UDC 351.82

MECHANISMS OF PUBLIC MANAGEMENT IN THE PERSONAL DATA PROTECTION IN CYBER PHYSICAL SYSTEMS

KHLAPONIN D.,
postgraduate,
Institute of personnel training of the State Employment Service of Ukraine

У статті аналізуються питання захисту персональних даних відповідно до Регламенту (ЄС) 2016/679 Європейського Парламенту та Ради від 27 квітня 2016 року про захист фізичних осіб у зв'язку з обробкою персональних даних та про вільне переміщення таких даних та скасування Директиви 95/46/ЄС та відповідно до Закону України «Про захист персональних даних» [4] як невід'ємної частини безпечного, надійного, стійкого, конфіденційного функціонування кіберфізичних систем в таких сферах, як розумне виробництво, керування дорожнім рухом, енергетика із акцентом в сфері охорони здоров'я. Проаналізовані різноманітні елементи обробки персональних даних, умови законної обробки персональних даних, фундаментальні права і свободи суб'єкта персональних даних з окремими виключеннями, обов'язки наглядового органу, контролера даних та розпорядника даних відповідно до Регламенту у порівнянні із правовим статусом володільця персональних даних та розпорядника персональних даних відповідно до Закону [4]. Також проведено порівняння прав певних юридичних осіб та асоціацій щодо підготовки кодексів поведінки у сфері захисту персональних даних з відповідними правами професійних, самоврядних асоціацій відповідно до [4]. Крім цього проаналізовані повноваження Уповноваженого Верховної Ради України з прав людини та надані пропозиції щодо додаткових повноважень Уповноваженого та інших механізмів державного управління, які стосуються захисту персональних даних в сфері кіберфізичних систем. Надані пропозиції щодо покладання адміністративної відповідальності у формі штрафів на володільця персональних даних та розпорядника персональних даних, а також оператора кіберфізичної системи.

Ключові слова: *захист персональних даних, суб'єкт персональних даних, контролер даних, розпорядник даних, кіберфізична система, електронна система охорони здоров'я, оператор кіберфізичної системи.*

В статье анализируются вопросы защиты персональных данных в соответствии с Регламентом (ЕС) 2016/679 Европейского Парламента и Совета от 27 апреля 2016 года о защите физических лиц в связи с обработкой персональных данных и о свободном перемещении таких данных и отмене Директивы 95/46/ЕС и в соответствии с Законом Украины «О защите персональных данных» [4] как неотъемлемой части безопасного, надежного, устойчивого, конфиденциального функционирования киберфизических систем в таких сферах, как умное производство, управление дорожным движением, энергетика с акцентом в сфере здравоохранения. Проанализированы разнообразные

элементы обработки персональных данных, условия законной обработки персональных данных, фундаментальные права и свободы субъекта персональных данных с отдельными исключениями, обязанности органа надзора, контролера данных и распорядителя данных в соответствии с Регламентом в сравнении с правовым статусом владельца персональных данных и распорядителя персональных данных согласно с Законом [4]. Также проведено сравнение прав определенных юридических лиц и ассоциаций касательно подготовки кодексов поведения в сфере защиты персональных данных с соответствующими правами профессиональных, самоуправляемых ассоциаций в соответствии с Законом [4]. Кроме этого проанализированы полномочия Уполномоченного Верховного Совета Украины по правам человека и представлены предложения касательно дополнительных полномочий Уполномоченного и других механизмов государственного управления, которые касаются защиты персональных данных в сфере киберфизических систем. Представлены предложения о возложении административной ответственности в форме штрафов на владельца персональных данных и распорядителя персональных данных, а также оператора киберфизической системы.

Ключевые слова: *защита персональных данных, субъект персональных данных, контролер данных, распорядитель данных, киберфизическая система, электронная система здравоохранения, оператор киберфизической системы.*

The Article analyzes the issues of the personal data protection in accordance with the Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (Regulation) and in accordance with the Ukrainian Law "On the personal data protection" [4] as an integral part of secure, reliable, resilient, confidential cyber physical systems functioning in such fields as smart manufacturing, traffic management, energy with the emphasis on the healthcare. Various elements of the personal data processing are analyzed, the conditions of lawful processing, fundamental rights and freedoms of the personal data subject with certain exceptions are analyzed, the obligations of the supervisory authority, data controller and data processor according to the Regulation in comparison with the legal status of personal data possessor and personal data processor according to the Law [4] are assessed. Also the comparison of the rights of certain legal persons and associations to prepare codes of conduct in the field of the personal data protection with the relevant rights of the professional, self-governing associations according to the Law [4] is made. Besides the authority of the Commissioner of the Verkhovna Rada of Ukraine on human rights is analyzed and the propositions as to the additional authority of the Commissioner and other mechanisms of public management with regard to the personal data protection in the field of cyber physical systems are made. The propositions for imposing of administrative responsibility in the form of fines on the data possessor and the data processor as well as a CPS operator are made.

Keywords: *personal data protection, personal data subject, data controller, data processor, cyber physical system, the electronic healthcare system, cyber physical systems operator.*

The general articulation of the issue and its connection with the important research and practice tasks. More than ten years ago in the world has emerged the concept "cyber physical system" and till today cyber physical systems have developed in various fields such as smart manufacturing, energy (smart grid), traffic management, healthcare etc. Cyber physical systems are smart systems that include engineered interacting networks of physical and computational components [1]. The essential requirements to functioning of these systems are safety, security, reliability, resilience, confidentiality. Automated decision-making, including profiling in the personal data processing constitutes a significant part of cyber physical systems functioning. As the personal data is processed automatically, computations are performed in the "cloud" in the network of distant servers, there is a risk of various cyber threats and real cyber attacks on certain cyber physical system which may cause a damage or losses to the personal data subject as a result of unlawful destruction, use, alteration or disclosure of the personal data. The Ukrainian legislation does not contain the concept "cyber physical system". The unsolved problem in the Ukrainian legislation is the recognition of the personal data subject as a central element of any cyber physical system and the necessity of ensuring balance between the fundamental rights and freedoms of the personal data subject and the rights of the data possessors, data processors, data protection officials, the authority of the Commissioner of the Verkhovna Rada of Ukraine on human rights who gain access to the personal data by means of personal data subject consent. Thus the important issue is the clear definition of the responsibility of the data possessors, data processors, data protection officials as well as CPS operators with regard to the personal data protection and the necessity of determining the body which shall have the authority to impose administrative fines on the guilty person. The abovementioned features of cyber physical system characterize the topicality of the scientific research of the mechanisms of public management of cyber physical systems functioning and their normative-legal regulation as an element of public management.

The analysis of recent research and publications regarding the issues this Article deals with (identification of parts of the general problem that have not been previously addressed). In this Article the Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (Regulation) [5] is analyzed which is applied from 25 May 2018 and is binding in its entirety and directly applicable in all Member States. The comparative analysis of the Regulation with the Ukrainian Law [4] which refers to various elements of the processing of personal data in different processing systems, to the rights and obligations of the data controller, the data processor, the supervisory authority with regard to ensuring lawful, secure, confidential processing of personal data is made. The unsolved problem in the Ukrainian legislation is the recognition of the personal data subject as a central element of any cyber physical system and the necessity of ensuring balance between the fundamental rights and freedoms of the personal data subject and the rights of the data possessors, data processors, data protection officials, the authority of the supervisory authority who gain access to the personal data by means of personal data subject consent. Another unsolved problem is the issue who will bear responsibility in the instance of the accidental or unlawful loss, destruction, use, alteration, disclosure of personal data to

third parties without personal data subject consent and what body will have the authority to impose administrative fines or initiate criminal procedure against suspect in cases of incurred damages or losses to the personal data subject. The role of the Commissioner of the Verkhovna Rada of Ukraine on human rights in the protection of rights of personal data subject in the field of cyber physical systems functioning as well as the authority in case of any cyber attacks and cyber threat to the security of personal data should also be clearly defined.

The purpose of the Article. The purpose of the Article is to analyze the personal data protection in accordance with the Regulation [5] in comparison with the Law "On the personal data protection" [4]. This analysis is aimed at the revealing of the progressive provisions of the Regulation which refer to the various elements of the processing of personal data in different processing systems (including cyber physical systems), to the rights and obligations of the data controller, the data processor, the supervisory authority with regard to ensuring lawful, secure, confidential processing of personal data. Also the purpose of the Article is to analyze the authority of the Commissioner of the Verkhovna Rada of Ukraine on human rights and to suggest additional authority in personal data protection in the field of cyber physical systems functioning.

Presentation of the main research material. In the scientific paper [2] by the scientists of Riga Technical University the following definition of cyber-physical system is proposed: "Cyberphysical systems (CPSs) are complex engineering systems that rely on the integration of physical, computation, and communication processes to function".

CPSs integrate computing, communication, data storage with real world's objects and physical processes. All the above-mentioned processes must occur in real-time, in a safe, secure and efficient manner.

In this Article emphasis is made on the analysis of specifics of personal data protection in the area of medical cyber-physical systems.

CPS sensors generate the sensitive data that must be protected and shared only in a secure manner. The rapid development of wireless sensor networks, medical sensors and cloud computing systems makes cyber-physical systems impressive candidates for use in inpatient and outpatient health care improvement [2].

Health Level 7 is a group of standards for the exchange, integration, sharing, and retrieval of electronic health information [2]. Currently, there are no standards and regulations, which relate directly to healthcare cyber-physical systems.

In healthcare facilities only certified cyber-physical systems must be in use.

The Regulation [5] is applied from 25 May 2018. The Regulation indicates that it shall be binding in its entirety and directly applicable in all Member States.

Ukraine has adopted the Law "On the ratification of the Convention for the protection of individuals with regard to automatic processing of personal data and the Additional protocol to the Convention for the protection of individuals with regard to automatic processing of personal data with regard to the supervisory bodies and to the transborder flow of data" [3].

In accordance with the Law [3] the body which is imposed the authority according to the Article 13 of the Convention is the Commissioner of the Verkhovna Rada of Ukraine on human rights. In conformity with the Law [3] this Law enters into force simultaneously with the entrance into force of the Law [4] on 01 January 2011.

In accordance with the Law [4] this Law applies to the processing of personal data carried out in whole or in part with the use of automated means, as well as to the processing of personal data contained in the card index or intended to be added to the card index, using non-automated means. The same provision is stated in the Article 2 of the Regulation.

According to the Article 2 of the Law [4] personal data is the information or a set of information about an individual that is identified or can be specifically identified. According to the Article 4 of the Regulation [5] "personal data" means any information relating to an identified or identifiable natural person ("data subject"); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person.

In comparison with the definition of the concept "personal data" contained in the Regulation the definition of this concept contained in the Law is rather simplified. The factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of the natural person should be also taken into account in developing the definition of the concept "personal data".

The Article 2 of the Law [4] contains the concept "personal data processing" which consists of many elements and among others of the concept "depersonalization" and "dissemination", which in turn, includes the concept "realization". The concept "personal data depersonalization" means extracting information that allows you to directly or indirectly identify a person. The Regulation [5], on the other hand, does not contain concepts "personal data realization" and "depersonalization".

In accordance with Article 4 of the Regulation "pseudonymisation" means the processing of personal data in such a manner that the personal data can no longer be attributed to a specific data subject without the use of additional information, provided that such additional information is kept separately and is subject to technical and organizational measures to ensure that the personal data are not attributed to an identified or identifiable natural person [5].

The Ukrainian law [4] does not contain the concept "pseudonymisation", however to the author's opinion this concept is extremely important in personal data protection in different areas as well as in the operation of cyber physical systems. Therefore, the concept "personal data depersonalization" should be substituted in the Ukrainian law with the concept "pseudonymisation" with the abovementioned definition.

In accordance with the Article 4 of the Regulation [5] 'profiling' means any form of automated processing of personal data consisting of the use of personal data to evaluate certain personal aspects relating to a natural person, in particular to analyze or predict aspects concerning that natural person's performance at work, economic situation, health, personal preferences, interests, reliability, behavior, location or movements.

It can be concluded from the abovementioned concept that "profiling" can be performed in cyber physical systems in such areas as healthcare, energy (smart grid), traffic management etc. The Ukrainian law does not contain the concept "profiling". This concept should be introduced into the law with the abovementioned definition.

According to the Article 4 of the Regulation [5] “personal data breach” means a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to, personal data transmitted, stored or otherwise processed. The Ukrainian law does not contain the concept ‘‘personal data breach’’ and it should be introduced into the Law for the ensuring of better legal regulation of the personal data protection as a mechanism of public management.

In accordance with the Article 4 of the Law [4] the subjects of the relationship connected with the personal data are: personal data subject, personal data possessor, personal data processor, third party, Commissioner of the Verkhovna Rada of Ukraine on human rights.

There is a difference in meaning of the concept ‘processor’ in accordance with the Regulation and the concept “data processor” in accordance with the Ukrainian Law. According to the Regulation [5] the concept “processor” means a natural or legal person, public authority, agency or other body which processes personal data on behalf of the controller. According to the Law [4] the concept “data processor” means only a natural or legal person who is given by the possessor or by the legislation a right to process personal data on behalf of the possessor.

Article 5 of the Regulation [5] defines certain Principles relating to processing of personal data. It is indicated that personal data shall be: (a) processed lawfully, fairly and in a transparent manner in relation to the data subject (‘lawfulness, fairness and transparency’); (b) collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes (‘purpose limitation’); (c) adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed (‘data minimization’); (d) accurate and, where necessary, kept up to date; (‘accuracy’); (e) kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed; (‘storage limitation’);(f) processed in a manner that ensures appropriate security of the personal data, including protection against unauthorized or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organizational measures (‘integrity and confidentiality’).

All these principles are crucial to the processing of personal data in any kind of legal relationship between the natural and legal persons, public authority and other subjects as well as in the operation of cyber physical systems. However the principle “integrity and confidentiality” is one of the most important principles and is ensured by the appropriate technical characteristics in the design of CPS. If this principle is not ensured in the design of CPS these systems will be subject to cyber attacks of different levels of complexity with the subsequent damage to the secure, reliable, resilient functioning of CPS and confidential processing of the personal data will not be guaranteed.

In accordance with the Article 6 of the Regulation [5] processing shall be lawful only if and to the extent that at least one of the following applies: (a) the data subject has given consent to the processing of his or her personal data for one or more specific purposes; (b) processing is necessary for the performance of a contract to which the data subject is party or in order to take steps at the request of the data subject prior to entering into a contract; (c) processing is necessary for compliance with a legal obligation to which the controller is subject; (d) processing is necessary in order to protect the vital interests of the data subject or of another natural person; (e)

processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller.

In conformity with paragraph 1 of the Article 9 of the Regulation [5] processing of personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, and the processing of genetic data, biometric data for the purpose of uniquely identifying a natural person, data concerning health or data concerning a natural person's sex life or sexual orientation shall be prohibited. There is an exception from this rule according to paragraph 2 if processing is necessary for the purposes of preventive or occupational medicine, for the assessment of the working capacity of the employee, medical diagnosis, the provision of health or social care or treatment or the management of health or social care systems and services on the basis of Union or Member State law or pursuant to contract with a health professional.

Thus it can be concluded that personal data may be processed in case when a patient is provided a distant medical supervision by means of special cyber physical systems on the basis of Union or Member State law or pursuant to contract with a health professional.

In accordance with paragraph 3 of the Article 9 of the Regulation [5] personal data referred to in paragraph 1 may be processed for the purposes referred to in point (h) of paragraph 2 when those data are processed by or under the responsibility of a professional subject to the obligation of professional secrecy under Union or Member State law or rules established by national competent bodies or by another person also subject to an obligation of secrecy under Union or Member State law or rules established by national competent bodies.

That means the processing of genetic data, biometric data for the purpose of uniquely identifying a natural person, data concerning health for the purpose of the management of health or social care systems (which can be considered cyber physical systems) and services may only be carried out by or under the responsibility of a medical professional who has an obligation not to disclose special categories of personal data.

Article 9 of the Regulation also contains the provision that Paragraph 1 shall not apply if processing is necessary for reasons of public interest in the area of public health, such as protecting against serious cross-border threats to health or ensuring high standards of quality and safety of health care and of medicinal products or medical devices, on the basis of Union or Member State law which provides for suitable and specific measures to safeguard the rights and freedoms of the data subject, in particular professional secrecy [5].

According to the Article 16 of the Regulation [5] the data subject shall have the right to obtain from the controller without undue delay the rectification of inaccurate personal data concerning him or her. The Ukrainian law does not contain the concept rectification of personal data within the concept data processing.

The Ukrainian Law [4] contains the general requirements to the personal data processing and the special requirements to the personal data processing.

According to the Article 6 of the Law [4] the general requirements to the personal data processing are: the personal data shall be accurate, authentic and shall be renewed if necessary with regard to the purpose of their processing; the composition and content of the personal data shall be relevant, adequate and not excessive with

regard to the defined purpose of their processing; the processing of confidential information about the natural person is not allowed without his or her consent with the exceptions defined by the legislation and only in the interests of national security, economic welfare and the rights of people; the personal data are processed in a form that allows the identification of the relevant natural person not longer than it is required for the legal purpose of their collection or further processing.

The special requirements to the personal data processing are defined in the Article 7 of the Law [4]. In conformity with the Article 7 of the Law the processing of the personal data with regard to the racial or ethnic origin, political, religious or philosophical beliefs, political parties or trade union membership, conviction of a criminal punishment and data concerning health, sex life, genetic data, biometric data shall be prohibited.

The provisions of paragraph 1 of this Article shall not apply if the processing of personal data: 1) is carried out on condition that the personal data subject has given an unambiguous consent to the processing of such data; 2) is required for the justification, satisfaction or defence of legal claims; 3) is necessary for the purpose of healthcare, establishment of a medical diagnosis, for the provision of care or treatment or the provision of medical services, the functioning of the electronic healthcare system, provided that such data are processed by a medical worker or other person of the healthcare institution or an entrepreneur who has received a license for the conduct of economic activity in medical practice and by his or her employees who are imposed obligations for the ensuring of the personal data protection and who are subject to the legislation on the medical secrecy, 4) refers to data which were clearly made public by the personal data subject.

From the abovementioned follows that the processing of data concerning health, genetic data, biometric data and other special categories of personal data shall be allowed, among other instances, if it is required for the establishment of a medical diagnosis, the functioning of the electronic healthcare system which can be considered as a special CPS for the provision of distant medical supervision. The essential requirement of such processing of the personal data is the obligation of medical worker not to disclose or otherwise unlawfully use the personal data of a patient (who is a personal data subject). Today such means of distant medical assistance is called telemedicine.

In conformity with Paragraph 1 of the Article 22 of the Regulation [5,43] the data subject shall have the right not to be subject to a decision based solely on automated processing, including profiling, which produces legal effects concerning him or her or similarly significantly affects him or her. Paragraph 1 shall not apply if the decision: (a) is necessary for entering into, or performance of, a contract between the data subject and a data controller; (b) is authorized by Union or Member State law to which the controller is subject and which also lays down suitable measures to safeguard the data subject's rights and freedoms and legitimate interests; or (c) is based on the data subject's explicit consent.

The similar provision is laid down in the Article 8 of the Law [4] which emphasizes that the personal data subject shall have the right to the protection from the automated decision which produces legal effects concerning him or her.

For instance, in CPS personal data is automatically processed in order to fulfil the functions of CPS in certain areas of deployment. Automated processing and

computation are performed in the cloud (with many distant servers) and are inevitable for the appropriate functioning of CPS. However, these operations in the cloud may constitute a risk of personal data breach and to avoid such consequences an appropriate technical measures should be taken by the CPS operator in order to ensure security and confidentiality of the personal data.

In accordance with Article 32 of the Regulation [5] taking into account the state of the art, the costs of implementation and the nature, scope, context and purposes of processing as well as the risk of varying likelihood and severity for the rights and freedoms of natural persons, the controller and the processor shall implement appropriate technical and organizational measures to ensure a level of security appropriate to the risk, including inter alia as appropriate: (a) the pseudonymisation and encryption of personal data; (b) the ability to ensure the ongoing confidentiality, integrity, availability and resilience of processing systems and services; (c) the ability to restore the availability and access to personal data in a timely manner in the event of a physical or technical incident; (d) a process for regularly testing, assessing and evaluating the effectiveness of technical and organizational measures for ensuring the security of the processing.

In accordance with paragraph 3 of the Article 32 of the Regulation adherence to an approved code of conduct as referred to in Article 40 or an approved certification mechanism as referred to in Article 42 may be used as an element by which to demonstrate compliance with the requirements set out in paragraph 1 of this Article.

On the basis of the abovementioned it can be concluded that the controller and the processor implement technical and organizational measures to ensure a level of security of the personal data which are similar to the technical and organizational measures to ensure security of the personal data which have to be implemented by the CPS operator. In particular, it refers to the ability to ensure the ongoing confidentiality, integrity, availability and resilience of processing systems (which may be considered as CPSs).

According to the Article 40 of the Regulation the Member States, the supervisory authorities, the European Data Protection Board and the European Commission shall encourage the drawing up of codes of conduct intended to contribute to the proper application of this Regulation, taking account of the specific features of the various processing sectors and the specific needs of micro, small and medium-sized enterprises.

In accordance with paragraph 2 of the Article 40 of the Regulation [5] associations and other bodies representing categories of controllers or processors may prepare codes of conduct, or amend or extend such codes, for the purpose of specifying the application of this Regulation, such as with regard to: 1) fair and transparent processing; 2) the legitimate interests pursued by controllers in specific contexts; 3) the collection of personal data; 4) the pseudonymisation of personal data; 5) the information provided to the public and to data subjects; 6) the exercise of the rights of data subjects; 7) the notification of personal data breaches to supervisory authorities and the communication of such personal data breaches to data subjects; or 8) out-of-court proceedings and other dispute resolution procedures for resolving disputes between controllers and data subjects with regard to processing.

According to paragraph 5 of the Article 40 of the Regulation [5] associations and other bodies referred to in paragraph 2 of this Article which intend to prepare a

code of conduct or to amend or extend an existing code shall submit the draft code, amendment or extension to the supervisory authority which is competent pursuant to Article 55. The supervisory authority shall provide an opinion on whether the draft code, amendment or extension complies with this Regulation and shall approve that draft code, amendment or extension if it finds that it provides sufficient appropriate safeguards. Where the draft code, or amendment or extension is approved in accordance with paragraph 5, and where the code of conduct concerned does not relate to processing activities in several Member States, the supervisory authority shall register and publish the code.

In accordance with the Article 27 of the Law [4] professional, self-governing and other public associations or legal entities may develop codes of conduct for the purpose of ensuring effective protection of the rights of the data subjects, the observance of the legislation on the protection of personal data taking into account the specifics of the processing of personal data in various spheres. In developing such a code of conduct or making amendments to it, the relevant association or legal entity may apply for a conclusion to the Commissioner.

The features of the Article 27 of the Law [4] which distinguish it from the Article 40 of the Regulation [5] are as follows: according to the Article 40 of the Regulation associations and other bodies representing categories of controllers or processors have the obligation to submit the draft code, amendment or extension to the supervisory authority and according to the Article 27 of the Law the relevant association or legal entity have the right to apply for a conclusion to the Commissioner; according to the Article 40 of the Regulation the supervisory authority has the obligation to provide an opinion on whether the draft code, amendment or extension complies with this Regulation and has the obligation to approve that draft code, amendment or extension and according to the Article 27 of the Law the Commissioner of the Verkhovna Rada of Ukraine on human rights has the authority to provide, upon appeal of professional, self-governing and other public associations or legal entities, conclusions regarding draft codes of conduct in the field of the personal data protection and amendments to them.

In accordance with the Article 23 of the Law [4] the Commissioner of the Verkhovna Rada of Ukraine on human rights has the following authority in the field of the personal data protection: 1) to receive propositions, complaints of the natural and legal persons on the issues of the personal data protection and to make a decisions with regard to them; 2) to carry out on the appeal or on his or her own initiative external or internal, planned or unplanned audit (control) of the possessors or processors of the personal data; 3) to receive on his or her demand and to have access to any data (documents) of the possessors or processors which are required for ensuring of the personal data protection; 4) to approve the normative-legal acts in the field of the personal data protection; 5) as a result of the audit or appeal to issue mandatory demands (orders) for the prevention or elimination of the violation of the personal data protection legislation; 6) to appeal with propositions to the Verkhovna Rada of Ukraine, the President of Ukraine, the Cabinet of ministers of Ukraine with regard to the adoption, making amendments to the normative-legal acts in the field of the personal data protection; 7) to provide on the appeal of the professional, self-governing or other public associations and legal persons the conclusions on the draft codes in the field of the personal data protection and alterations to them; 8) to form

administrative responsibility protocols and to send them to court according to the legislation.

Accordingly to the Commissioner of the Verkhovna Rada of Ukraine on human rights has a vast authority in the field of the personal data protection, however the scope of the rights and obligations of the Commissioner should be reviewed and expanded with regard to the personal data protection in CPS.

Conclusions and the prospects of the further research. According to the definition of the concept "controller" in the Regulation [4] it has the same meaning as the concept "possessor" in the Ukrainian Law [4].

On the basis of the abovementioned the controller as well as the possessor shall ensure the appropriate safeguards to the personal data protection, which may include encryption or pseudonymisation. The essential requirement to the security and confidentiality of the personal data in any kind of processing systems (including CPS) is that different types of personal data relating to a relevant natural person shall be kept separately in order to avoid easy establishment of that person and an obligation of professional secrecy shall be strictly observed by the controller as well as the possessor.

The possessor as well as the controller shall appoint a data protection official who has a required level of expertise in order to assess the observance of the fundamental rights and freedoms of the personal data subject and in case of any infringement of these rights and freedoms shall demand the action to be taken by the possessor to stop the unlawful processing of the personal data and to return to the required state of processing of the personal data.

The responsibility of the possessor and processor as well as of CPS operator for the personal data breach shall be clearly defined and administrative fines shall be imposed on the guilty natural or legal person. A criterion shall be developed for imposing a certain type of administrative fines and the appropriate amendments shall be made to the Code on the administrative offences of Ukraine as the mechanism of public management, in particular in the field of CPS functioning.

Automated decision-making, including profiling in the personal data processing constitutes a significant part of CPS functioning. Taking into account the existence of various types of CPS, which are not interoperable, in different fields, such as energy, manufacturing, traffic management, healthcare, a specific codes of conduct should be developed in every field of their deployment. And the workers with the sufficient level of expertise have to ensure reliable, secure, resilient, confidential functioning of the relevant CPS. The state, in turn, has to develop a typical principles of any CPS functioning and to ensure training of highly qualified workers on the newly created working places.

CPS operator as a data possessor or a data processor shall ensure by all technical and organizational means the appropriate level of confidentiality in the CPS functioning. The Commissioner of the Verkhovna Rada of Ukraine on human rights shall be entitled with a right and an authority to assess the level of the protection of personal data in CPS. Also the Commissioner shall include the report on the state of the observance of the personal data protection in CPS into the annual report of the Commissioner.

Consequently we can come to a conclusion that the data subject is the central element of any cyber physical system functioning and his or her fundamental rights

and freedoms are strictly observed in any developed country of the world and in some cases even if the data subject has given his or her consent to the processing of special categories of personal data the prohibition to their processing cannot be lifted.

Further research is required in the field of the personal data protection with the emphasis on the peculiarities of functioning of various CPS with a strict cooperation of CPS operators, personal data subjects, data controllers and data processors, data protection officials, supervisory authorities with optimization of interrelation of the obligations of professional secrecy of certain subjects with the ensuring of availability of high quality services.

References:

1. Framework for Cyber-Physical Systems Release 1.0 May 2016 CPS Public Working Group. Retrieved from www.nist.gov.

2. State of the Art in the Healthcare Cyber-physical Systems. Information Technology and Management Science. doi: 10.1515/itms-2014-0019. 2014/17. URL: https://ortus.rtu.lv/science/en/publications/20065-State+of+the+Art+in+the+Healthcare+Cyber-physical+Systems.

3. Про ратифікацію Конвенції про захист осіб у зв'язку з автоматизованою обробкою персональних даних та Додаткового протоколу до Конвенції про захист осіб у зв'язку з автоматизованою обробкою персональних даних стосовно органів нагляду та транскордонних потоків даних: Закон України від 6.07.2010 р. N 2438-VI. URL: http://zakon3.rada.gov.ua/laws/show/2438-17.

4. Про захист персональних даних: Закон України від 1.06.2010 р. № 2297-VI. URL: http://zakon3.rada.gov.ua/laws/show/2297-17.

5. The Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC. Official Journal of the European Union. URL: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex%3A32016R0679.

The Article analyzes the issues of the personal data protection in accordance with the Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC and in accordance with the Ukrainian Law “On the personal data protection” as an integral part of secure, reliable, resilient, confidential cyber physical systems functioning in such fields (industries) as smart manufacturing, traffic management, energy (smart grid) with the emphasis on the healthcare.

Various elements of the personal data processing are analyzed, the conditions of lawful processing, fundamental rights and freedoms of the personal data subject with certain exceptions are analyzed, the obligations of the supervisory authority, data controller and data processor according to the Regulation in comparison with the legal status of personal data possessor and personal data processor according to the Ukrainian Law are assessed.

The controller as well as the personal data possessor shall ensure the

appropriate safeguards to the personal data protection, which may include encryption or pseudonymisation.

Also the comparison of the rights of certain legal persons and associations to prepare codes of conduct in the field of the personal data protection according with the Regulation with the relevant rights of the professional, self-governing associations is made according to the Ukrainian Law.

Cyber physical systems are smart systems that include engineered interacting networks of physical and computational components. The essential requirements to functioning of these systems are safety, security, reliability, resilience, confidentiality.

Automated decision-making, including profiling in the personal data processing constitutes a significant part of cyber physical systems functioning. There is a risk of various cyber threats and real cyber attacks on certain cyber physical system which may cause a damage or losses to the personal data subject as a result of unlawful destruction, use, alteration or disclosure of the personal data.

The unsolved problem in the Ukrainian legislation is the recognition of the personal data subject as a central element of any cyber physical system and the neccessity of ensuring balance between the fundamental rights and freedoms of the personal data subject and the rights of the personal data possessors, personal data processors, data protection officials, the authority of the Commissioner of the Verkhovna Rada of Ukraine on human rights who gain access to the personal data by means of personal data subject consent.

The responsibility of the personal data possessor and personal data processor as well as of CPS operator for the personal data breach shall be clearly defined and administrative fines shall be imposed on the guilty natural or legal person.

A criterion shall be developed for imposing a certain type of administrative fines and the appropriate amendments shall be made to the Code on the administrative offences of Ukraine as the mechanism of public management, in particular in the field of cyber physical systems functioning.