DOI https://doi.org/10.30525/978-9934-26-504-4-12

THE PROBLEM OF FORMING INFORMATION HYGIENE SKILLS IN COMPUTER SCIENCE LESSONS

Semenikhina O. V.

INTRODUCTION

Society today uses a variety of gadgets, computers, and the Internet, opening up new horizons of knowledge and entertainment. However, at the same time, there are specific problems with the safe use of information technologies – such as violation of confidentiality, leakage of personal data, loss of important information, the shutdown of large organizations due to cyber-attacks, and the spread of misinformation, which together can cause a threat to national security. Adequate protection against these information threats is becoming a vital aspect of the development of the information society. It requires joint efforts from state institutions and each citizen in particular. Therefore, the need to comply with information hygiene is actualized, which is particularly important in the context of children's learning outcomes in general secondary education institutions.

Researchers such as A. Berko, O. Boychenko, L. Yevdochenko, B. Kuzmenko, O. Lytvynenko, A. Marushchak, A. Pogrebnyak, and others have delved into the realm of information threats. Their work focuses on developing the theoretical foundations of 'information security,' identifying and categorizing these threats, and laying the groundwork for countermeasures. Other scholars, including S. Alekseeva, O. Malykhin, O. Semenoh, O. Topuzov, and others, have explored the risks associated with digitalization and underscored the critical role of digital literacy in the population. They have also highlighted the importance of fostering digital competence in young people, particularly in media literacy and information hygiene.

The school computer science course should contribute to the development of not only technical skills but also a critical perception of technology. Students should learn to distinguish between true and false information, identify reliable sources, and assess the risks and consequences of uncritical use of technology. Mastering these skills will help young people reduce the likelihood of falling for fraudsters and manipulators online, which, in turn, will have a positive effect on their social adaptation. So, the problem of forming the skills of information hygiene of young people is urgent, and its solution is naturally associated with teaching computer science in general secondary education institutions.

The **purpose** of the study is to characterize the information hygiene skills of young people and to substantiate the possibility of their formation in computer science lessons.

The goal of the study led to the solution of several **tasks**:

1) analyze possible information threats that arise due to the spread of information technologies;

2) analyze the interpretation of information hygiene from the standpoint of scientific and pedagogical research;

3) analyze the current curricula in computer science on the formation of information hygiene skills;

4) to investigate the practical state of awareness of pupils of Sumy secondary schools about the observance of information hygiene.

Methods

We used several research methods to achieve the goal.

Theoretical: analysis and systematization of scientific sources to characterize the state of elaboration of the research problem; terminological analysis to clarify the thesaurus of the study; content analysis to identify classifications of information threats and ways to avoid them; modeling educational content for the development of lessons focused on the formation of information hygiene skills;

Empirical: surveys will be conducted to characterize the current development of the problem of forming students' information hygiene skills in computer science lessons, and teachers and students will be observed in computer science lessons to identify effective methods and means of forming students' information hygiene skills.

This research was a local project, and it was studied as a separate result of the project "Specialist's Professional Development in a Digital Educational Environment" (0120U100572), which involved master's students of the Department of Informatics of Sumy State Pedagogical University named after A. S. Makarenko.

1. Information Threats as a Consequence of the Development of IT

Information technology has become a component of modern life, providing convenience, accessibility, and speed in information exchange. However, new information security challenges have emerged along with the growing role of the digital environment. Information threats are reaching a new level of development, threatening the successful development of society and each person in particular. Today, they are directly connected with access to the Internet, Internet technologies, and social networks, the primary corporate and interpersonal communication tools.

The concept of "threat" is interpreted differently in different situations. Threats are any situations and events in the external environment that can

lead to a dangerous event under appropriate conditions. In other words, threats are potentially adverse impacts. For example, an open organization may not have a privacy risk because all information is considered public (media). However, in most cases, access to private information is a danger.

Information threats (security threat) – threats of theft, alteration, or destruction of information[1], any action or event that may result in a breach of confidentiality, integrity, or availability of information. There are many different types of information threats. They can be accidental or intentional, and various factors, such as human error, technical issues, and criminal activity, can cause them.

According to the methods of influencing the objects of information security, threats are subject to the following classifications: informational, software, physical, radio-electronic, and organizational-legal[2]. Information threats include:

- Unauthorized access to information resources.
- Illegal copying of data in information systems.
- Theft of information from libraries, archives, banks, and databases.
- Violation of information processing technology.
- Unlawful collection and use of information.

Software threats include exploitation of bugs and vulnerabilities in software, computer viruses and malware, and Setting program bookmarks. Physical threats include:

- The destruction or destruction of information processing and communication facilities
- Theft of data carriers
- Theft of software or hardware keys and cryptographic data protection tools

Radio-electronic threats include introducing electronic information interception devices into technical means and premises, interception, decryption, substitution, and destruction of information in communication channels. Organizational and legal threats include procurement of imperfect or outdated information technologies and informatization tools, violation of the law's requirements, and delay in making the necessary regulatory and legal decisions in the information sphere.

According to information security, which information threats are aimed at, the following threats are distinguished[3]:

[1] Platonenko A.V. Modern threats of information security for public and private institutions of Ukraine. *Modern information protection*. 2015. № 4. pp. 86–90.

[2] Bekhter L. A. Threats to information security and information protection as a component of economic security of agricultural enterprises. *Agrosvit*. 2020. № 12. pp. 66–70

[3] Bodnar I. R. Information Security as the Basis of National Security. *Mechanism of Economic Regulation*, 2014, No. 1. P. 68-75.

Confidentiality threats (unauthorized access to information) occur when information becomes known to someone who does not have the authority to access it. Such threats can arise due to the "human factor" (for example, an accidental delegation of one or another user to the privileges of another user) or software and hardware failures.

Integrity threats (unlawful alteration of data) are related to the likelihood of modifying particular information stored in an information system. Violation of integrity can be caused by various factors, from deliberate personnel actions to equipment failure.

Accessibility threats (actions that make it impossible or difficult to access the information system's resources) are the creation of conditions under which access to a service or information will be either blocked or possible for a time that will not ensure the fulfillment of specific goals.

Among the most common information threats, the following deliberate threats are distinguished.

Distribution of malware. Malware is software designed to harm a computer or network. It can steal personal information, destroy files, or disrupt your computer.

Hacker attack: Trying to gain unauthorized access to your computer or network. Hackers can use various methods, such as password cracking, malware, or social engineering.

Malicious behavior is any action that violates an organization's privacy or security policies. Employees, customers, or other third parties can perpetrate malicious behavior.

Technical issues. Technical problems can also lead to a breach of confidentiality, integrity, or availability of information. For example, a data center disaster can lead to data loss, and a software bug can lead to a privacy breach.

We detail the elements of individual deliberate information threats[4].

Espionage, or cyber espionage, is a type of threat that involves unauthorized access to information to carry out espionage operations. Information extraction occurs when an attacker is faced with conditions that prevent theft from being committed or intends to commit theft of information within the organization. Cyber spies can access restricted information, secrets, essential company data, and other sensitive information.

Theft of equipment or information. Computers and storage devices tend to shrink in size and increase power (e.g., laptops, PDAs, smartphones,

[4] Shemchuk V.V. Information Security and Information Defense in the Context of the Development of Domestic Doctrine and Legislative Framework. *Theory and History of State and Law; History of Political and Legal Doctrines. Scientific Notes of V.I. Vernadsky TNU. Series: Legal Sciences*, 2019. Vol. 30 (69) No. 4. P. 29-37.

digital cameras, chips, etc.). It has led to the device being easy to steal. Human error caused by being too careless with things can lead to theft/loss of an electronic device. The cost of losing electronic devices includes:

The loss of essential data.

Loss of intellectual property.

Replacement of new equipment.

Loss of overall performance.

A software attack. The circulation of various software is growing. Taking advantage of this, attackers use malware to infect as many computers as possible worldwide. Viruses and malware are program codes that can infect computers and other devices by spreading through file systems, email, social networks, etc. They can harm the system, steal data, destroy files, or monitor other computers and their activities.

Cyberterrorism. Such an information threat refers to malicious actions committed by an attacker to use a computer system, primarily via the Internet, to cause physical and intellectual damage[5]. These actions are usually designed to attack critical infrastructure.

Phishing is an attack method that uses social engineering to obtain sensitive information from users. That typically involves sending emails or messages that appear to be legitimate information from businesses, banks, or other organizations and asking users to provide their details, such as passwords, credit card numbers, etc.

Kinks are unauthorized access to a system, network, or program to gain control over it or perform destructive actions. Crackers can use various methods, including fixing vulnerabilities and stealing passwords.

The global Internet, intranet (local network), email, and portable media are how information threats of various types are spread.

Information threats can affect the development of the information society at various levels. They require careful consideration and countermeasures, from economic damage and data privacy loss to national security threats. Adequate protection against information threats is becoming a vital aspect of the development of the information society, which requires joint efforts of individuals, organizations, and states.

Developing counteraction strategies and using appropriate means to combat information threats effectively is necessary. That may include more than just using modern antivirus programs and firewalls. A separate counteraction method can be observing information hygiene by each member of society.

[5] Koterlin I. B. Information Security in the Conditions of Martial Law in the Aspect of Ensuring Information Rights and Freedoms. *Actual Problems of Domestic Jurisprudence*. No. 1. 2022. C. 150-155.

2. Information hygiene in the results of scientific and pedagogical research

The term "information hygiene" came into use due to the development of information technology and almost unlimited access of people to various types of information. An adequate response to all news and events, verification of the accuracy of the information, and compliance with simple digital security rules are the keys to successful information hygiene. In the context of constant robust information flows, the observance of information hygiene makes it possible to protect a person from manipulating information and its consequences.

The problem of information hygiene in society began to be actively discussed at the beginning of the 21st century. Such concepts as the following have appeared:

– Information hygiene is "the prevention and preservation of human health, determination of information life priorities, and preservation of one's own time as the most valuable resource of[6];

– Infomedia literacy as "a set of skills to work correctly with Internet sources"[7], media literacy as the ability to work carefully with Internet sources[8] and features of their formation[9];

– ability to resist information influences[10];

– information and digital literacy and information and digital culture[11].

Scientific research on the impact of information on society in Ukraine and European countries has become the most actual. There are publications in which the information hygiene of Ukrainian online media is characterized; various aspects of combating disinformation in the news and media are

[6] Khalamendyk V. B. Information hygiene as a factor of preservation of human mental health. *Humanitarian Bulletin of Zaporizhzhya State Engineering Academy*, 2008. No 35. P. 83-91.

[7] Drushliak M. G., Semenoh O. M., Grona N. V., Ponomarenko N. P., Semenikhina O. V. Typology of Internet resources for the development of infomedia literacy of youth. *Information Technologies and Teaching Tools*, 2022. No. 88(2). P. 1-22. https://doi.org/10.33407/itlt.v88i2.4786.

[8] Rudenko Y., Ahadzhanova S., Ahadzhanov-Honsales K., Bieliaieva O., Korovai A., Semenikhina O. Effective Educational Ukrainian Practices of the Formation of Media Literacy, 2023 *46th MIPRO ICT and Electronics Convention (MIPRO)*, Opatija, Croatia, 2023, pp. 654-659. https://doi.org/10.23919/MIPRO57284.2023.10159822.

[9] Semenog O., Semenikhina O., Oleshko P., Prima R., Varava O., Pykaliuk R. Formation of Media Educational Skills of a Future Teacher in the Professional Training. *Revista Românească pentru Educaţie Multidimensională*, 2020. Vol. 12. Is. 3. p. 219-245. https://doi.org/10.18662/rrem/12.3/319.

[10] Rudenko Y. O., Drushliak M. G., Shamonya V. G., Ostroha M. M., Semenikhina O. V. Development of the ability of student youth to resist information influences. *Information technologies and teaching tools*. 2023. №94(2). Pp. 54–71. https://doi.org/10.33407/itlt.v94i2.5162.

[11] Lazorenko S. A., Semenikhina O. V. Current state of the problem of formation of information and digital culture of future specialists in physical culture and sports. *Bulletin of Cherkasy Bohdan Khmelnytsky National University*, 2020. No 4. P. 42-47.

considered, and the attention is focused on the harmful effects of disinformation and measures against its spread[12].

Different approaches to interpreting information hygiene are. Information hygiene is a set of measures and rules to ensure the rational, safe, and effective use of information technologies and resources. The essence of this concept is to prevent possible negative consequences arising from uncontrolled information consumption.

Also, information hygiene is a branch of knowledge that studies the patterns of influence of information flows that come to people on the human body and public health[13].

Information hygiene aims to prevent information from negatively impacting the mental, physical, and social well-being of individuals, social groups, and entire populations, prevent information-related diseases, and improve the environment[14]. The tasks of information hygiene are:

– The development of the principles of ecological and hygienic information behavior.

– Scientific demonstration of sanitary measures for organizing information networks and information processes.

– Production, distribution, consumption, storage, and reproduction of hygienically sound information.

– Scientific demonstration of hygienic standards for information.

– Information environment, information networks, and information processes.

– Information hygiene is an interdisciplinary science field with the right to independent development.

Information hygiene studies the regularities of the influence of information on a person's mental, physical, and social well-being, working capacity, life expectancy, and public health of society. It develops standards and measures to improve the environmental information environment and optimize intellectual activity. Information hygiene is an interdisciplinary science intersection of hygiene, physiology, biology, biochemistry, mathematics, physics, computer science, psychology, information security, conflict studies, and other sciences. It has the right to develop and complicate both in terms of the methods of scientific research and the areas

[12] Loukas G., Murugesan S., Andriole S. J. Information Hygiene: The Fight Against the Misinformation "Infodemic". *IT Professional*, 2022. Is. 24(2). pp. 16-18. https://doi.org/10.1109/MITP.2022.3163007.

[13] Gelyukh M. *Information hygiene: why it is needed and how not to become victims of fakes*, 2020. URL: https://ua.news/ua/technologies/informatsionnaya-gigiena-zachem-nuzhna-i-kak-ne-stat-zhertvami-fejkov.

[14] Khalamendyk V. B. Information hygiene as a factor of preserving human mental health. *Humanitarian Bulletin of Zaporizhzhya State Engineering Academy*, 2008. No 35. P. 83-91.

of application and implementation of the knowledge system. In this regard, the following main tasks can be distinguished[15]:

– study of the characteristics and regularities of information carriers, processes, and flows, perception, processing, storage, and production of new information; the dependence of individual and public health on information;

– determination of hygienic standards of information, information environment, information networks, and processes; scientific substantiation of hygienic information behavior;

– development of sanitary measures for the organization of information networks and processes, hygienically justified production, distribution, consumption, storage, and reproduction of information;

– Development of measures to optimize information and intellectual activities.

The objects of information hygiene include information, information environment, patterns of information processes, a person, social groups, the population as a whole, health disorders associated with information, morbidity, mortality of the population, and preventive measures to improve the environmental information environment[16].

It is necessary to list some *principles of information hygiene*: comprehensiveness, purposefulness, socio-political activity, scientificity, accessibility, integrity, consistency, qualitative and quantitative approach in the analysis of the data obtained, consistency, differentiated and individual approach, continuity of protection, ease of application of protective methods and means, reasonable sufficiency, the flexibility of management and application, the openness of algorithms and protection mechanisms, the validity of access, personal responsibility and others[17].

So, information hygiene is a branch of knowledge that studies the patterns of influence of information flows that come to people on the human body and public health. The development of the information society involves observing information hygiene to prevent the negative impact of information load from sources on the population's health, especially children. The formation of information hygiene skills among young people is necessary to develop a harmonious personality capable of functioning confidently in the digital world.

Information threats can seriously affect society's and the information space's development. Knowledge about them can involve using information

[15] Denisov E.I., Eremin A.L., Sivochalova O.V., Kurierov N.M. Information hygiene and regulation of information for vulnerable groups of the population. Hygiene and Sanitation, 2014. No5. P.43-49.

[16] *The World Health Report 2001* – Mental Health: New Understanding, New Hope. Geneva: WHO; 2001. URL: http://www.who.int/publications/list/whr01/ru.

[17] Demianenko V.M. Information hygiene in the era of "Post-Truth". *Young Scientist*, 2017. No 9.1 (49.1). P. 46-50.

technology and observing information hygiene in general. Therefore, we will describe the knowledge, ideas, and skills necessary for information hygiene below.

Insights into data privacy. One of the most severe consequences of information threats is the loss of data confidentiality. It can lead to the leakage of personal information, financial data, and commercial and scientific secrets[18]. Loss of privacy can lead to blackmail, identity theft, and other negative consequences for individuals and organizations.

Insights into data integrity. Information threats can also lead to the loss of data integrity, which means misrepresenting, modifying, or destroying information. It can have severe implications for the accuracy of decisions based on this data. Loss of integrity can also lead to psychological pressure and mistrust in the information environment.

Insights into information attacks. Information attacks, such as cyberattacks or virus attacks, can cause organizations to shut down. It can seriously affect the organization's business processes, financial situation, and reputation. Losses associated with the shutdown of activities can be significant and require time and resources to resume normal operations. Information threats can also become a threat to national security. Cyberattacks on critical infrastructure, communications systems, defense systems, and other necessary facilities can seriously affect a country's stability and security. Those attacks can be used for destabilization, espionage, and other criminal purposes.

Knowledge of ways to avoid or eliminate information threats. Some of the measures that organizations can take to protect information include[19]:

- use of strong passwords and multi-factor authentication;
- use of anti-virus software and other anti-malware tools;
- information security training;
- use of secure practices for storing and processing information;
- Regular data backups.

Knowledge of the rules for choosing sources of information. Information hygiene includes the right choice of sources of information. Inaccurate, distorted, or fake information can lead to poor decisions and negative

[18] Shemchuk V.V. Information Security and Information Defense in the Context of the Development of Domestic Doctrine and Legislative Framework. Theory and History of State and Law; History of Political and Legal Doctrines. *Scientific Notes of Vernadsky TNU. Series: Juridical Sciences*, 2019. Vol. 30 (69) No. 4. P. 29-37.

[19] Yanovsky A. O. Emotional and motivational content of the process of forming a culture of safe use of the information environment in future teachers. *Scientific Bulletin of the South Ukrainian National Pedagogical University named after K. D. Ushynsky*, 2019. Issue 4 (129). P. 7-12.

consequences. It is essential to use trusted sources to verify the information before sharing it with others[20].

Information hygiene is essential for anyone who uses computers, networks, and other information technologies. Let's describe the most common information hygiene skills.

Password protection. Passwords are the key to your information, so using strong passwords and keeping them safe is essential.

Malware protection. Malware, viruses, Trojan horses, and adware can damage your information. It's important to use antivirus software and keep it up to date.

Safe use of the Internet. The Internet is a significant resource, but it can also be dangerous. It is essential to be cautious when using the Internet and not to disclose personal information to strangers.

Protection against social engineering. Social engineering is a type of fraud in which criminals use human behavior to obtain information or access computers. It is essential to be careful when communicating with strangers online and not to give them personal information.

Regular data backups. Regularly backing up your data is one of the best ways to protect your information from being lost. Storing your backups in a secure location, such as an external drive or cloud, is essential.

Information hygiene can be considered a set of practices for safely using information technology[21]. Information hygiene skills are an essential component of educational outcomes for young people. It includes various aspects – from the correct mode of working at the computer to the critical assessment of information and the ability to protect your data on the network. Let's dwell on this in more detail.

1. Critical evaluation of information is an integral aspect of information hygiene. In the digital age, we are surrounded by much information, but only some are reliable and useful. Developing students' skills in recognizing excessive informational/emotional load and identifying reliable information sources is essential. Popular science articles, statistics, and official documents are reliable sources. In addition, it is necessary to recognize fake news and manipulation. It helps to maintain intellectual independence and avoid the spread of inaccurate information. The ability to critically evaluate information is essential for forming a personal criterion of truthfulness. Not only does this help improve learning outcomes, but it also makes students less vulnerable to manipulation and misinformation.

[20] Demianenko V.M. Information Hygiene in the Era of "Post-Truth". *Young Scientist*, 2017. No 9.1 (49.1). P. 46-50.

[21] Demchenko, P. *Cybernetic Security as the Newest Direction of the Information Component of National Security of Ukraine: Constitutional and Legal Aspect*. URL: http://publications.lnu.edu.ua/bulletins/
index.php/law/article/view/9560.

2. Ability to see information noise. Based on the results of the Internet content analysis, we have identified possible sources of information noise: network advertising (media, contextual, contextual, etc.), Spam (e-mail, comments, private messages, and otherwise), search engine optimization results (SEO—white, gray, and black optimization), repost and rewrite, etc.

Network advertising appeared at the first stage of the Internet's development and quickly spread after the advent of Web 2.0 technologies. Display advertising is one of the first types of network advertising, similar to advertising in print media and with a specific manipulative message[22]. Display advertising considers the site's target audience so it can partially satisfy users' needs. Taking into account modern algorithms that "respond" to the user's search queries and the type of content he consumes, we should talk about contextual advertising – it is either issued by the user's queries in the search engine or with a rigid connection with the words on the page, or concerning his profile in a social network. Geo-contextual advertising is tied to the user's location and is often provided according to their location. Network advertising generally interferes with the consumption of information and other goods on the network even though it seems synchronized with the user's needs.

Spam refers to "unsolicited commercial emails used to engage email address owners in marketing. These mass mailings are sent to recipients by email and are highly profitable to the sender since you can appeal to a large audience[23]. When it first appeared, email spam caused significant irritation among users. Still, in the early noughties, mail services found tools to combat spam, and users' consumer practices were transformed towards those mail services that provided more effective protection against spam mailings (in particular, mail gmail.com is considered such). Today, almost all email services offer protection against spam, but this does not mean it has disappeared.

Search engine optimization, rewriting, and reposting as a type of information noise cause the most negative reactions from users. Search results optimization is done to raise the site's position in the search engine results for specific queries. "Raising" one site in the search results "bypasses" other sites that are perhaps more relevant to the search. Optimization can be white, gray, or black:

White involves promoting the site using permitted methods (e.g., a well-organized site structure, mailing press releases, reviews with a link to the site, and participation in affiliate programs for link exchange).

[22] Muzhanova T.M. Internet censorship as a threat to citizens' rights in the field of information security. *Modern Information Protection* No. 2, 2015. P. 84-88.

[23] Koterlin I. B. Information Security in the Conditions of Martial Law in the Aspect of Ensuring Information Rights and Freedoms. *Actual Problems of Domestic Jurisprudence* No. 1. 2022. C. 150-155

Gray involves using many identical words (often query keywords, in the results of which it is necessary to promote the site).

With black optimization, SEO specialists create third-party sites, pages, and links that are only necessary to increase the citation of the promoted site.

After search bots started indexing blogs, it became possible to optimize search results for blogs and wind up the number of links to the journal to bring it to the top of the search engine rankings.

A rewrite is a compilation of a unique text based on other network texts; therefore, it does not carry anything new. Reposting is copying (without changes or with minor modifications) the content of other sites with unique materials, often violating copyright. As a result, a search query may return many identical messages, making it challenging to consume information[24].

Deviant communications (flood, flame, holy war, trolling, selfiing, etc.) should also be attributed to information noise. Communication in the network is not emotionally neutral and, like any human communication, is focused on making the consumption of information and other goods on the network comfortable. Behavior in places of multi-user network communication is often information noise, which includes Flooding, which is the placement of the same type of and, at the same time, useless information on several discussion platforms; Flame is a "dispute for the sake of argument" that is often no longer relevant to the root cause of the dispute; Holywar is an argument over a question that does not have one correct answer in advance; trolling is the posting of provocative messages; Elfing is a subtype of trolling when provocative messages are disguised as positive feedback about one or more participants in the discussion. Often, such deviant communications are not perceived by users as information noise, although such communications do not carry any meaningful load.

The sources of information noise are described above, but some of its parameters should be given, on which its impact on consumers of information in the network depends:

– message length (due to the increase in the amount of information coming to Internet users, with the emergence of new media culture, consumer practices have shifted towards shorter messages; clip thinking and a decrease in the ability to perceive significant texts have become decisive for consumers of information);

– frequency of messages (advertisers know that three meetings with an advertising message are enough to remember it, and a higher number of appearances causes rejection);

– Design messages (pictures, highlights, CAPSLOCK, melodies, etc.). Design elements that irritate the organs of perception can influence

[24] Vovk V. M. Fakes as a Threat to National Security in the Context of Hybrid War. *Philosophical and Methodological Problems of Law*, 2022. № 2 (24). C. 80-85.

consumer practices to reduce the time of information consumption or completely abandon it. If earlier in society, a bright wrapper was an integral part of consumption, now the situation is changing;

– "sounding" the message. A beautifully and brightly written text or a skillfully created illustration is of an advertising nature, but they are less noisy than the impact of information noise due to "sound." A pattern of thinking characterizes consumer society, so going beyond patterns gives more advantages in the eyes of consumers;

– The recipient of the message. For some, any message is noise; for others, it is a helpful thought. Due to the redundancy of information in the consumer society, consumers have a stronger tendency to evaluate everything subjectively – if earlier the standard of behavior was to read a book on their own and form their own opinion, now there is no time to read everything. Therefore, recommendations, ratings, tops, and selections of valuable links from authoritative users are significant.

1. Protecting personal data is a crucial aspect of information hygiene. In the digital age, when a lot of information is stored and processed electronically, it is essential to ensure your data's confidentiality. You should pay attention to privacy settings on social networks, set strong passwords, and avoid sharing personal data on unreliable resources. That helps to reduce the risk of owners' data being used for criminal purposes. Understanding the importance of protecting personal data and communicating ethically online is also essential for learning outcomes. Knowing how to protect your data from unauthorized access helps you avoid the risk of cyberattacks and privacy breaches. In addition, the culture of ethical communication is essential for building positive interpersonal relationships and contributes to improving students' social adaptation.

2. Ethics and culture of communication. Ethics and communication culture are becoming increasingly important in a digital society. Virtual space provides quick and convenient communication opportunities, but it can also become an arena for conflicts and miscommunication. Information hygiene supports a communication culture in which it is essential to observe politeness, respect for the interlocutor, and avoid rudeness and offensive statements. A culture of virtual communication also includes the ability to express one's thoughts constructively, listen to others, and have informed discussions. Thoughtless expressions, insults, and even digital conflicts can negatively affect the psychological state of children and cause disorientation in the study of academic subjects. It is essential to teach children the ethical aspects of virtual communication promptly, to cultivate respect for the opinions and differences of others, and to develop positive interaction skills. The culture of communication also includes the rules for the use of linguistic

means and the creation of content that corresponds to the norms and values of society.

3. Analysis of computer science curriculato forming information hygiene skills

In today's rapidly evolving information society, where technology is becoming an integral part of everyday life, it is crucial to implement educational approaches that contribute not only to the acquisition of academic knowledge but also to the development of competencies for the safe and effective use of information technology. One key aspect in this context is forming information hygiene skills among students.

Educators hold a pivotal role in shaping students' approaches to technology during their schooling years. Information hygiene is of utmost importance in the educational process. By incorporating this paradigm into computer science courses, we can actively contribute to the formation of students' understanding of information hygiene[25],[26],[27]. We will analyze current curriculums for developing skills to comply with information hygiene.

We consider a model curriculum for secondary schools in "Computer Science" (grades 5-6). This program is relevant for students who moved to the 5th grade in 2022 and study according to the New Ukrainian School (NUS) concept.

According to the model program, while studying computer science, students develop several cross-cutting skills, among which we highlight:

– read with comprehension, which implies the ability to emotional, intellectual, and aesthetic perception and comprehension of what has been read, understanding of information recorded (transmitted) in various ways or reproduced by technical devices, which includes, in particular, the ability to identify hidden and obvious information, make assumptions, prove the reliability of arguments, supporting one's conclusions with facts and quotes from the text, express ideas related to understanding the text after its analysis and selection of counterarguments;

– think critically and systematically, which is manifested in determining the characteristic features of phenomena, events, ideas, and their

[25] *Model Curriculum. "Informatics. Grades 5-6" for general secondary education institutions* (authors Morze N.V., Barna O.V.). Ministry of Education and Science, 2021. 39 p. URL: https://drive.google.com/file/d/11eaTWGqRcI5SxsO35VFrTV3ipNaUu5X6/view.

[26] *The curriculum of the elective-compulsory subject "Informatics" for students of 10-11 grades of general secondary education (standard level).* Ministry of Education and Science. URL: https://mon.gov.ua/storage/app/media/zagalna%20serednya/programy-10-11-klas/2018-2019/informatika-standart-10-11.docx.

[27] *The program "Informatics" for grades 5 – 9 of secondary schools.* Ministry of Education and Science, 2017. 66 p. URL: https://mon.gov.ua/storage/app/media/zagalna%20serednya/programy-5-9-klas/onovlennya-12-2017/programa-informatika-5-9-traven-2015.pdf.

relationships; the ability to analyze and evaluate the evidence and weight of arguments in judgments, take into account opposing opinions and counterarguments, distinguish facts, their interpretations, recognize attempts to manipulate data, using various resources and methods of assessing the quality of evidence, the reliability of sources and the reliability of information;

– to act creatively, which involves creative thinking, the production of new ideas, the virtuous use of other people's ideas and their refinement, the use of one's knowledge to create new objects and ideas, the ability to test new ideas;

– risk assessment, which involves the ability to distinguish between acceptable and unacceptable risks, taking into account significant factors;

– problem-solving, which involves the ability to analyze problem situations, formulate problems, put forward hypotheses, practically test and justify them, obtain the necessary data from reliable sources, and present and argue solutions.

The model program is based on implementing the content lines of the State Standard for Teaching Informatics[28]. The last content line, "Safety and Responsibility," is attractive in the context of our research. It teaches during both the 5th and 6th grades. It contains topics that are directly relevant to the development of students' information hygiene skills. For example, when studying the topic "Search for information on the Internet," students can be introduced to real examples of inaccurate information, its harmfulness, and ways of recognition; teach students to search for accurate and reliable information; acquire the skills of evaluating sources, separating objective sources from subjective ones, as well as sources with scientific support from blogs or personal sites, etc. When studying "Security in network communities," it is worth paying attention to risk analysis, ethics and norms of behavior in network communities, analysis of information posts, and the creation of correct publications.

In the Curriculum for grades 5-9, among the tasks in the subject "Computer Science," there are those that can be used to develop students' skills in maintaining information hygiene. In this program, the section "Information, Information Processes, Systems, Technologies," which is studied in the 5th (4 hours), 8th (3 hours), and 9th (2 hours) grades, is appropriate for the development of information hygiene skills.

Let's take a closer look at the description of the section "Information, Information Processes, Systems, Technologies" in grades 8 and 9. Moreover, in the 8th grade, only the topic "Data Coding" is considered. The situation is

[28] Standard of School Education in Informatics. URL: https://ukped.com/informatyka/631-standart-shkilnoi-osvity-z-informatyky.html

different in the 9th grade, where there is a topic, "Information Technologies in Society." The following sub-themes are highlighted in this topic:

– The concept of the information society, Intellectual Property, and Copyright;

– Ethics and law in the creation and use of information resources;

– The idea of information culture, information literacy, and ICT competence.

When studying this topic, it is advisable to talk about the formation of the concept of information hygiene because information literacy (a comprehensive skill of understanding, evaluating, critically analyzing, and effectively using information from various sources and media platforms; an information-literate person can effectively work with information resources, recognize inaccurate information, determine its sources and authority, as well as apply ethical standards when using information) and information hygiene closely related to each other.

A more interesting topic for forming the concept of "information hygiene" in the 9th grade is "Fundamentals of Information Security." It includes the following topics: Classification of security threats and data corruption in computer systems. Ethical and legal bases for protecting information and data; Data protection. Malware, its types, principles of operation, and the fight against it; threats that arise when working on the Internet; browser tools designed to ensure security. Secure sites; Spam protection; Secure Data Storage; Data Backup and Restore; Secure deletion of data.

Expected learning outcomes on the topic:

– The student has an idea about secure sites;

– The student explains the need for data protection;

– The student concept and general principles of operation of malware;

– The pupil describes the ethical and legal basis for the protection of data and information resources; threats that arise in the process of using the Internet; features of boot and file viruses, macro viruses, network viruses, worms, and Trojan horses; the purpose of anti-virus scanners, monitors, inspectors, blockers; rules for preventing malware from infecting your computer;

– The student classifies data security threats;

– The student can scan and disinfect folders and drives; configure settings for periodic anti-virus scans and automatic updating of anti-virus databases; use browser tools to protect data; protect against spam; backup and restore data. Securely delete data.

The formation of information hygiene skills in studying the topic "Fundamentals of Information Security" is essential, as it contributes to the understanding and practical application of the principles of safe use of

information technology. The fundamentals of information security provide knowledge about potential threats on the Internet and methods to prevent them. However, building information hygiene skills helps turn this knowledge into practical strategies students can use to protect their personal and financial information. The formation of information hygiene skills contributes to developing a culture of safety on the Internet among students. That is important because ensuring personal and information security should become integral to their behavior in the digital environment.

In the curriculum of the elective-compulsory subject "Informatics" for students of grades 10–11 of general secondary education at the standard level, it is essential to consider the elective module "Information Security," for the study of which 17 hours are allocated. There are three big themes here:

Fundamentals of Information Technology Security. Basic concepts in the field of information technology security. The main reasons for the aggravation of the problem of ensuring the security of information technologies. Information and information relations. Subjects of information relations, their interests, security, and ways of harming them. Information Technology Security. Threats to information security in automated systems. The primary sources and ways of implementing security threats are penetration channels and unauthorized access to information and program code. Major unintentional and deliberate artificial threats. Hardware and software means of information extraction

They are ensuring the security of information technology. Objects of protection. Types of measures to counter security threats. Basic principles of building an information security system in an automated system. Legal basis for ensuring the security of information technologies. The primary defense mechanisms are implemented within various measures and means of protection. Identification and authentication of users. Cryptographic methods of information protection. Control over the integrity of software and information resources. Attack detection. Protection of the perimeter of computer networks. Controls protection mechanisms. International Information Security Standards

They are ensuring the security of computer systems and networks. Problems of providing security in computer systems and networks. Network security tools. Purpose, capabilities, and basic protective mechanisms of firewalls. The main protection mechanisms are packet filtering, network address translation, intermediate authentication, script rejection, mail verification, virtual private networks, counteracting attacks to disrupt network services, and additional functions. Security policy when accessing a public network. Virtual Private Networks (VPNs). Anti-virus protections. General rules for the use of anti-virus tools in automated systems. Virus

detection technologies. Anti-virus protection as a means of neutralizing threats.

The formation of information hygiene skills and the study of the elective module "Information Security" are closely related concepts aimed at the safe and effective use of information resources. Their connection is seen in the following:

1. Protection against threats. Information hygiene includes a set of rules and practices for using information resources that help prevent negative consequences from using technology. It also means implementing security measures to protect against threats like viruses, malware, identity theft, etc.

2. Reliability of information. Information hygiene teaches you to evaluate the sources of information critically. This is important to confirm the reliability of data used in information technology. Recognizing inaccurate or fake information protects you when using digital resources.

3. Personal data. Information hygiene emphasizes the importance of protecting personal data and privacy. Awareness of the risks of personal information leakage and the ability to properly use privacy settings in online services is necessary for information technology security.

4. Correct use of resources. Information hygiene emphasizes that information technology must be practical and ethical. Preventing spam, inappropriate content, aggressive online behavior, and the correct use of resources contributes to creating a safe and friendly digital environment.

5. Responsible consumption of content. Information hygiene teaches the ability to choose and consume content that promotes personal development and growth and does not harm the psycho-emotional state. That is essential for psychological safety in today's information world.

6. Social Engineering Prevention. Information hygiene emphasizes never divulging sensitive information through phone, email, or networks, such as passwords or bank card details. That helps prevent social engineering attacks.

7. Protection against cyberattacks. Information hygiene includes knowledge of typical cyber threats, such as phishing and spamming, and carefully prepared attacks using vulnerabilities. Staying safe online helps prevent such attacks.

Therefore, studying the elective module "Information Security" plays an essential role in forming information hygiene skills, helping to monitor risks, protecting personal data, recognizing dangerous sources of information, and ensuring the ethical and safe use of digital resources.

According to the current computer science curricula for secondary schools, information hygiene skills can be formed almost every year of schooling. However, looking at these topics, little time is devoted to

studying the rules of information hygiene. Therefore, we see the point of offering additional classes on information hygiene for students.

Thus, the school course in computer science has significant potential for implementing the paradigm of forming information hygiene skills. A school computer science course should promote the development of not only technical skills but also critical thinking about the use of technology. Students should learn to distinguish information, identify credible sources, and assess the risks and consequences of uncritical use of technology. Mastering these skills will help students reduce the likelihood of falling for scammers and manipulators online, which, in turn, will have a positive effect on their learning outcomes and social adaptation.

The study of computer science should include technical aspects and skills of ethical behavior on the Internet. Students should learn the rules of ethical communication, respect the rights of other users, and avoid statements that could cause harm. Fostering an appropriate culture that includes tolerance, mutual respect, and respect for copyright will be an essential component of the successful use of technology.

A project-oriented approach to learning can introduce the paradigm of the formation of information hygiene skills. Students can carry out projects to develop the conscious use of technology: developing recommendations for the safe use of social networks, creating their digital portfolio, promoting ethical standards among peers, etc.

Mastering the skills of effective use of technology, developing ethical norms and digital culture, doing project-oriented tasks, and having an active role as a teacher will contribute to the development of conscious and responsible users of information technology. Implementing this paradigm will help prepare the younger generation to use technology safely and productively in a digital society.

4. Determination of the awareness of students about the observance of information hygiene

In 2023, we surveyed children's awareness of information hygiene. We followed[29]. The survey involved 49 students (9-10 class) from five schools in the city. The survey was conducted remotely using Google Forms. Initially, a survey was developed, providing a bank of test questions of both open and closed types (Table 1).

[29] Rudenko Yu., Proshkin V., Naboka O., Yurchenko A., Semenikhina O. Using Bloom's taxonomy to assess information hygiene skills. *E-learning & Artificial Intelligence (AI) Scientific Editor Eugenia Smyrnova-Trybulska "E-learning"*, 15, Katowice–Cieszyn 2023. pp. 137–148 https://doi.org/10.34916/el.2023.15.12.

Table 1

Survey details

№	Questions	Answers
1.	Do you understand the meaning of "information hygiene"?	– Yes, I fully understand – Yes, I partially understand – No, I rather do not understand – No, I do not understand at all
2.	Do you agree with the following statement: the purpose of information hygiene is to reduce the negative impact of information on a person's mental, physical, and social well-being?	– Yes – No – Hard to say
3.	Do you trust information found on the Internet?	– I always trust – Sometimes I trust – Never trust
4.	What, in your opinion, is effective in verifying the authenticity of information from the Internet?	– The photo cannot be verified, so you should not pay attention to it. – It is worth checking whether the headline corresponds to the main part of the message. – The author with the specified name and photo is a real person, so this information should be trusted. – Check for emotional impact in the message. – Errors in the text are just typos, so do not pay attention to them.
5.	How would you characterize the term "spam"?	– mass mailing of unsolicited mail – taking possession of another's property or acquiring the right to property by deception or breach of trust – a type of fraud aimed at luring personal data from gullible or inattentive network users – your own version
6.	Which of the following statements is correct in your opinion?	– Fake news often has catchy titles written in capital letters with exclamation points. – Fake websites never make mistakes in spelling and punctuation. – Copies of well-known pages or websites are often created to promote fake information. – Fake news contains real photos and videos. – Many fake news stories have no date of publication.
7.	In your opinion, what can be a sign that a news item published on the Internet is fake?	– the headline has nothing to do with the text of the news –no reference or source from which certain statements were taken – if no other reliable source reports on these events – the author is a journalist and has never written fake articles
8.	What can you do to check a fake?	– Check primary sources, google – Find information about the author – Check the date of publication – Believe the fake
9.	What is not a reliable source in the news?	– Expert opinion – Statistical data – Data from government agencies – Anonymous informant
10.	If people started calling you rude names on the Internet, what would be your reaction?	

№	Questions	Answers
11.	Who can access your passwords?	– Parents only – Parents and friends – Closest friends – Teachers – No one else
12.	What can't be reported online?	– Favorite music group – Password – Home address – Passport details – Your name – time when you and your family are going on vacation
13.	What is the name of the procedure for checking the compliance of a subject and the person he or she is trying to impersonate with the help of some unique information?	– depersonalization – denationalization – authentication – authorization
14.	Will you take part in a survey to win a prize if you see this message on Viber?	–Yes. Why not try, maybe you'll get lucky. – No, some personal data may be stolen – Yes, the company often holds promotions. Besides, 500–5000 UAH is not a big amount for a well-known network
15.	How to protect yourself from computer viruses?	– Do not visit suspicious sites – Do not use the Internet – You should use antivirus programs with up-to-date signatures – Do not use questionable storage media – Do not open emails with attachments if you do not know who they are from
16.	What tasks do bots perform in the context of information warfare?	– Filling forums with meaningless additional content – Raising funds for specific needs – Manipulating the consciousness of the masses – Deliberate production of certain moods in society
17.	In your opinion, what is the most popular source of news information?	– Radio – Print media – Television – Online media – Social media – YouTube
18.	What are the characteristics of a malicious blogger?	– Uses bots to artificially increase popularity. – Cooperates with media outlets from the "white list" of the Institute of Mass Information. – Emphasizes his/her wealth and popularity. – Comments on only one topic in which he is an expert. – Agrees with constructive criticism.
19.	What threats and risks can arise when using the Internet and other information technologies?	
20.	What rules of ethical communication do you follow when using Internet resources and social networks?	

We conditionally divide all the questions of the questionnaire into four categories.

Understanding Information Hygiene. This category is of utmost importance in our digital world. It aims to assess your understanding of "information hygiene" and the potential risks of not following Internet safety rules. The questions are designed to make you reflect and include: "Do you understand the meaning of the concept of "information hygiene"?"; "Do you agree with the statement: the purpose of information hygiene is to reduce the negative impact of information on the mental, physical, and social well-being of a person?"; "Do you trust the information found on the Internet?"; and more.

Analysis of fake information. The questions in this category aim to identify whether students can distinguish counterfeit messages and news from true ones, identify signs of a fake and the possibility of verifying it, and others. For example, this includes the following questions: "What do you think can be a sign that the news published on the Internet is fake?" "What can be done to check the fake?" "What is not a reliable source in the news?" etc.

Communication in social networks. Questions within this category make it clear how well students can communicate with each other in social networks/messengers, the ability to choose the right interlocutor, etc. Here, we can highlight such questions as "If you are called rude words on the Internet, what will be your reaction?", "What should not be reported on the Internet?" "What characteristics can be used to recognize a harmful blogger?" "What rules of ethical communication do you follow when using Internet resources and social networks?".

Security of personal data. The last category, according to which we can see how safe students behave on the Internet, is whether they do not disclose their confidential data, do not download suspicious files, do not infect their computers with malware, etc. This category includes the following questions: "How to protect yourself from computer viruses?", "To whom can you share your passwords?" "What tasks do bots perform in the context of information warfare?" "What threats and risks may arise when using the Internet and other information technologies?".

Let's analyze the answers to some questions of the questionnaire, which was designed to gauge the understanding and awareness of information hygiene and fake news, for each of the categories.

When asked about their understanding of the term "information hygiene" in the category "Understanding information hygiene," it was concerning to find that the majority of students (69%) were not familiar with this crucial concept. 12% admitted to having no idea about it, and 57% may have heard something about it but do not know what it is. This lack of awareness underscores the urgency of our mission to educate about information hygiene.

The purpose of information hygiene, as perceived by the respondents, was a topic of diverse opinions. While the majority (51%) agreed that it is to reduce the negative impact of information on a person's mental, physical,

and social well-being, a significant 18% categorically disagreed with this view. This diversity of opinions highlights the complexity of the issue and the need for further discussion.

The following answers were given to the questions of the "Analysis of Fake Information" category. Thus, when choosing the correct statements, the students noted that "copies of well-known pages or sites are often created to promote fake information" – 71%, "Much fake news does not have a publication date" – 59%, although the least plausible statement was "Fake news often has bright names written in capital letters with exclamation marks" – 31%. These responses highlight the students" understanding of some common tactics used in the creation and dissemination of fake news.

When asked what, in the students' opinion, could be a sign that the news published on the Internet is fake, it was encouraging to see that the majority of students (84%) correctly identified that a headline having nothing to do with the text of the news is a red flag. Other signs they recognized include the lack of reference or source from which certain statements were taken (49%) if no other reliable source reports these events (39%), and the author is a journalist who has never written fake articles (31%). This demonstrates their growing information literacy skills and gives us hope for the future.

In the "Communication in social networks" category, we considered questions with an open-answer form. So, there were many answers regarding the question, "If they started calling you rude words on the Internet, what would be your reaction?". Among the positive (not rude) answers, the most interesting are: "I will answer politely and try to find out why this happened," "I will ignore this message and continue my activities," "I will ask myself whether it is worth responding to such provocations," "I will try to respond with humor or irony to relieve tension," "I will answer from a position of tolerance and try to understand why the person acted this way." Some students gave a rude answer, in particular, among such answers we highlight: "I will respond in a rude tone back and enter into a conflict," "I will take a screenshot of an offensive message and post it on social networks for public criticism", "I will delete or block the user who sent such a message."

One of the questions in this category was, "What rules of ethical communication do you follow when using Internet resources and social networks?". There were also some exciting answers to this question, including: "express your opinion politely and reasonably, without using offensive words," "avoid conflict situations, do not engage in controversial discussions and do not provoke others," "Check facts before sharing information or links," "do not make critical reviews and comments about the appearance, nationality or religious beliefs of others," etc.

In the "Personal Data Security" category, we considered two questions – "Who can you share your passwords with?" and "How can you protect yourself from computer viruses?". As for the answers to the first question

about providing access to passwords, almost half of the students indicated that access to personal passwords should not be shared with anyone (49% of respondents), 18% said that access should only be given to parents, 14% – both parents and friends and some believe that access to passwords can be given even to teachers – 6%.

Children gave different answers to the second question about computer viruses, but the majority (73%) believe that visiting suspicious sites can affect a computer's vulnerability. 45% believe that the use of dubious media affects vulnerability. And 18% of respondents generally noted that to avoid infecting your computer with viruses, you should not use the Internet (18%).

After analyzing the students' answers, there is reason to conclude that most students need to develop the skills of information hygiene, and knowledge of information hygiene still needs to be completed. However, most students follow specific information security rules when using the Internet.

CONCLUSIONS

1. Information threats appear and spread under the influence of the development of information technology. The ways of spreading information threats are the global Internet, intranet (local network), e-mail, and portable media. General attention to different types of information threats and developing adequate protection and countermeasures are essential for society. A separate countermeasure can be the observance of information hygiene by each member of society.

2. Information hygiene is a branch of knowledge that studies the patterns of influence of information flows on human health and public health. The formation of information hygiene skills among young people is necessary to develop a harmonious personality capable of functioning confidently in the digital world.

3. The analysis of computer science curricula showed that it has significant potential for introducing the paradigm of forming information hygiene skills in grades 5–9 and 10–11 by cyclically studying the topics "Fundamentals of Information Security" and "Information Security." At the same time, a quantitative analysis of the hours spent on these topics shows that more hours are needed to develop students' information hygiene skills successfully.

4. The practical state of awareness of pupils of Sumy region about the formation of information hygiene skills revealed that most students do not have formed information hygiene skills, and knowledge about information hygiene is fragmentary, although most students adhere to certain rules of information security when using the Internet.

5. The conducted research actualizes other areas of scientific and methodological research: the formation of students' skills in observing information hygiene at different levels of school education, the formation of

students' skills in observing information hygiene in the conditions of differentiated learning, in the conditions of non-formal education, based on a competence approach, etc.

SUMMARY

The problem of forming information hygiene skills in young people is relevant, and we naturally associate its solution with teaching computer science. The purpose of the study is to characterize the information hygiene skills of young people and to substantiate the possibility of their formation in computer science classes. We have analyzed computer science curricula and shown that the school computer science course has significant potential for implementing the paradigm of developing information hygiene skills in grades 5-9 and 10-11 and cyclically when studying the topics “Fundamentals of Information Security” and “Information Security.” A quantitative analysis of the hours for teaching these topics shows that they are insufficient to develop the students' information hygiene skills successfully. The practical state of students' awareness of information hygiene has demonstrated that most students need to gain the appropriate skills, and their knowledge of information hygiene needs to be more cohesive and systematic.

BIBLIOGRAPHY

1. Bekhter L. A. Threats to information security and information protection as a component of economic security of agricultural enterprises. *Agrosvit*. 2020. № 12. pp. 66–70.

2. Bodnar I. R. Information Security as the Basis of National Security. *Mechanism of Economic Regulation*, 2014, No. 1. P. 68–75.

3. Demchenko, P. Cybernetic Security as the Newest Direction of the Information Component of National Security of Ukraine: Constitutional and Legal Aspect. URL: http://publications.lnu.edu.ua/bulletins/index.php/law/article/view/9560.

4. Demianenko V.M. Information hygiene in the era of "Post-Truth". *Young Scientist*, 2017. No 9.1 (49.1). P. 46–50.

5. Denisov E.I., Eremin A.L., Sivochalova O.V., Kurierov N.M. Information hygiene and regulation of information for vulnerable groups of the population. Hygiene and Sanitation, 2014. No5. P. 43–49.

6. Drushliak M. G., Semenoh O. M., Grona N. V., Ponomarenko N. P., Semenikhina O. V. Typology of Internet resources for the development of infomedia literacy of youth. *Information Technologies and Teaching Tools*, 2022. No. 88(2). P. 1-22. https://doi.org/10.33407/itlt.v88i2.4786.

7. Gelyukh M. Information hygiene: why it is needed and how not to become victims of fakes, 2020. URL: https://ua.news/ua/technologies/informatsionnaya-gigiena-zachem-nuzhna-i-kak-ne-stat-zhertvami-fejkov.

8. Khalamendyk V. B. Information hygiene as a factor of preservation of human mental health. *Humanitarian Bulletin of Zaporizhzhya State Engineering Academy*, 2008. No 35. P. 83–91.

9. Khalamendyk V. B. Information hygiene as a factor of preserving human mental health. *Humanitarian Bulletin of Zaporizhzhya State Engineering Academy*, 2008. No 35. P. 83–91.

10. Koterlin I. B. Information Security in the Conditions of Martial Law in the Aspect of Ensuring Information Rights and Freedoms. Actual Problems of Domestic Jurisprudence No. 1. 2022. C. 150–155.

11. Koterlin I. B. Information Security in the Conditions of Martial Law in the Aspect of Ensuring Information Rights and Freedoms. *Actual Problems of Domestic Jurisprudence* No. 1. 2022. C. 150–155.

12. Lazorenko S. A., Semenikhina O. V. Current state of the problem of formation of information and digital culture of future specialists in physical culture and sports. *Bulletin of Cherkasy Bohdan Khmelnytsky National University,* 2020. No 4. P. 42–47.

13. Loukas G., Murugesan S., Andriole S. J. Information Hygiene: The Fight Against the Misinformation “Infodemic”. IT Professional, 2022. Is. 24(2). pp. 16–18. https://doi.org/10.1109/MITP.2022.3163007.

14. *Model Curriculum. "Informatics. Grades 5-6" for general secondary education institutions* (authors Morze N.V., Barna O.V.). Ministry of Education and Science, 2021. 39 p. URL: https://drive.google.com/file/d/11eaTWGqRcI5SxsO35VFrTV3ipNaUu5X6/view

15. Muzhanova T.M. Internet censorship as a threat to citizens' rights in the field of information security. *Modern Information Protection* No. 2, 2015. P. 84–88.

16. Platonenko A.V. Modern threats of information security for public and private institutions of Ukraine. *Modern information protection*. 2015. № 4. pp. 86–90.

17. Rudenko Y. O., Drushliak M. G., Shamonya V. G., Ostroha M. M., Semenikhina O. V. Development of the ability of student youth to resist information influences. *Information technologies and teaching tools*. 2023. №94(2). Pp. 54–71. https://doi.org/10.33407/itlt.v94i2.5162

18. Rudenko Y., Ahadzhanova S., Ahadzhanov-Honsales K., Bieliaieva O., Korovai A., Semenikhina O. Effective Educational Ukrainian Practices of the Formation of Media Literacy, 2023 *46th MIPRO ICT and Electronics Convention* (MIPRO), Opatija, Croatia, 2023, pp. 654-659. https://doi.org/10.23919/MIPRO57284.2023.10159822.

19. Rudenko Yu., Proshkin V., Naboka O., Yurchenko A., Semenikhina O. Using Bloom’s taxonomy to assess information hygiene skills. *E-learning & Artificial Intelligence (AI) Scientific Editor Eugenia Smyrnova-Trybulska “E-learning”,* 15, Katowice–Cieszyn 2023. pp. 137–148 https://doi.org/10.34916/el.2023.15.12

20. Semenog O., Semenikhina O., Oleshko P., Prima R., Varava O., Pykaliuk R. Formation of Media Educational Skills of a Future Teacher in the Professional Training. *Revista Românească pentru Educaţie Multidimensională*, 2020. Vol. 12. Is. 3. p. 219-245. https://doi.org/10.18662/rrem/12.3/319.

21. Shemchuk V.V. Information Security and Information Defense in the Context of the Development of Domestic Doctrine and Legislative Framework. Theory and History of State and Law; History of Political and Legal Doctrines. Scientific Notes of V.I. Vernadsky TNU. Series: Legal Sciences, 2019. Vol. 30 (69) No. 4. P. 29–37.

22. Shemchuk V.V. Information Security and Information Defense in the Context of the Development of Domestic Doctrine and Legislative Framework. Theory and History of State and Law; History of Political and Legal Doctrines. Scientific Notes of Vernadsky TNU. Series: Juridical Sciences, 2019. Vol. 30 (69) No. 4. P. 29–37.

23. *Standard of School Education in Informatics*. URL: https://ukped.com/informatyka/631-standart-shkilnoi-osvity-z-informatyky.html

24. *The curriculum of the elective-compulsory subject "Informatics" for students of 10-11 grades of general secondary education (standard level).* Ministry of Education and Science. URL: https://mon.gov.ua/storage/app/media/zagalna%20serednya/programy-10-11-klas/2018-2019/informatika-standart-10-11.docx

25. *The program "Informatics" for grades 5 – 9 of secondary schools. Ministry of Education and Science*, 2017. 66 p. URL: https://mon.gov.ua/storage/app/media/zagalna%20serednya/programy-5-9-klas/onovlennya-12-2017/programa-informatika-5-9-traven-2015.pdf

26. *The World Health Report 2001 – Mental Health*: New Understanding, New Hope. Geneva: WHO; 2001. URL: http://www.who.int/publications/list/whr01/ru

27. Vovk V. M. Fakes as a Threat to National Security in the Context of Hybrid War. *Philosophical and Methodological Problems of Law*, 2022. № 2 (24). S. 80–85.

28. Yanovsky A. O. Emotional and motivational content of the process of forming a culture of safe use of the information environment in future teachers. *Scientific Bulletin of the South Ukrainian National Pedagogical University named after K. D. Ushynsky*, 2019. Issue 4 (129). P. 7–12.

Information about the author:
Semenikhina Olena Volodymyrivna,
Doctor of Pedagogical Sciences, Professor,
Professor at the Computer Sciences Department
Makarenko Sumy State Pedagogical University
87, Romenska St, Sumy, 40002, Ukraine