UDC 621.391.1

Palahniuk D.M., *5th year student of the specialty "Telecommunications and radio engineering"*
Bereziuk O.V., *Cand. Sc. (Eng), Associate Professor of the Department of Life Safety and Safety Pedagogics*

BASIC PRINCIPLES OF INFORMATION SECURITY

Vinnytsia National Technical University, Ukraine

In the modern society, the main productive force, the most important strategic resource that ensures its further development, is information. That is why the information, as well as any other resources that need special protection. Next to the term "information security", the term "information security"is widely used. Information security describes the process of creating circumstances that provide the necessary information security, and the achieved state of this level of security reflects information security [1, 2].

Issues of information security have acquired special significance in the modern conditions of widespread use of information automated systems based on the use of computer and telecommunications tools [3-8]. While ensuring information security, threats caused by deliberate (criminal) actions of citizens have become absolutely probable. The first news of unauthorized access to information have been associated, generally, with the hackers ("electronic thieves"). In the last decade, information security violations have been increasing with the use of software tools, as well as with the use of the Internet. Infecting computer systems with computer viruses is also a very common threat to information security.

So, due to the increasing importance of information resources in the life of modern society, as well as the likelihood of numerous threats in terms of their security, information security issues require more and constant attention. The systemic nature of the impact of a large set of different circumstances on information security, which also have a different physical nature, cause different consequences and pursue different goals, lead to the need for a systematic approach to solving this issue.

The relevance of the research is to increase and improve information security and software.

Information security (IB) is a state of the security level of the information environment, and information protection is an activity aimed at preventing leakage of protected information, unintended and unauthorized impacts on protected information, that is, the process aimed at achieving this state [9]. The main goal of implementing an IB of any object is to implement an information security system for this object.

Understanding information security as "the state of the level of protection of the information environment of society, ensuring its formation, development and use in the interests of organizations and citizens", it is legitimate to establish threats to the security of information, their sources, methods of their implementation and goals, other circumstances and actions that violate security. Naturally, it is necessary to consider measures to protect information from criminal actions that cause damage.

Information security threats are understood as possible events or actions that may lead to information security violations. The types of threats to information security are very diverse and have many classifications. For the type of object of influence, threats are divided into threats to information itself, activities to ensure the information security of the object and the object's personnel. After a more detailed consideration of information threats, they can be classified into threats: to confidential information carriers, their location (placement), information exchange systems (transmission channels), as well as information stored in electronic (documented) form on various information carriers.

One of the most common variants of information security principles is shown in figure 1.

Fig. 1. Principles of information security

Therefore, the action of the object's IB threats is aimed at creating probable channels for the leakage of information to be protected, the reasons for its leakage, and directly at the leakage of this information.

When developing the necessary tools, measures, and methods to protect information, a large number of different factors must be taken into account.

Information as an object of protection, in principle, can be presented on various technical media. These carriers can also be even people from the service staff and users. Information can be processed by computer systems, transmitted over communication channels, and displayed by various devices. It may differ in its significance. Objects that are subject to protection and that may contain information are not only computers and communication channels, but also buildings, premises, and the surrounding area. The qualification of hackers, as well as the channels and methods used for unauthorized access to information, may differ significantly.

An example of security application is the protection of files with test questions and answer options by cryptographic algorithms, which are necessary for checking students ' knowledge by computer testing [10-12].

So, the main principles of information security are the following [13]:

- complexity;
- openness of algorithms and security mechanisms;
- systems;
- ease of use of protective measures and tools;
- reasonable sufficiency;
- continuity of protection;
- flexibility of management and application.

All measures to ensure the security of computer systems by methods of implementation are distinguished by:

- moral and ethical;
- legislative (legal);
- hardware-software;

- physical;
- organizational and administrative.

So, in the latest realities, the security of information resources can only be ensured by a comprehensive information security system, which must be planned, continuous, specific, targeted, reliable, and active. The information security system should be based on a set of types of personal security that can carry out its functioning both in everyday situations and in critical situations.

References

1. Черевко О. В. Теоретичні засади поняття інформаційної безпеки та класифікація загроз системі інформаційного захисту / О. В. Черевко // Ефективна економіка [Електронне наукове фахове видання]. – 2014. – № 5. – Режим доступу : http://www.economy.nayka.com.ua/?op=1&z=3304.

2. Палагнюк Д. М. Принципи забезпечення інформаційної безпеки / Д. М. Палагнюк, Д. С. Тищук, О. В. Березюк // Якість і безпека. Сучасні реалії. Матеріали Науково-практичної конференції 14-15 березня 2018 року : збірник тез доповідей. – Вінниця : ВНТУ, 2018. – С. 19-22.

3. Березюк О. В. Безпека життєдіяльності : навчальний посібник / О. В. Березюк, М. С. Лемешев. – Вінниця : ВНТУ, 2011. – 204 с.

4. Березюк О. В. Безпека життєдіяльності : практикум / О. В. Березюк, М. С. Лемешев, І. В. Заюков, С. В. Королевська. – Вінниця : ВНТУ, 2017. – 99 с.

5. Поліщук О. В. Методичні вказівки до самостійної та індивідуальної роботи з дисципліни «Цивільний захист та охорона праці в галузі архітектури та будівництва. Частина 1. Цивільний захист» для спеціальності 192 – «Будівництво та цивільна інженерія» / О. В. Поліщук, М. С. Лемешев, О. В. Березюк. – Вінниця : ВНТУ, 2017. – 37 с.

6. Березюк О. В. Проблеми при викладанні безпеки життєдіяльності в процесі підготовки фахівців радіотехнічного профілю / О. В. Березюк // Педагогіка безпеки. – 2019. – № 2. – С. 104-111. – https://doi.org/10.31649/2524-1079-2019-4-2-104-111.

7. Березюк О. В. Міжпредметні зв’язки у процесі вивчення дисциплін циклу безпеки життєдіяльності майбутніми фахівцями радіотехнічного профілю / О. В. Березюк // Педагогіка безпеки. – 2017. – № 2. – С. 21-26.

8. Березюк О. В. Застосування комп’ютерних технологій під час вивчення студентами дисциплін циклу безпеки життєдіяльності / О. В. Березюк // Педагогіка безпеки : міжнародний науковий журнал. – 2016. – № 1 (1). – С. 6-10.

9. Кавун С. В. Інформаційна безпека : навчальний посібник. Ч.1 / С. В. Кавун, В. В. Носов, О. В. Мажай. – Харків : Вид. ХНЕУ, 2008. – 352 с.

10. Березюк О. В. Комп’ютерна програма для тестової перевірки рівня знань студентів / О. В. Березюк, М. С. Лемешев, І. В. Віштак // Тезиси науково-технічної конференції студентів, магістрів та аспірантів «Інформатика, управління та штучний інтелект», 26-27 листопада 2014 р. – Харків : НТУ «ХПІ», 2014. – С. 7.

11. Березюк О. В. Перспективи тестової комп’ютерної перевірки знань студентів із дисципліни "Безпека життєдіяльності" / О. В. Березюк, М. С. Лемешев, М. А. Томчук // Матеріали дев'ятої міжнародної науково-методичної конференції "Безпека життя і діяльності людини – освіта, наука, практика". – Львів : ЛНУ, 2010. – С. 217-218.

12. Березюк Л. Л. Тестова комп’ютерна перевірка знань студентів із дисципліни «Медична підготовка» / Л. Л. Березюк, О. В. Березюк // Науково-методичні орієнтири професійного розвитку особистості : тези доповідей учасників IV Всеукраїнської науково-методичної конференції, 20.04.2016. – Вінниця : ТОВ «Меркьюрі – Поділля», 2016. – С. 96-98.

13. Аникин И. В. Теория информационной безопасности и методология защиты информации : учебное пособие / И. В. Аникин, В. И. Глова, Л. И. Нейман, А. Н. Нигматуллина. – Казань : Изд-во Казан. гос. техн. ун-та, 2008. – 358 с.