5].

Notwithstanding to the information delivery channels – internet, telephone, fax, etc. – that is used for the safe transmission of information electronically between the two parties (for example, the relationship between the person who ordered the document and the person who received the order), it is significant to ensure the security criteria such as listed in the form of confidentiality, integrity, authentication and non-refusal. The meanings of these concepts in information security are: "non-disclosure of the contents of the delivered data

[5] D Önel, A Dinçkan, *Bilgi Güvenliği Yönetim Sistemi Kurulumu* (TÜBİTAK Ulusal Bilgi Güvenliği Kapısı 2007) 12.

to third parties", "ensuring the protection of the data as it is during delivery", "proof of identity of the sender" and "no claim of the sender on the denial of the information sent".

Information security is basically ensured by three means: Confidentiality; Integrity; Availability.

In many sources, information security is represented as the CIA, which is a combination of the initials of these three tools. Other sources add two concepts to these three concepts, which are called accountability and empowerment tools.

Confidentiality. Privacy, which is the most essential part of security, is provided by the encryption of messages during data transmission. Messages sent via electronic data delivery are encrypted and made incomprehensible so that they cannot be detected by others. The user who receives the message decrypts and reads the message using the same algorithm.

Confidentiality can be explained by the fact that the information is closed to unauthorized access. Another definition is that privacy is prohibited from being disclosed by unauthorized persons. Confidentiality is intended to ensure the safe transfer of data from a transmitter, such as a disk, CD, DVD, or via the Internet, to the sender. Attackers can gain unauthorized data in a number of ways, such as stealing a password or a document containing the data, accessing the data, or tracking the user's password.

Confidentiality is a guarantee that information can only be obtained by authorized persons. Privacy refers to the removal of sensitive information within the system[6]. Crypto systems are designed to maintain this dimension of information security. The main reason for the use of encryption today is privacy and integrity. Not every concept of information security is equally important for every organization. Confidentiality is more significant for government agencies and banks[7].

Confidentiality is the protection of the transmitted news or data stored in information and communication systems against the unauthorized access to information transferred by information and communication networks. In particular, the confidentiality of information is needed to ensure the confidentiality of the information conveyed through the delivery of personal information[8].

Confidentiality is used to prevent information from being collected, processed, delivered, or obtained by an organization or any person not authorized by the owner during any process.

Such control mechanisms as encryption, safety interlocking, notification, etc. can be used as an example of ensuring the confidentiality of an entity

[6] M D John Hunter, *An Information Security Handbook* (Springer-Verlag 2001) 12.

[7] E V Ersoy, *Iso/Iec 27001 Bilgi Güvenliği Standardı* (ODTÜ Yayıncılık 2012) 73.

[8] Communication from the Commission to the Council, the European Parliament, the European Economic and Social Committee and the Committee of the Regions – Network and Information Security: Proposal for A European Policy Approach COM/2001/0298 <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex%3A52001DC0298> (accessed: 14.11.2021).

in any format. Confidentiality is defined by the International Organization for Standardization (ISO) as "access to information only by authorized persons". The main purpose of the use of encryption in many information and communication companies today is to ensure the confidentiality of information.

Confidentiality as a key concept is "preventing the disclosure of information by unauthorized persons"[9].

Confidentiality is mandatory for the public or private sector, especially if it is provided for in a law, legal act or standard. For instance, information such as the relationship between a lawyer and a client, or the relationship between a doctor and a patient, is protected by law. In some cases, the parties pass a lot of information to each other in the contract, and in this case, the confidentiality agreement is included in the contract. In both cases, privacy is essential[10].

Another example can be given in the telecommunications sector. In this sector, privacy is also mentioned as the most important concept among information security concepts. Article 2 of the Law of the Republic of Azerbaijan "On Information, Informatization and Protection of Information" under the title "Basic Concepts" defines confidential (confidential) information as the following: documented information, the acquisition, processing, transmission or use of which is restricted in accordance with the legislation of the Azerbaijan Republic[11]. Furthermore, Article 8 states that the rules for the formation and processing of confidential information constituting a state secret are determined by the legislation of the Republic of Azerbaijan. Article 9 stipulates that information that is not a state secret, but must be kept confidential in order to protect the legitimate interests of citizens, departments, enterprises and organizations, may be collected, processed, used and disseminated only in cases specified by the legislation of the Republic of Azerbaijan.

Integrity. The concept of integrity indicates the cases when the information sent has been altered by another user. This is also explained as the integrity of the data. Integrity: ensuring that information sent, received or stored is complete and unaltered. Integrity is especially important for commercial and industrial projects, where medical information is important to ensure identification at the time of contracting, or when the accuracy of the information is crucial[12]. Integrity is ensuring the accuracy and integrity of information and its processing. For instance, the ABC application can only be changed by authorized persons[13]. In the event that an encrypted information is intercepted by another, the attacker will not make changes because the content of the information cannot be clarified. Even if changes are made, it will be

[9] Önel, Dinçkan (n 5) 6.

[10] B Yıldız, 'Bilgi Güvenliği ve E-Devlet Kapsamında Kamu Kurumlarında Bilgi Güvenliği Yönetimi Standartlarının Uygulanması' (Yüksek Lisans Tezi, 2007) 47.

[11] Law of the Republic of Azerbaijan on information, informatization and protection of information April 3, 1998 N 460-1G <https://wipolex.wipo.int/ru/text/490279> (accessed: 14.11.2021).

[12] Network and Information Security: Proposal for A European Policy Approach COM/2001/0298 (n 8).

[13] C Alberts, A Dorofee, *Managing Information Security Risks: The Octave Approach* (Pearson Education Inc. 2004) 102.

understood that the new information will be meaningless and the integrity will be damaged.

This means that the information is guaranteed to be accurate and complete at the place where it is stored and sent. Therefore, that it has been processed correctly and has not been altered in an unauthorized manner.

According to the National Information Assurance, the integrity of data is the protection of data or information against alteration or destruction by unauthorized persons[14]. Integrity is the protection of the content of information against the threat of alteration, deletion or destruction in any way by unauthorized persons. Integrity is, in short, the absence of accidental or intentional violation of integrity of information[15].

Intentional or accidental breaches of the data do not change the existing reality. Those who take security measures must take precautions against both types of risks. The criteria of "Accuracy, Correctness and Reality" must be ensured for the integrity of the information[16].

Integrity control mechanisms and methods are available to ensure that the integrity of incoming data is not compromised in telecommunications systems and other data devices. For instance, control mechanisms that validate input/output data, such as user terms and other controls.

Integrity is also the protection of the content of information against the threat of alteration, deletion or destruction in any form by authorized persons. For the sake of integrity, we can briefly say that it is a random or intentional violation of information. To paraphrase, it is the delivery of information to the recipient in the form in which it came from the sender. In this case, it is transmitting the information to the recipient without alteration of the channels in which the information is flowing, adding up any new information, duplicating neither part nor all pieces of the information sent, changing the sequence of the information sent.

The integrity of the information must meet the following three criteria:

– Determination;
– Accuracy;
– Reliability;

Availability. This means that information is available when it is required. The availability of such information in case of any problem or any problem emerged is a key feature of usability and should be within the user's rights. It is an indicator of how secure the service is. Each government and non-government sector determines the importance of the service and prepares the data for this need. According to the principle of usability, every user must have access to the source of information to which s/he has access. Utility is the guarantee that authorized users have access to information and related resources as needed. A system is considered secure if it can ensure the confidentiality, integrity and

[14] Yıldız (n 10) 26.
[15] Önel, Dinçkan (n 5) 16.
[16] Yıldız (n 10) 97.

accessibility of information. Recently, identification and denial of identity have also been perceived as information security[17].

Accessibility means ensuring that information is available and that services continue to be provided in the event of power outages, natural disasters such as accidents or attacks. This situation is especially vital in the event that deficiencies in communication networks lead to shortages in terms of other serious infrastructure, such as air transportation or energy sources[18]. This means that the information is available or accessible when needed by authorized organizations and individuals. Namely, the probability that a person in need will have the service she/he needs when s/he requires it is called usability, accessibility. This is an indicator of how reliable the service is. Another concept of accessibility is that information is ready to be used whenever needed[19]. One of the key features of accessibility is the availability of such information when there the issue emerges or is likely to be a problem. This access must be within the user's rights. According to the principle of accessibility, every user must be able to access the source of information to which s/he has the right, within his/her authorized time. For this reason, it is important to keep in mind that the organization's security rules prohibit access to data.

As mentioned above, there are additional tools which have impact information security, such as accountability, authorization, authentication, non-denial, commitment, access control, reliability and security.

Accountability. Accountability is a type of personal responsibility. The shortest definition of accountability is that individuals are held accountable for their actions and for what they do not do when they have an obligation to proceed. Such topics as being accountable and liability, which are key concepts of accountability, are at the centre of major debates, Accountability is beginning to be assessed with a little higher value than the other three concepts. The most important concept of accountability in government is transparency. The main requirement is that the actions of the state bodies in accordance with their duties and the decisions they make are clearly explained to the citizen.

Authorization. From the point of view of information security, authorization is a system of authentication. Authorization during access to information is a means of controlling the accessibility of information by the right person. In everyday life, we use unauthorized access to social networks on almost every computer. Each time a password is entered into Microsoft Windows, the answer is sent back to the controller that received the password, which is checked in the Kerberos system. After this stage, when a person wants to access each network, the closed system confirms the identity of the person from the domain server. It is important to pay attention to the issue of authorization, which is the "minimum information" rule applicable in information systems.

[17] C Landwehr, 'Computer Security, Springer-Verlag' [2001] (1) 1 International Journal of Information Security 6.

[18] Network and Information Security: Proposal for A European Policy Approach COM/2001/0298 (n 8).

[19] Yıldız (n 10) 97.

www.pravoua.com.ua

This rule, which is minimal at the beginning, should inform the organization where you work that it is important for anyone to know the minimum amount of information needed to do their job. It is not possible to ensure information security with technical security alone (antivirus programs, encryption, etc.).

Identification. In any network, an authentication tool is used to recognize and validate a user's activity, to determine if the work is actually done by him, and to know what sources the person performing the operation has access to. To simplify, it is proof that the person is the person they claim. This is ensured by entering the user's password into the system[20]. The system compares the entered password with the registered password and verifies the identity of the user. If the entered password coincides with the registered password, the identity is confirmed. Identification is the process of identifying a person by a system after the person has already been registered in the system. Algorithms, sending a confirmation message to a personal phone, e-signatures and certificates are mainly used to eliminate the shortcomings of authentication and take the necessary measures. It is relevant to note here that this confirmatory activity in the electronic environment is more reliable than in real life[21].

It is tool of ensuring that the parties who receive or send an information do not deny that they have received or sent that information. To simplify it, it means that the sender does not deny later that the message was sent or that the recipient received the message. The technical measure against denial is the e-signature[22].

It is essential to ensure that in the system set-up for secure exchange of information in internet the above-mentioned information security is provided, and thus to guarantee that in case of problems and attacks, the information is transmitted to the other party without any damage or interception.

Reliability. It is the ability of a computer, an information or communication system to function in a way that is constantly and accurately adapted to the contract, the needs of the project, and to perform this in a very secure manner, so to ensure that the system handles it.

Security. It pertains to the functional environment of a computer system or program, it includes measures to prevent effects or events that may pose an unwanted potential or direct threat to itself or the environment to which it belongs.

Tracking is basically provided in 5 steps:

1. Identification: this step identifies the person entering the system. It is currently provided with a simple term "Username". It is significant that each user in the system has a username or number that belongs to him/her and identifies or represents him/her.

[20] M Bishop, *Computer Security: Art and Science* (Addison-Wesley Professional 2015) 310.

[21] Ş Sağıroglu, M Alkan, *Her Yönüyle Elektronik _İmza, E-_İmza* (Grafiker Yayınları 2005) 129.

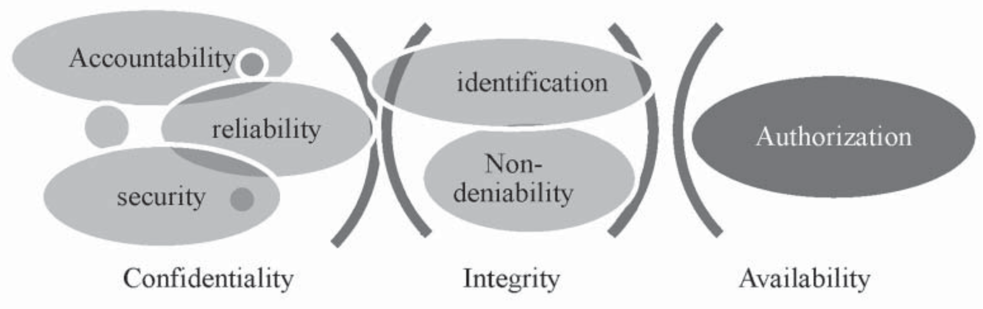
[22] J K Tudor, *Information Security Architecture: An Integrated Approach to Security in the Organization* (CRC Press 2001) 15.

2. Authentication: this step is a step to verify that the user trying to log in to the system is the person who actually logs into the system. In this step, the user trying to log in enters the "password" to the system. If the password and username match, it is confirmed. In other words, it covers the accessibility of authorized users.

3. Authorization: In this phase, after the user is approved by the system, the authority held by that user is delegated to the system and made available to the user. In other words, the service is allowed to be performed, and the applicants are allowed to do only the work and operations that are allowed to them.

4. Auditing (audit, control): This is the stage when all the activities and actions of users who can access the system and work and operate are monitored. This is the stage where the work and operations are checked and registered, such as which user performed which operation, where it entered, what is deleted and which operation is changed. To paraphrase, whether or not related users are allowed to work or operate outside of their authorized business or operations involves tracking issues.

5. Accountability: During this phase, the information obtained in the first 4 stages is collected, interpreted, and the accountability itself emerges. A security application provided in this way only allows the authorized persons to be sure that they have access to the system and to be aware of what the intruders will do. It should be noted that the implementation of all these tools will not ensure 100% information security. As can be seen from the table below, which still maintains its reliability, the lack of one or more of these tools will lead to security failures. It should never be forgotten that these tools are complementary[23].



Conclusion. Information security ensures the protection of information from a wide range of threats in order to ensure the speed of work in the organization, reduce possible shortcomings in the work and increase the future return on investment. Information comes in many forms. Information may be stored on paper, in electronic form, delivered by mail or e-mail, or expressed

[23] Gülnaz Mesut, 'Kamusal Web Güvenliği' (Yüksek Lisans Tezi, 2010) 23, 26.

in words between individuals. Information in any form must be protected in an appropriate form.

Information security is one of the most debated and significant issues in developed and developing countries. Information security is an information technology tool that protects the personal, commercial, professional and state secrets of everyone, regardless of who processes and uses the information.

If we divide the concept of security into classes, there will be two types of organizational approaches. The first of these is a security tool. Information security is naturally part of security management. In addition, information security is being studied within information management. In this regard, there are two directions of information security.

The weakest link in the chain of information security system is a person. The human factor plays a key role in ensuring adequate and sufficient security. A person should be constantly educated on this issue for the security of both the organization s/he works for and his personal information. For this reason, it is necessary to pay more attention to the human factor. In this sense, an entity at all levels must create the required conditions for the employee to understand/grasp his/her responsibilities in the field of information security.

The following problems may arise as a result of potential threats to information security:

– Vital information can be stolen, modified or deleted;

– Forfeiture of work, time and trust can occur due to the failure of the information system;

– Failure of the information system can lead to material and non-material deprivations.

At the heart of all these problems lies responsibility factor. Responsibility is the ability to determine who or what is responsible for a particular action. Typically, a documentation of cases is needed to track records and an account review system that will examine these records. If the systems cannot be tracked, it will not be possible for the actions and activities in the system to be controlled. Therefore, it is useful to first make sure that the system can be tracked, and then bring up the means that ensure its security.

REFERENCES

Bibliography

Authored books

1. Alberts C, Dorofee A, *Managing Information Security Risks: The Octave Approach* (Pearson Education Inc. 2004) (in English).
2. Bishop M, C*omputer Security: Art and Science* (Addison-Wesley Professional 2015) (in English).
3. Ersoy E V, *Iso/Iec 27001 Bilgi Güvenliği Standardı* (ODTÜ Yayıncılık 2012) (in Turkish).
4. Hunter M D John, *An Information Security Handbook* (Springer-Verlag 2001) (in English).

5. Önel D, Dinçkan A, *Bilgi Güvenliği Yönetim Sistemi Kurulumu* (TÜBİTAK Ulusal Bilgi Güvenliği Kapısı 2007) (in Turkish).
6. Sağıroglu Ş, Alkan M, *Her Yönüyle Elektronik _İmza, E-_İmza* (Grafiker Yayınları 2005) (in Azerbaijani).
7. Tudor J K, *Information Security Architecture: An Integrated Approach to Security in the Organization* (CRC Press 2001) (in English).

Journal articles

8. Landwehr C, 'Computer Security, Springer-Verlag' [2001] (1) 1 International Journal of Information Security 6 (in English).
9. Maslow A, 'A Theory of Human Motivation' (1943) 50 Psychological Review 370–96 (in English).

Theses

10. Gülnaz Mesut, 'Kamusal Web Güvenliği' (Yüksek Lisans Tezi, 2010) (in Azerbaijani).
11. Yıldız B, 'Bilgi Güvenliği ve E-Devlet Kapsamında Kamu Kurumlarında Bilgi Güvenliği Yönetimi Standartlarının Uygulanması' (Yüksek Lisans Tezi, 2007) (in Azerbaijani).

Websites

12. 'Safety' *(Obastan – onlayn lüğətlər və ensiklopediyalar)* <https://obastan.com/axtar/?l=az&q=safety> (accessed: 14.11.2021) (in English).
13. 'Security' *(Online Etymology Dictionary)* <https://www.etymonline.com/word/security#etymonline_v_30368> (accessed: 14.11.2021) (in English).

Айтакін Назим Ібрагімова

ІНФОРМАЦІЙНА БЕЗПЕКА ТА ФАКТОРИ ВПЛИВУ

Анотація. Перераховуючи потреби людини, А. Маслоу зосередився спочатку на фізіологічних потребах, а потім на потребах безпеки. Люди прагнуть відчувати себе у безпеці в будь-якому середовищі. Отже, ідея підтримки безпечного середовища, щоб люди жили більш комфортно та безпечно, була неоціненною реальністю протягом усієї історії. Кожній державі потрібні закони, які й надалі існуватимуть і забезпечуватимуть її внутрішню безпеку, та влада, яка їх забезпечуватиме. Незважаючи на те, що держава зобов'язана забезпечувати й підтримувати безпеку, кожен має бути освіченим щодо безпеки та виконувати свої обов'язки.

Метою статті є аналіз ключових аспектів інформаційної безпеки та факторів впливу.

Інформаційна безпека забезпечує захист інформації від широкого спектру загроз з метою забезпечення швидкості роботи в організації, зменшення можливих недоліків у роботі та підвищення майбутньої окупності інвестицій. Інформація надходить у багатьох формах. Інформація може зберігатися на папері, в електронному вигляді, доставлятися поштою чи електронною поштою, а також висловлюватися словами між особами. Інформація у якій би формі вона не була, має бути захищена.

Ключові слова: інформаційна безпека; ключові аспекти інформаційної безпеки; фактори, що впливають на безпеку; класифікація безпеки.