STUDIA NAD BEZPIECZEŃSTWEM

Nr **7** **ss. 39–47** **2022**

ISSN 2543–7321

Przyjęto: 06.10.2022
Zaakceptowano: 06.10.2022

Oryginalna praca badawcza

DOI: 10.34858/SNB.7.2022.003

Wiesław Babik
Jagiellonian University
w.babik@uj.edu.pl
ORCID: 0000-0002-7074-8992

INFORMATION SECURITY AS A GLOBAL CHALLENGE FOR THE 21ST CENTURY

BEZPIECZEŃSTWO INFORMACJI GLOBALNYM WYZWANIEM XXI WIEKU

Abstract: The subject of this article is information security treated as a global challenge of the 21st century. The reason for this is the existence of many contemporary threats to information, both in the public and private spheres, which place information in a dangerous situation. The answer to this challenge is, among others, information ecology, whose info-ecological guidelines on how to make information safe in the mentioned spheres are noteworthy. The article presents appropriately categorised threats to information, as well as info-ecological principles of information security which are useful in the face of the challenges and threats of cyberspace.

Zarys treści: Przedmiotem artykułu jest bezpieczeństwo informacji potraktowane jako globalne wyzwanie XXI wieku. Powodem tego jest istnienie wielu współczesnych zagrożeń informacji, zarówno w sferze publicznej, jak i prywatnej, które stawiają informacje w niebezpiecznej sytuacji. Odpowiedzią na to wyzwanie jest m.in. ekologia informacji, której infoekologiczne wytyczne dotyczące tego jak uczynić informację bezpieczną w wymienionych sferach są godne uwagi. W wystąpieniu zostaną zaprezentowane odpowiednio skategoryzowane zagrożenia informacji, jak również infoekologiczne zasady bezpieczeństwa informacyjnego przydatne współczesnemu człowiekowi w obliczu wyzwań i zagrożeń cyberprzestrzeni.

Keywords: information security, threats to the infosphere, information ecology
Słowa kluczowe: bezpieczeństwo informacji, zagrożenia infosfery, ekologia informacji

Introduction

Although information security as a subject of scientific consideration emerged in Poland in the late 1990s, it did not gain research momentum until after 2010, and it is still accompanied by a separate scientific discipline called "Security Science."[1]

[1] Batorowska, H., *Od alfabetyzacji informacyjnej do kultury informacyjnej*, Wydawnictwo Stowarzyszenia Bibliotekarzy Polskich, Warszawa 2012, p. 9.

In the 21st century, the role and importance of information is undeniably growing. At the same time, as the importance of information increases, so do the threats to its security. In the age of widespread computerisation, threats are emerging that did not exist before. The American programmer Edward Yourdon, who died in 2016, argued that "[...] if the 1980s were described as the decade of quality, the 1990s as the decade of productivity, then the first decade of the new century will be the decade of security."[2] Information security is now one of the key issues of the 21st century, stemming from the world's dependence on information technology and especially computer technology and the Internet. This is fostered by Poland's current geopolitical situation and the accompanying narrative about the threats generated by the information society, including the risks associated with information security governance.

Information security has been recognised as a broader term in relation to information security, thus constituting a foundation for an interdisciplinary approach to this complex of problems related to the secure collection, processing and sharing of information, and at the same time the subject of research in security and information sciences, as well as the shaping of an appropriate information security policy and culture.[3]

Information security, its essence and attributes

Colloquially, information security is defined as a desired state of harmony and absence of threats. In operational/processing terms, it is a set of processes aimed at defining, achieving and maintaining an assumed level of information security attributes, that is, confidentiality, integrity and availability of information. In ICT systems, accountability, authenticity and reliability are additionally taken into account. A breach of one of the security aspects, i.e. confidentiality, availability or integrity, can lead to huge losses and even bankruptcy.[4]

For information security, the key is the proper identification of threats, vulnerabilities and also the assessment of risk and the application of appropriate safeguards to bring this risk down to an acceptable level. There are no two identical types of information. Each type of information has its own characteristics and is accompanied by different threats. Consequently, it is impossible to apply identical safeguards to different types of information. The level of information security is therefore a product of the exposure and safeguards against them, and the threats and defences against them. Security as a characteristic of information is not binary, but a continuous characteristic. The basis for understanding the role of information security is therefore to understand the definitions of the basic terms that define it. Currently, according to ISO/IEC 27001: 2005 Information Security Management System, information security is "the maintenance

2 Yourdon, E., *Wojna na bity*, Wydawnictwo Naukowo-Techniczne, Warszawa 2004.

3 Fehler, W., *O pojęciu bezpieczeństwa informacyjnego*, [in:] *Bezpieczeństwo informacyjne w XXI wieku*, M. Kubiak, S. Topolewski (eds.), Siedlce–Warszawa 2016; Lidermann, K., *Bezpieczeństwo informacyjne. Nowe wyzwania*, Wydawnictwo Naukowe PWN, Warszawa 2017.

4 Zawistowski, T., *Bezpieczeństwo informacji. Suplement*, Fundacja Rozwoju Demokracji Lokalnej, Warszawa 2011.

of the confidentiality, integrity and availability of information; additionally and other properties such as authenticity, accountability, non-repudiation and trustworthiness may be included." The increased awareness of the importance of information and its security is reflected in the dynamic development of international standards for information security management systems and the growing interest in them.

Thus, following researchers of this problem, I treat information security as a complex of undertakings designed to ensure the security of the information environment, as well as its formation, use and development in the interests of citizens, organisations and the state. The area of scientific inquiry and exchange of experience in the field of information security is not only people, information, information and communication processes and technologies, but also the infosphere itself, which is exposed to both intentional and unintentional attacks, the infosphere in which there is a constant information battle. Its defence is also carried out in the space of permanent education of the whole of society.

Information security concerns basically all characteristics of information, including such characteristics as relevance, accuracy, timeliness, completeness, consistency, appropriateness of form, accessibility, unambiguity, credibility, communicability, reliability, flexibility, redundancy, usefulness, complexity, naturalness, semantic compatibility, structural compatibility, verifiability and variability reputation.[5] It also concerns the functions performed by information. After all, information is a commodity, and often of a strategic nature, a basic element of business processes, a tool for controlling processes in automated information and search systems.[6] It is therefore not surprising that information is most often protected by law or concluded contracts.[7]

Information security is attributed with the following attributes: confidentiality, authenticity, availability, integrity (of data, system), accountability, reliability.[8] The components of information security are therefore physical security, personal/organisational security, ICT security and legal security.

The literature identifies three pillars of information security. These are confidentiality, integrity and availability. These are the cornerstones of so-called strong information protection that form the foundation of the information security infrastructure.

Information security is the practice of protecting information to prevent unauthorised access, use and disclosure. It includes the implementation of policies and procedures that are designed to protect information and help prevent data loss or theft. Information security is a set of security tools and procedures that broadly protect a company's confidential information from misuse, unauthorised access, disruption or destruction.

---

5 Czerwiński, A., Krzesaj, M., *Wybrane zagadnienia oceny jakości systemu informacyjnego w sieci WWW*, Uniwersytet Opolski, Opole 2007, pp. 49–50.

6 Hetmański, M., *Świat informacji*, Wydawnictwo Difin, Warszawa 2015.

7 Klimek, G., *Bezpieczeństwo informacji w perspektywie rozwoju Internetu rzeczy*, [in:] *Informacja – dobro publiczne czy prywatne?*, A. Czerwiński, A. Jańdziak, M. Krzesaj (eds.), Wydawnictwo Uniwersytetu Opolskiego, Opole 2016.

8 Białas, A., *Bezpieczeństwo informacji i usług w nowoczesnej instytucji i firmie*, Wydawnictwo Naukowo-Techniczne, Warszawa 2007, p. 34.

The EN ISO 27001 standard identifies three basic attributes of information: confidentiality, integrity and availability. Information security assurance focuses on securing these three aspects through information hiding, encryption and coding.

An information security management system is an operational strategy to ensure that information is properly protected. This strategy is intended to ensure that the actions and procedures taken are continuously improved in order to optimise the risks associated with a breach of confidentiality.

Information security risks

Threats to information security arise, among other things, as a result of the creation/broadcasting/reception of information by incompetent, biased, uno.eliable persons; targeting of information to the wrong audience; manipulation of information; slowing down the process of information reaching the recipient; destruction of trust in information; relativisation of truth and uncontrolled development of artificial intelligence (chatGPT-4, BING app, DALL-E); carelessness about the quality of information; populism; promotion of a particular ideology; hypocrisy of the sender; emotional rather than rational treatment of information.[9]

Threats to information security are also threats in cyberspace, such as information pollution, an unprecedented scale of information manipulation, information distortion and information inflation. Information bubbles, hate speech, post-truth, fake news, espionage and cyber-terrorism are also threats to information security.

Information security and protection measures should consist of protecting information from unauthorised human actions, human and organisational errors, hardware failures and software defects, the effects of disasters and terrorist actions.

Countermeasures include:

- attention to information balance and sustainability of the information environment;
- individual information management as a defence tool against threats on the Web;
- multiplication/duplication of information, but without intrusive propaganda and advertising.

Abuses in this subject are countered by: information ethics, information law, information etiquette, information education, information culture and information ecology. An essential factor and foundation of information security in everyday life is information culture,[10] mutual trust between people and trust in information.[11]

---

[9] Pala, M., *Współczesne zagrożenia dla bezpieczeństwa informacyjnego*, [in:] *Bezpieczeństwo informacyjne w XXI wieku*, M. Kubiak, S. Topolewski (eds.), Siedlce–Warszawa 2016.

[10] Kisilowska, M., *Kultura informacji*, Wydawnictwo Stowarzyszenia Bibliotekarzy Polskich, Warszawa 2016.

[11] Sztompka, P., *Zaufanie fundament społeczeństwa*, Wydawnictwo Znak, Kraków 2007; *Vademecum bezpieczeństwa informacyjnego*, vol. 1–2, O. Wasiuta, R. Klepka (eds.), Kraków 2019.

"Green" information security

Information balance and the sustainability of the human information environment as well as individual information management are tools for defence against threats on the Web.

It is also effective information security management. Information security management is particularly concerned with the secure execution of information processes such as: generating and acquiring information; collecting and storing information; processing information; sharing, distributing and disseminating information. Information security management, therefore, is primarily the appropriate control of the course of the aforementioned information processes aimed at optimising them.

In situations of threat, which can be caused by both internal factors (linguistic phenomena, changes in function and meaning) and external factors (extra-linguistic phenomena and information obsolescence), information protection is particularly important.

As such, information protection is primarily concerned with its attributes: secrecy, integrity, availability, accountability, non-repudiation, authenticity.[12] Dangerous information is false information that objectifies people. Safe information (green information), on the other hand, is "pure" (reliable), true, objective and complete information.

Information ecology, which offers solutions to optimise this process in accordance with the needs and possibilities of information users (senders, intermediaries and receivers),[13] is therefore a response to the contemporary problems of the communication process in its broadest sense, including information. Information security is a secure human being. Hence, it is necessary to consider the application of principles of prevention, hygiene and a kind of information diet, as well as the need to anticipate the consequences of one's own decisions in terms of influencing the information homeostasis of one's own body and others. The key to information ecology is to change mentalities/attitudes and build public awareness on the subject.

Information ecology proposes in this respect a practical activity consisting of:

- basing information policy on an appropriate and broad understanding of it;
- nurturing human information consciousness as an essential element in information processes;
- protecting people from being objectified by means of information (manipulation);
- developing people's information competence;
- educating people to be responsible for creating/generating, processing, disseminating and using information;
- balancing human development in a world of technology and information;

---

12 Liderman, K., *Bezpieczeństwo informacyjne*, Wydawnictwo Naukowe PWN, Warszawa 2012, p. 19.

13 Górski, A., *Informacja naukowa na tle przeobrażeń procesów komunikacji społecznej i jako wyzwanie gospodarki rynkowej*, Uniwersytet Szczeciński, Szczecin 1997.

– the skilful use of information to build individual and collective knowledge for the individual and common good of humanity;[14]
– managing information security in the human information environment.

Information, from the point of view information theory, is safe when:
– the creators of the information are competent, objective and reliable persons;
– is "immune" to all sorts of differing interpretations;
– is difficult to distort (e.g. scientific information);
– is not "long-winded";
– is provided with context;
– is not too redundant;
– is appropriately preserved in content and form;
– is made available/disseminated in an appropriate manner (on an appropriate channel);
– reaches the right audience.

Information education and information culture can be a kind of remedy to these problems.[15] Appropriate education and the nurturing of humanistic values are the most effective ways to counter information security threats. The lack of moral and social order and the tensions caused by the free market and the globalisation of capital rather than values force the protection of information as a commodity. Information is, after all, a commodity/product/value subject to special protection. The fragmentation of information and knowledge is becoming a worrying phenomenon. It is therefore necessary to introduce values into education, such as the feeling that the individual is part of humanity and not just the nation, moving away from Eurocentrism, and promoting tolerance, even though this is contrary to the neo-liberal economic model.[16]

Infoeducation is a new educational area in the field of information security, which allows the formation and improvement of information competences, the formation of social awareness of new opportunities and threats concerning information and the technologies of its generation, dissemination and reception, which is particularly important in connection with the dynamic development of the technological possibilities of digital media and the formation of a completely new quality of the human information environment.[17]

---

[14] Babik, W., *Ekologia informacji*, Wydawnictwo Uniwersytetu Jagiellońskiego, Kraków 2014, p. 138.

[15] Babik, W., *Kultura informacyjna – spojrzenie z punktu widzenia ekologii informacji*, „Bibliotheca Nostra. Śląski Kwartalnik Naukowy" 2012, no 2(28).

[16] *Ibidem*.

[17] Batorowska, H., *Bezpieczeństwo informacyjne w dyskurskie naukowym – kierunki badań*, [in:] *Bezpieczeństwo informacyjne w dyskursie naukowym*, H. Batorowska, E. Musiał (eds.), Kraków 2017.

Conclusions

The selected problems of information security highlighted in the article indicate, among other things, the new role and place of the global transformations currently taking place in the world of information, which have a great impact both on information itself and on human functioning in the information world. Information security is an important problem for society and the contemporary information world, not only of an epistemological (theoretical) nature, but also of a practical one. It is therefore not surprising that it has become the subject of a separate academic discipline. It would, therefore, be very useful to use the theoretical thought and actions proposed by information ecology in efforts to promote information and human security in the contemporary world. Its pronouncement is timeless and has a universal dimension. On the path of searching for new ways of human functioning in the modern world, information should be a kind of secure social keystone creating a secure information environment that is a meeting place for people, data sets and information services.[18] Information security can be ensured not only by consistent and courageous decisions on adequate data protection and copyright compliance, but above all by awareness of responsibility for information and an information security ecoculture built on it, which can help to avoid the so-called information stupidity and should be a permanent reference point for all information activities of humans, institutions and organisations.[19] Information security is one of the security dimensions in such questioning.

The key to ensuring information security is to quickly define the sources of potential threats and take action appropriate to counter the threat. It is important to be able to take appropriate action to prevent information security threats in a given area. Identifying information security threats and taking effective countermeasures is a skill without which it is difficult to function in an increasingly fast-paced information-based society.

An ecological approach to information forms the basis for the security of the information society and the knowledge economy. An element of information security culture is not only the ability to recognise a threat, but also to take appropriate action in response. These two elements also define the mental dimension of information security culture.

---

[18] Bednarek, J., *Społeczne kompetencje medialno-informacyjne w kontekście bezpieczeństwa w cyberprzestrzeni i świata wirtualnego*, [in:] *Człowiek w obliczu szans cyberprzestrzeni i świata wirtualnego*, J. Bednarek (ed.), Wydawnictwo Difin, Warszawa 2014.

[19] Materska, K., *Informacja w organizacjach społeczeństwa wiedzy*, Wydawnictwo Stowarzyszenia Bibliotekarzy Polskich, Warszawa 2017.

Bibliography

Babik, W., *Ekologia informacji*, Wydawnictwo Uniwersytetu Jagiellońskiego, Kraków 2014.

Babik, W., *Kultura informacyjna – spojrzenie z punktu widzenia ekologii informacji*, „Bibliotheca Nostra. Śląski Kwartalnik Naukowy" 2012, no. 2(28).

Batorowska, H., *Od alfabetyzacji informacyjnej do kultury informacyjnej*, Wydawnictwo Stowarzyszenia Bibliotekarzy Polskich, Warszawa 2012.

Batorowska, H., *Bezpieczeństwo informacyjne w dyskurskie naukowym – kierunki badań*, [in:] *Bezpieczeństwo informacyjne w dyskursie naukowym*, H. Batorowska, E. Musiał (eds.), Kraków 2017.

Bednarek, J., *Społeczne kompetencje medialno-informacyjne w kontekście bezpieczeństwa w cyberprzestrzeni i świata wirtualnego*, [in:] *Człowiek w obliczu szans cyberprzestrzeni i świata wirtualnego*, J. Bednarek (ed.), Wydanictwo Difin, Warszawa 2014.

Białas, A., *Bezpieczeństwo informacji i usług w nowoczesnej instytucji i firmie*, Wydawnictwo Naukowo-Techniczne, Warszawa 2007.

Czerwiński, A., Krzesaj, M., *Wybrane zagadnienia oceny jakości systemu informacyjnego w sieci WWW*, Wydawnictwo Uniwersytetu Opolskiego, Opole 2007.

Fehler, W., *O pojęciu bezpieczeństwa informacyjnego*, [in:] *Bezpieczeństwo informacyjne w XXI wieku*, M. Kubiak, S. Topolewski, (eds.), Wydawnictwo Uniwersytetu Przyrodniczo-Humanistycznego w Siedlcach, Siedlce–Warszawa 2016.

Górski, A., *Informacja naukowa na tle przeobrażeń procesów komunikacji społecznej i jako wyzwanie gospodarki rynkowej*, Uniwersytet Szczeciński, Szczecin 1997.

Hetmański, M., *Świat informacji*, Wydawnictwo Difin, Warszawa 2015.

Kisilowska, M., *Kultura informacji*, Stowarzyszenia Bibliotekarzy Polskich, Warszawa 2016.

Klimek, G., *Bezpieczeństwo informacji w perspektywie rozwoju Internetu rzeczy*, [in:] *Informacja – dobro publiczne czy prywatne?*, A. Czerwiński, A. Jańdziak, M. Krzesaj (eds.), Wydawnictwo Uniwersytetu Opolskiego, Opole 2016.

Kwieciński, M., *Bezpieczeństwo informacji i biznesu. Zagadnienia wybrane*, Krakowskie Towarzystwo Edukacyjne, Oficyna Wydawnicza Krakowskiej Akademii im. Andrzeja Frycza Modrzewskiego, Kraków 2010.

Liderman, K., *Bezpieczeństwo informacyjne,* Wydawnictwo Naukowe PWN, Warszawa 2012.

Lidermann, K., *Bezpieczeństwo informacyjne. Nowe wyzwania*, Wydawnictwo Naukowe PWN, Warszawa 2017.

Materska, K., *Informacja w organizacjach społeczeństwa wiedzy*, Wydawnictwo Stowarzyszenia Bibliotekarzy Polskich, Warszawa 2017.

Pala, M., *Współczesne zagrożenia dla bezpieczeństwa informacyjnego*, [in:] *Bezpieczeństwo informacyjne w XXI wieku*, M. Kubiak, S. Topolewski (eds.), Wydawnictwo Uniwersytetu Przyrodniczo-Humanistycznego w Siedlcach, Siedlce–Warszawa 2016.

Sztompka, P., *Zaufanie fundament społeczeństwa*, Wydawnictwo Znak, Kraków 2007.

Vademecum bezpieczeństwa informacyjnego, vol. 1–2, O. Wasiuta, R. Klepka (eds.), Kraków 2019.

Yourdon, E., *Wojna na bity*, Wydawnictwo Naukowo-Techniczne, Warszawa 2004.

Wawak, T. (ed.), *Zarządzanie bezpieczeństwem informacji i programami antykorupcyjnymi*, Wydawnictwo Wyższej Szkoły Administracji w Bielsku-Białej, Bielsko-Biała 2007.

Zawistowski, T., *Bezpieczeństwo informacji. Suplement*, Fundacja Rozwoju Demokracji Lokalnej, Warszawa 2011.

Summary

In view of the threats and challenges in the sphere of information security existing in the modern world and especially on the Internet, information ecology, including info-ecological principles of information security, is of particular importance. In this view, the basis of information security – in addition to ethics and law – is education and information culture, forming an appropriate level of information maturity based on information awareness and based on responsibility and trust in information. Undoubtedly, this is also fostered by the practical implementation of the concept of sustainable formation and development of the information environment, both on an individual (anthropospheric), local and global scale. Thus, information ecology contributes and helps both in the theoretical sphere and in the practical sphere to shape the information security awareness and culture that is so necessary and even indispensable nowadays.