# Цифровизация в образовании
# Digitalization of education

Original article
DOI: 10.14529/ped220206

## INFORMATION SECURITY CHALLENGE OF MODERN SOCIETY

***Ju. Anttila**, juhani.anttila@gmail.com, https://orcid.org/0000-0001-8884-3739*
*International Academy for Quality, Helsinki, Finland*

***Abstract.*** Information security is vital for all living organisms, people, organizations and society as a whole, since information security is the basis of all life activities. The ambiguity of understanding the terms "information" and "security" leads to the need to clarify the conceptual apparatus on the problem of ensuring information security. The article reveals the meaning of information security as a challenge to modern society. The concept of "information security" is clarified. Information security is considered in terms of privacy protection, security of organizational operations and cybersecurity. The author's understanding of information security is given from the point of view of the organization's management, of individual subjects, and society. It is substantiated that people simultaneously use information security, provide it, and are also subject to information threats. Information security requires certain competencies, skills and actions from organizations and individuals, both in professional and personal life. Appropriate competencies are needed in education, research and social activities. To manage activities to ensure information security, a multi-disciplinary approach and interaction of organizations from different areas of activity of the human community is required. This determines the need for the members of society to master the competencies of information security, which is one of the tasks of modern education. The standardized requirements for the protection of personal data and confidentiality that exist in the EU, which must be observed by organizations and administrations, can serve as guidelines for the formation of information security competencies and for its provision in practice. The existence of standards provides a systematic and consistent practice of risk management and security.

***Keywords:*** information, information security, information society, digitalization, conceptualization, threats, risks

***For citation:*** Anttila Ju. Information security challenge of modern society. *Bulletin of the South Ural State University. Ser. Education. Educational Sciences*. 2022;14(2):65–70. DOI: 10.14529/ped220206

Научная статья
УДК 316.32:004-27.45
DOI: 10.14529/ped220206

## ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ КАК ВЫЗОВ СОВРЕМЕННОМУ ОБЩЕСТВУ

***Ю. Анттила**, juhani.anttila@gmail.com, https://orcid.org/0000-0001-8884-3739*
*Международная академия качества, Хельсинки, Финляндия*

***Аннотация.*** Информационная безопасность касается всех живых организмов, людей, организаций и общества в целом, поскольку безопасная информация является основой всех видов жизнедеятельности. Неоднозначность понимания терминов «информация» и «безопасность» приводит к необходимости уточнения понятийного аппарата по проблеме обеспечения информационной безопасности. Статья посвящена раскрытию смысла информационной безопасности как вызова современному обществу. Уточнено понятие «информационная безопасность». Информационная безопасность рассмотрена в аспектах защиты частной жизни, безопасности организационных операций и кибербезопасности. Дано авторское понимание информационной безопасности с точки зрения менеджмента организации, с позиции индивидуальных субъектов и общества. Обосновано, что люди

одновременно пользуются информационной безопасностью, обеспечивают ее, но и подвержены информационным угрозам. Информационная безопасность требует определенных компетенций, навыков и действий от организаций и отдельных лиц как в профессиональной, так и в личной жизни. Соответствующие компетенции необходимы в образовании, научных исследованиях и общественной деятельности. Для управления действиями по обеспечению информационной безопасности необходим мультидисциплинарный подход и взаимодействие организаций разных сфер деятельности человеческого сообщества. Этим обусловлена потребность в овладении членами общества компетенциями информационной безопасности, что составляет одну из задач современного образования. Ориентирами формирования компетенций информационной безопасности и для ее обеспечения на практике могут служить существующие в ЕС стандартизированные требования по защите личных данных и конфиденциальности, которые должны соблюдаться организациями и администрациями. Наличие стандартов обеспечивает системность и последовательную практику управления рисками и обеспечения безопасности.

***Ключевые слова:*** информация, информационная безопасность, информационное общество, цифровизация, концептуализация, угрозы, риски

***Для цитирования:*** Anttila Ju. Information security challenge of modern society // Вестник ЮУрГУ. Серия «Образование. Педагогические науки». 2022. Т. 14, № 2. С. 65–70. DOI: 10.14529/ped220206

## Introduction

Information security is a very ordinary thing but also a highly professional specialty. In organizations, information security [16] is one of the managerial knowledge areas, which also has become a significant basis for the reliable economic and social operation of the whole society, and hence, it also strongly influences the lives of individuals. It applies to the business information of the organizations, the privateness-related facts of individuals, and versatile information within the complex cyberspace [18] products, processes, systems, and infrastructures of society.

Organizations and societies are formed of people, and hence, the human aspects have the most important role also in implementing and perceiving information security [4] but also in causing the related uncertainty, insecurity, and threats [10]. Theoretical concepts and models, rules and practices, and technological, managerial, and societal solutions created by the human thinking process have a big influence on how information security is perceived, recognized, managed, evaluated, and how it will be developed. Very often technical aspects of the solutions of information and communication technology (ICT) are overly emphasized in information security discussions.

This article refers to the international information security management standards [17] as important references for organizational information security considerations. In addition to the management standards, there are a large number of specialized technical standards, the usefulness of which is based on the knowledge and skills of experts and management decisions. Unfortunately, the key principles and concepts are not handled consistently in the general information security management standards, and their linkages to recognized managerial models and practices are brought up inadequately. A problem is that the main ideas of the information security management standards, which (for instance ISO/IEC 27001 [17]) are widely used in organizations, are dating back decades. Hence, proactive innovative solutions for modern business and societal environments, which are characterized by the speed, changes, agility, and complexity originating from digitalization, have not enough been brought up in the standards.

## Conceptual ambiguousness and fragmented management

Information security comes a lot to the fore in scientific, political, and everyday writings and speeches today. In addition, the topic has a large and growing practical significance in the activities of people, organizations, and whole societies. However, we have recognized that information security is conceptually unclear, and information security management is fragmented. For instance, the technical and organizational/managerial perspectives are far apart, and human or social aspects are not sufficiently regarded.

Information security [19] is a broad and multidimensional concept, it includes privacy information [20] and cyber security [7] aspects, which often are dealt with separately. Hence, the basic related concepts, terms, and definitions are not considered consistently or logically even in the professional contexts. This situation is espe-

cially originated from the vague meanings of the words "information" and "security", which are used by many different disciplines and practical fields.

Terms *secure* and *security* can characterize a particular property, ability, or state of any object. Etymologically [14] they are positive features of the object: In Latin: sēcūrus – *being without worry*, including parts sē- [prefix] – without, and cūr(a) – worry + -us [adjective suffix]. Actually, some international standards define security according to this general understanding, as follows:

- State of being free from danger or threats where procedures are followed or after taking appropriate measures [15].
- Condition of being protected against hazards, threats, risks, or loss [23].
- Quality or state of being protected from unauthorized access or uncontrolled losses or effects [22, 25].

Another difficult part of the information security concept is *information*, which is a general everyday word but also has a philosophical background. The general dictionary explanation [27] is that information means *facts provided or learned about something or someone*. However, there also are many definitions, which bring up many aspects that relate to information, for instance, fact, data, information, knowledge, and wisdom. Information security also can be considered in relation to all of these. The information is not only alphanumeric but consists of a wide variety of human intellectual products. Information security can even be examined in the connection with human thoughts and mind [11], particularly due to modern technological means. The genetic information [2, 26] of humans and organisms, which is stored in genes in paired DNA (deoxyribonucleic acid) molecules in cells, and which is the essence of all life, may also be dealt with as a specific subject and concern of information security.

All real-world things and phenomena include many different kinds of *facts*. Through measuring those phenomena, we can get *data*. Analyzing data, we get contextually significant *information*. Information is a basis for reflecting on the situation and making decisions. When combining measurement-based information with *explicit knowledge* (articulated, documented, and shared information), *tacit knowledge* (personal implicit skills, ideas, and experiences), and *wisdom* (myths and values), one can consistently carry out the plans, acts, and interventions to control and improve the situation [24].

General information security management standards [16, 17] and experts have the main focus on ICT and often highlight problems, risks, hazards, threats, vulnerabilities, hostile actors, and reactive countermeasures against them. The search for proactive opportunities to prepare for future challenges has been left to those applying the standards. The standards [1, 17] refer to an old traditional way to deal with *information security* with an open list of concepts to preserve *confidentiality* (C), *integrity* (I), and *availability* (A) of information, and, in addition, to take into account also other pertinent concepts, such as authenticity, accountability, non-repudiation, and reliability. This is a reductionist way to define a concept and causes difficulties with the issues that do not seem to be on the list. Also, it is unclear in the standard approach, whether here information security is understood as a concept of feature or activity (preservation). These by the experts defined concepts of information security are often difficult concepts to understand within business situations and even among information security experts.

*Privacy protection* is a central and significant area of information security. Its role is, however, vague in the standards-based information security examinations. Nevertheless, privacy may be seen as a core issue of all other information security concepts and even been considered as the "archetype" of the whole information security discipline, from which the other concepts may be led [20].

Often today, people use the term cybersecurity instead of information security. This means information security in cyberspace, which is a complex environment resulting from the interaction of people, software, and services on the Internet by means of technology devices and networks connected to it. According to the CIA model, cybersecurity [21] implies the preservation of confidentiality, integrity, and availability of information in cyberspace.

The proper implementation of information security in organizations requires this issue to be taken into account in all activities and management of the organization. Accordingly, the concept of *information security management* can be formally defined as *management with regard to information security*. The means to do so are then set out in more detail for instance in the relevant standards [13].

**Information security from individuals to society**

Information security can be viewed from the perspective of people, organizations, and society as a whole. People play a key role because organizations and society are also made up of human individuals. In society, information security develops through diffusion by the activities and results of organizations and individuals. Each organization or individual has its own priorities regarding relevant information and the importance of information security. They also have their own vulnerabilities and risks and procedures for these.

In practice, information security is realized by doing the right thing, in particular, in organizations through business processes. In this context, too, the risks [20] may also materialize. Processes include people and various technical systems as resources. Persons interact within their working processes according to their skills, individual character traits, moral standards, and behavioral style. In human activities, information security is based on awareness, competence, and learning.

Practically all technical systems include ICT modules and software applications today. For technical solutions, information security solutions are the results of the design process. Communication protocols have an important role in information security as they define the rules, how different systems and system units share operational information. In addition to the operational information, also key system facts and settings are essential issues for information security and the vulnerability of the system.

People are both implementers and perceivers of information security but they are also subject to information security threats. In today's information society, people cannot cope without the access or skills to access society's information services.

There are international standard requirements for the protection of personal identity and privacy that should also be respected by organizations and administrations. They deal with the personally identifiable information (PII) [12], which consists of any information, (a) which can be used to identify the person to whom such information pertains, (b) from which such information can be derived, or (c) that is or might be directly or indirectly linked to a natural person. The EU's General Data Protection Regulation (GDPR) [23] is a serious challenge in protecting privacy and identity in all organizations operating in Europe or marketing products to EU residents. The GDPR has defined significant financial consequences for businesses that are not in compliance.

**Information security challenges, threats, and grievances of the digital society**

The modern information society poses difficulties and threats to many areas of people's lives, for instance regarding:

- Disadvantages in everyday activity, and behavioral, mental, and economic development.
- Privacy and security.
- Data overloading, misinformation, false news, or alternative facts.

The strong impact of digitalization requires increasing demands for new competencies, skills, and operations by organizations and individuals in job and private life in responding to the changing challenges of society. That should be taken into account also in education, research, and societal activities. Particular needs include a) innovative and adaptive thinking, b) virtual collaboration and social intelligence, c) ability to work across disciplines, d) literacy in different types of media, and e) computational thinking and analytics [14, 29].

Many existing global megatrends, including urbanization, geopolitical contradictions, refugee migrating, multicultural encountering, and economic uncertainty and crises, which have caused societal grievances and threats, are all closely linked with digital information and communication, and hence, also with information security. Modern wars and terrorism [3] are especially information-intensive – in practice, there is talk of information wars – and are filled with false or misleading narratives and conspiracy theories.

As large-scale examples, where information security violations and even criminal measures have currently existed, we can mention here the Covid-19 pandemic, climate change, as well as a global power play to control wealth, humanity, and humans [5, 8, 9, 28]. These global issues are very broad and have serious implications for societal operations. In these cases, a lot of deliberately manipulated, incorrect, or incomplete information has been shared, and correct information has been suppressed for ensuring spreading a certain kind of perception of things widely among the people. There are also scientific references for such approaches [6].

**Conclusions**

Information security is everyone's business and a relevant issue in all areas of life. It applies to people, organizations, and society as a whole.

Especially in a modern digital society and in times of crisis, its importance is emphasized.

Information security is a demanding issue. The phenomena associated with it are complex and intricate. Measures for information security are difficult because they today require multidisciplinary solutions incorporating humans and technology. In addition to expertise, decisions and measures are needed at the individual and organizational levels with competence, awareness, and the right attitude. The issue is hampered that the concepts of information security are – perhaps paradoxically – vague and ambiguous although based on international standards.

Also, criminal activity exists in the area of information security, as in all areas of human activity. However, detecting it and preparing for it is demanding. Expertise, examinations, and juridical solutions are needed for countermeasures, which, however, are available in society and should be used and exploited, too.

Widely used digitalization and information technology increase information security threats and vulnerabilities, but on other hand, its many solutions also provide help for challenging incidents and find solutions to problems. However, people always have the ultimate responsibility.

**References**

1. Anttila J., Savola R., Kajava J., et. al. Fulfilling the Needs for Information Security Awareness and Learning in Information Society. *The 6th Annual Security Conference.* Las Vegas, USA, 2007. Available at: https://www.semanticscholar.org/paper/Fulfilling-the-Needs-for-Information-Security-and-Anttila-Savola/b0aedf07ac73b0b4f74bb0d32fda065e82e3794b (accessed 12.03.2022). DOI: 10.1109/iccias.2006.295314

2. Anttila J. [Continuing Education for the Sustainable Development of a Quality Society]. *Obrazovanie cherez vsyu zhizn': nepreryvnoe obrazovanie v interesakh ustoychivogo razvitiya*. [Lifelong Learning: Continuing Education for Sustainable Development], 2015, no. 13. Available at: https://cyberleninka.ru/article/n/nepreryvnoe-obrazovanie-dlya-ustoychivogo-razvitiya-kachestvennogo-obschestva (accessed 13.03.2022). (in Russ.)

3. Anttila J., Jussila K. Sustainability as an Aspect of Societal Quality. *ICSD2021 Conference*. New York, USA, 2021. Available at: https://ic-sd.org/events/icsd-2021/ (accessed 13.03.2022).

4. Anttila J., Savola R., Kajava J., et. al. Fulfilling the Needs for Information Security Awareness and Learning in Information Society. The Information Institute. *The Annual Security Conference*. Las Vegas, USA, 2007. Available at: https://www.semanticscholar.org/paper/Fulfilling-the-Needs-for-Information-Security-and-Anttila-Savola/b0aedf07ac73b0b4f74bb0d32fda065e82e3794b (accessed 13.03.2022). DOI: 10.1109/iccias.2006.295314

5. Burt C. ID2020 and Partners Launch Program to Provide Digital ID with Vaccines, 2019. Available at: https://www.biometricupdate.com/201909/id2020-and-partners-launch-program-to-provide-digital-id-with-vaccines (accessed 13.03.2022).

6. Desmet M. Mass Formation – Fear Based Narrative, 2022. Available at: https://tegenwindmolen.be/mattias-desmets-fear-based-narrative/ (accessed 13.03.2022).

7. Etymology Dictionary. Security, 2022. Available at: https://www.etymonline.com/search?q=security (accessed 13.03.2022).

8. GlobeNewswire. Humanity 2.0 Chairman Fr. Philip Larrey Named Dean of Philosophy at Vatican's Pontifical Lateran University, 2020. Available at: https://www.globenewswire.com/news-release/2020/07/16/2063319/0/en/Humanity-2-0-Chairman-Fr-Philip-Larrey-Named-Dean-of-Philosophy-at-Vatican-s-Pontifical-Lateran-University.html (accessed 12.03.2022).

9. Herman E., Chomsky N. *The Political Economy of the Mass Media*. Pantheon Books Publ., 1988. 412 p.

10. IBM. Reviewing a Year of Serious Data Breaches, Major Attacks and New Vulnerabilities. *Cyber Security Intelligence Index*, 2016. Available at: https://public.dhe.ibm.com/common/ssi/ecm/se/en/sew03133usen/SEW03133USEN.PDF (accessed 12.03.2022).

11. Ilardi G. The 9/11 Attacks – A Study of Al Qaeda's Use of Intelligence and Counterintelligence, 2009. Available at: https://www.tandfonline.com/doi/full/10.1080/10576100802670803 (accessed 12.03.2022).

12. Intersoft Consulting. *General Data Protection Regulation GDPR*, 2016. Available at: https://gdpr-info.eu/ (accessed 12.03.2022). DOI: 10.1093/oso/9780198826491.003.0001

13. *ISO 31000: 2018 Risk Management – Principles and Guidelines,* Geneva, Switzerland, 2018. Available at: https://www.iso.org/standard/65694.html (accessed 10.03.2022).

14. *ISO 22 383: 2020 Security and resilience – Authenticity, Integrity and Trust for Products and Documents – Guidelines for the Selection and Performance Evaluation of Authentication Solutions for Material Goods*, Geneva, Switzerland, 2020. Available at: https://www.iso.org/standard/50285.html (accessed 10.03.2022). DOI: 10.3403/30392371u

15. *ISO 28002:2011 Security Management Systems for the Supply Chain – Development of Resilience in the Supply Chain – Requirements with Guidance for use*, Geneva, Switzerland, 2011. Available at: https://www.iso.org/standard/56087.html (accessed 10.03.2022). DOI: 10.3403/30217465u

16. *ISO/IEC 27000: 2018 Information technology – Security Techniques – Information Security Management Systems – Overview and Vocabulary*, Geneva Switzerland, 2018. Available at: https://www.iso.org/standard/73906.html (accessed 10.03.2022). DOI: 10.3403/30166243

17. *ISO/IEC 27001 Information Security Management*, Geneva, Switzerland, 2013. Available at: https://www.iso.org/isoiec-27001-information-security.html (accessed 10.03.2022). DOI: 10.3403/30428291u

18. *ISO/IEC 27002 Information Technology – Security Techniques – Code of Practice for Information Security Controls*, Geneva Switzerland, 2013. Available at: https://www.iso.org/obp/ui/#iso:std:iso-iec:27002:ed-2:v1:en (accessed 10.03.2022). DOI: 10.3403/30423203u

19. *ISO/IEC 27032:2012 Information Technology – Security Techniques – Guidelines for Cybersecurity*, Geneva Switzerland, 2012. Available at: https://www.iso.org/standard/44375.html (accessed 10.03.2022). DOI: 10.3403/30362593u

20. *ISO/IEC 29100Ж 2011 Information Technology – Security Techniques – Privacy Framework*, Geneva, Switzerland, 2011. Available at: https://www.iso.org/standard/45123.html (accessed 10.03.2022). DOI: 10.3403/30207803u

21. *ISO/IEC JTC 1/SC 27 Standards Catalogue IT Security Techniques.* Geneva Switzerland, 2018. Available at: https://www.iso.org/committee/45306/x/catalogue/p/1/u/0/w/0/d/0 (accessed 10.03.2022).

22. *ISO/TR 13569 Financial Services – Information Security Guidelines*, Geneva, Switzerland, 2005. Available at: https://www.iso.org/standard/37245.html (accessed 10.03.2022).

23. *ISO/IEC JTC 1/SC 27 Information Security, Cybersecurity and Privacy Protection*, 2022. Available at: https://www.iso.org/committee/45306.html (accessed 10.03.2022).

24. Lee J. 5 Key Skills Needed in the Digital Economy, 2016. Available at: https://www.linkedin.com/pulse/5-key-skills-needed-digital-economy-jaclyn-lee-phd?trk=mp-reader-card (accessed 10.03.2022).

25. *Lexicon. Information*, 2022. Available at: https://www.lexico.com/definition/information (accessed 10.03.2022).

26. *Lumen. Genetic Information*, 2022. Available at: https://courses.lumenlearning.com/wm-biology1/chapter/reading-genetic-information/ (accessed 10.03.2022).

27. *MedlinePlus. What is DNA*? 2021. Available at: https://medlineplus.gov/genetics/understanding/basics/dna/ (accessed10.03.2022).

28. Schwab K. and Malleret, T. Covid-19: The great reset, 2020. Available at: http://reparti.free.fr/schwab2020.pdf (accessed 10.03.2022).

29. Schwab K., Samans R. The Future of Jobs. Employment, Skills and Workforce Strategy for the Fourth Industrial Revolution. *World Economic Forum*, 2006. Available at: http://reports.weforum.org/future-of-jobs-2016/preface/ (accessed 10.03.2022).

***Information about the author***
**Juhani Anttila**, Academician, International Academy for Quality, Helsinki, Finland.
***Информация об авторе***
**Анттила Юхани**, академик, Международная академия качества, Хельсинки, Финляндия.

***The article was submitted 14.03.2022***
***Статья поступила в редакцию 14.03.2022***