UDC: 340:659.4.327.88 (477)

Lysenko Serhii Oleksiyovych,
PhD in Law, Associate professor, Associate professor of the Department of Security Management and Law Enforcement and Anti-Corruption Activities, Interregional Academy of Personnel Management, 03039, Kyiv, Str. Frometivska, 2, (044) 490 95 00, e-mail: crimeconsult@ukr.net
ORCID: 0000–0002–7050–5536

Лисенко Сергій Олексійович,
кандидат юридичних наук, доцент кафедри управління безпекою, правоохоронної та антикорупційної діяльності, Міжрегіональна Академія управління персоналом, 03039, м. Київ, вул. Фрометівська, 2, тел.: (044) 490 95 00, e-mail: crimeconsult@ukr.net
ORCID: 0000–0002–7050–5536

Лысенко Сергей Алексеевич,
кандидат юридических наук, доцент кафедры управления безопасностью, правоохранительной и антикоррупционной деятельности, Межрегиональная Академия управления персоналом, 03039, г. Киев, ул. Фрометовская, 2, тел.: (044) 490 95 00, e-mail: crimeconsult@ukr.net
ORCID: 0000–0002–7050–5536

SPECIAL THEORY OF ADMINISTRATIVE – LEGAL REGULATION OF INFORMATION SECURITY OF THE SOCIAL SYSTEMS

Abstract. The article deals with the principles of creating a special theory of administrative and legal regulation of information security, analyzes the process of its analogy with physical laws, analyzes the threats and dangers to interests and all information security that affect the process of modeling, determines the principles of constructing and researching models of information security of social systems.

It was noted that the administrative and legal regulation of information security is due to the need for state management of the processes of formation and use of information resources, the creation and application of information systems and the provision of information security of social systems. It is proved that to a large extent information security is caused by the need for administrative regulation of information relations in various spheres that form the system itself and maintain its integrity. It is determined that the administrative and legal basis of informa-

tion security of social systems should provide an ideal state of activity of subjects, system and its models. Selected concrete administrative and legal principles of information security, such as physical formulas, create its model. Of course, for each social system, the model of information security is individual. However, there are also general patterns of modeling, for example — the construction of the model should be based on the simple and optimal (as we are referred to by the flow of light), administrative and legal principles.

It is proved that high rates of development of information technologies, create new requirements to the sphere of security in general and to information security in particular. The reform of the legislation regulating activity in the field of information security should be based on the proper scientific theory. What is urgent is the need to create a General Security Theory, which would explain and regulate the set of processes of ensuring the safety of society.

Keywords: special theory, information security, modeling, administrative-legal regulation, safety of social systems.

СПЕЦІАЛЬНА ТЕОРІЯ АДМІНІСТРАТИВНО-ПРАВОВОГО РЕГУЛЮВАННЯ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ СОЦІАЛЬНИХ СИСТЕМ

Анотація. Розглянуто принципи створення спеціальної теорії адміністративно-правового регулювання інформаційної безпеки, досліджується процес її аналогії із фізичними законами, аналізуються загрози та небезпеки інтересам та всій інформаційній безпеці, що впливають на процес моделювання, визначаються принципи побудови та дослідження моделей інформаційної безпеки соціальних систем. Відмічено, що адміністративно-правове регулювання інформаційної безпеки обумовлено необхідністю державного управління процесами формування і використання інформаційних ресурсів, створення і застосування інформаційних систем і забезпечення інформаційної безпеки соціальних систем. Доведено, що у значній мірі інформаційна безпека обумовлена потребою адміністративного регулювання інформаційних відносин у різних сферах, що утворюють саму систему та підтримують її цілісність. Визначено, що адміністративно-правові засади інформаційної безпеки соціальних систем повинні забезпечувати ідеальний стан діяльності суб'єктів, системи та її моделей. Обрані конкретні адміністративно-правові засади інформаційної безпеки, на кшталт фізичних формул, створюють її модель. Звичайно, для кожної соціальної системи модель інформаційної безпеки є індивідуальною. Проте є і загальні закономірності моделювання, наприклад — побудова моделі повинна відбуватись на основі простих та оптимальних (як згадуваний нами потік світла), адміністративно-правових засад.

Доведено, що високі темпи розвитку інформаційних технологій породжують нові вимоги до сфери безпеки в цілому і до інформаційної безпеки зокрема. Реформування законодавства, що регулює діяльність у сфері інформаційної безпеки має відбуватись на базі належної наукової теорії.

Нагальною є потреба створення Загальної теорії безпеки всього, яка б пояснювала та регулювала сукупність процесів забезпечення безпеки суспільства.

Ключові слова: спеціальна теорія, інформаційна безпека, моделювання, адміністративно-правове регулювання, безпека соціальних систем.

СПЕЦИАЛЬНАЯ ТЕОРИЯ АДМИНИСТРАТИВНО-ПРАВОВОГО РЕГУЛИРОВАНИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ СОЦИАЛЬНЫХ СИСТЕМ

Аннотация. Рассмотрены принципы создания специальной теории административно-правового регулирования информационной безопасности, исследуется процесс ее аналогии с физическими законами, анализируются угрозы и опасности интересам и всей информационной безопасности, влияющие на процесс моделирования, определяются принципы построения и исследования моделей информационной безопасности социальных систем. Отмечено, что административно-правовое регулирование информационной безопасности обусловлено необходимостью государственного управления процессами формирования и использования информационных ресурсов, создание и применение информационных систем и обеспечения информационной безопасности социальных систем. Доказано, что в значительной степени информационная безопасность обусловлена потребностью административного регулирования информационных отношений в различных сферах, образуют саму систему и поддерживают ее целостность. Определено, что административно-правовые основы информационной безопасности социальных систем должны обеспечивать идеальное состояние деятельности субъектов, системы и ее моделей. Избранные конкретные административно-правовые основы информационной безопасности, вроде физических формул, создают ее модель. Конечно, для каждой социальной системы модель информационной безопасности является индивидуальной. Однако есть и общие закономерности моделирования, например — построение модели должно происходить на основе простых и оптимальных (как упоминавшийся нами поток света), административно-правовых основ.

Доказано, что высокие темпы развития информационных технологий порождают новые требования к сфере безопасности в целом и к информационной безопасности в частности. Реформирование законодательства, регулирующего деятельность в сфере информационной безопасности, должно происходить на базе надлежащей научной теории. Неотложной является необходимость создания Общей теории безопасности всего, которая объясняла и регулировала совокупность процессов обеспечения безопасности общества.

Ключевые слова: специальная теория, информационная безопасность, моделирование, административно-правовое регулирование, безопасность социальных систем.

Formulation of the problem. The high pace of information technology development, the introduction of high-tech devices in the production processes, training, communication, everyday life of the ordinary citizen, the steady growth of the role of information, its impact on the state, society, individuals, all this creates new demands on the security sector in general and information security in particular. Under such conditions, when operation of the security authorities, legislators, and sometimes scientists aren't always able to match the increasing demands and threats, openly trailing from reality, the very acute need for a theory that would become a cornerstone for law-making, enforcement, research activities in the field of legal regulation and practical implementation of information security, which will allow to systematize existing knowledge, to crystallize them, to remove excess, to form the basis for further development. Thus, the strategic goal of our research is to create a General theory of the security of the entire (STBV), which could explain and regulate a set of security processes of companies. Create STBV is a goal that should be treated as the creation of the general theory of relativity of A. Einstein. Create STBV will include the development, presentation, and communication of General laws of development and security, which would represent a fine universal formula. According to plan, the conclusion is simple and accessible to the General theory of security can only be proved after the creation and development of the laws of the Special theory of administrative-legal regulation of information security of social systems (STARS) at different

levels of complexity, which will cut unnecessary regulatory complications in the legislation.

Analysis of recent researches and publications. Individual aspects of information law and administrative-legal regulation of information security in particular have devoted their attention to domestic and foreign scientists: I. Aristova, N. Banchuk, K. Belyakov, V. U. Baskakov, V. Brizhko, D. Dovgal, G. Vinogradova, L. Zadorozhnaya, V. Sarosilo, R. Kalyuzhny, M. Koval, B. Kormych, V. Lipkan, A. Marushchak, A. Movchan, A. Podolyaka, E. Skulish, V. Tsimbalyuk and others.

However, the rapid development of information technology, the transformation of social relations, the emergence of new threats to society calls for new integrated studies-defined scope with a view to the formation of the special theory of administrative-legal regulation of information security of social systems.

The purpose of this article is the proof of the necessity of creating the special theory of administrative-legal regulation of information security of social systems (STARS), and the formulation of its principles, in analogy with the physical laws.

Presentation of the basic material. Everything in the Universe obeys rational and simple, objective laws of physics and synergetics, and develops exclusively in the framework outlined by them. Even light and heat are transmitted in a straight line, that is the simplest and shortest way that provides the greatest sense and the economy [1]. Why, then, are the laws of security companies should create complex and develop the shortest and most efficient

way? After all, the unfounded and irrational complexity creates many weak points, the contradictions, which in turn reduces the effectiveness of these laws, sometimes reducing it to zero.

At the same time, it's worth noting that not always a ray of light travels in a straight line. On the verge of two States (e. g. air and water or air and glass), the light changes its direction. Why? Because the function of light — is to reach your goal in the shortest period of time while minimizing the cost of energy for what it needs to choose the most effective and fastest way. For a better understanding of our ideas we present an analogy with the dangerous situation. Pretty girl begins to sink in the sea, a lifeguard, noticing this, runs to save her. The lifeguard can run the beach straight on (perpendicular) to the water and then swim diagonally to the girl. But then it's much more time in swimming, he'll get to sinking girl later, because the swim speed is much lower than the running speed. The rescuer may also be approached by land to a point which is the closest to the girl (for example — to run out on the pier, which is issued far out to sea) and from there to sail. However, the total time that it needs to be spent on the overcoming of such a path may be too large. That is, the optimal route will lie somewhere between the above extremes. So, as light chooses the optimal path in two different environments where it will be spent less time to achieve the goal, and as the rescuer selects the optimal route, which will be the victim and security theory should be as simple as possible, but to have sufficient (not excessive) level of complexity for the optimal performance of its functions.

When creating this theory, you should display beautiful and simple security laws by analogy with physical ones. Further derived laws should be reflected in the regulations, which will gradually transform regulatory legislation in the sphere of security in a slender, harmonious design with sufficient and yet not excessive level of difficulty. The introduction of such changes, in turn, will provide transparency, clarity and simplicity in social relations. To achieve our goal, we will create a system of analogies, where the physical quantity has had its counterpart of the indicators of the security sector and law.

From the postulates of the modern physical Sciences we know that all matter around is composed of atoms and molecules, which in their existence and interaction obey the laws of physics. With the positions of social Sciences, all that surrounds us around is society, specifically the social systems of different levels of difficulty, it's also the matter. Matter, as we have noted, consists of atoms and molecules. If atoms and molecules, their interactions and movement, impossible to describe and explain within the laws of physics and using formulas, the properties of the society, its social systems, the relationship in the middle, too, must obey the same laws and formulas [2].

Safety performs in society the role of a common unifying force, glue, like the force of gravity in physics. Gravity is the basis of all physical laws in the General theory of relativity of A. Einstein. On this basis, we believe that it's possible to create STAPRIBSS, which will describe the laws and formulas such similar physical.

From the law of universal gravitation we know that the force of gravity is proportional to the mass of the bodies and inversely proportional to the square of the distance between them [1]. Drawing an analogy of this statement with the society, we propose to assume that security force, which we call "stability of the social system" may be identical with gravitation. For the notion of the definition of "security" we have prepared another analogy. Moreover, in this context, the physical concept of "force" is identical to the legal concept of "level". The level (force) of stability depends on the structure and density of the social system and inversely proportional to the distance between the systems or their component elements.

In the macrocosm, at the level of stellar (solar) systems and in the microcosm — in the middle of the atoms, two forces act simultaneously. The first power in the middle of the atom is the force that attracts electrons (negative charge) to the nucleus (with positive charge). Simultaneously with it the force of repulsion that repels the electron, not allowing him to get closer to the core. Thus, the nucleus and the electrons attract and repel at the same time, being in the stable condition. Similarly, in the middle of the social system there are two forces, which are determined by the concept "level". This is, firstly, the level of development of the social system which moves the components, trying to expand the boundaries of the social system, striving for expansion, increase and improvement. And the second force is the security level that connects the system limits its growth without letting it fall apart. Therefore, the physical or natural concept of "unity and struggle of opposites" is reflected in society, in the social system.

Another postulate, which should be considered in our theory — physical energy depends on speed and gravity (mass) that flows out of the well-known formula $E = mc^2$ [2]. The stability of the social system, which depends on its reliability, but also the energy. This, in turn, depends on the volume and the mass of information in the system. And the speed of circulation of information is analogous to physical velocity. Uninterrupted operation of all information processes in the social system, their optimal speed should provide information security. This is another argument in favor of the need of the study we proposed the Special theory of administrative-legal regulation of information security of social systems (STALRISS).

As noted earlier, physical processes occur at the level of star systems and galaxies, around the celestial bodies move in regular orbits of planets and satellites, falling on their surface. The same thing we observe at the level of the microcosm — in the middle of atoms. These laws are governed by quantum physics. Therefore, I believe that the future development of the Special theory of administrative-legal regulation of information security of social systems and the General theory of security only to apply the analogy with the laws of quantum physics. This assumption is especially appropriate if you recall that all the processes in the human body are biochemical (metabolism) and electric (mental, analytical-synthetic activity) basis, that is to happen according to the laws of physical interaction.

Administrative-legal regulation of information security due to the need of state management of the processes of formation and use of information resources, creation and application of information systems and information security of social systems. Largely information security due to the necessity of the administrative regulation of information relations in various fields that compose the system itself and maintain its integrity [3].

Administrative-legal bases of information security of social systems should provide an ideal state of activities of entities of the system and its models. Selected specific legal and administrative foundations of information security, like physical formulas, create its model. Of course, for every social system model of information security is the individual. However, there are General patterns of modeling, for example — build model must be based on simple and optimal (as mentioned by us the stream of light), administrative-legal framework.

The process of ensuring information security of social systems constructed in accordance with the applicable laws and corporate regulations. Any similar process is associated with subjective perception and interpretation of the legal norms regulating these relations by the subjects. Relations arising in the sphere of ensuring information security of social systems, regulated primarily by the Constitution of Ukraine (article 17) [4]. In addition, the regulation is in accordance with the Laws of Ukraine "On information" [5] "About National program of Informatization" [6], and in addition there are Orders and Instructions relating to the social system, as enshrined in their charters, or protocols.

Realizing that the model of information security that you want to achieve the social system is the main objective, the management and security professionals (as subject), should choose the way to achieve it. If the goal activity is the process activity, we observe a negative phenomenon, which doesn't contribute to the positive result. To achieve a specific purpose, as indicated in the preceding analogies (with the savior and a ray of light), there is always a few ways. In the process of the election the way the subjects of information security, must take into account all the existing threats and risks. The procedures and steps of selection are regulated by administrative-legal bases of information security of the social system by these principles.

In theory, this way of constructing a model of information security is considered to be the most reasonable, given the fact that all participants in the process fully understands the objectives, represent the final goal and make it impossible (or aspire to be) superfluous and erroneous actions. In practice, in our society, unfortunately seen the trend of ridiculous things when reforms are carried out without a certain obvious sense. One gets the impression that sometimes reforms are for the sake of reforms. Even worse, when changes and reforms are carried out for the purpose, which is not an ideal model for the social system, and meets the interests of only a narrow circle of people. This situation leads to the degradation of society, and further to the destruction and disappearance of the entire social system [7].

The main feature of the proposed STALRISS is enshrined in this process, the patterns and relationships of objects and phenomena inherent in the social system. The simulation process is based on the laws of reflection and general communication, in accordance with the laws of analogy, because the very models of information security are considered as an object in the process of analysis and knowledge [8].

The modeling tools depend on features of the object-system, relationships between its components, objectives of its activities and modeling techniques. By administrative processes when modeling takes place a threefold approach: the subject of cognition (human) – model – the object of knowledge (the social system phenomenon). The principles of implementation and general relationships are the objective basis for using the model as an intermediate link in the process of knowing and analyzing the model itself. According to our plan, this is the general linear process. The introduction of models in specific cases in specific social systems, of course, there's a certain number of additional variables, however, they relate directly to individual cases and on General theory will not affect. However, the General rules of introduction of specific cases and solving the problem with additional variables will be studied and presented in the framework of the theory.

The patterns reflect the basic qualities of the model, providing consistency between the model and the ultimate goal, that's the purpose of its creation. Compliance is a specific way of administration of the fundamentals of modeling and reveals itself in common charac-teristics of the model and the ultimate goal (goal modeling). Such unity is the main feature in each case of the simulation depends on the goals of the company and its interests. Simply put, the goal consists of the set of fundamental interests, but is formed to the specific shape [9].

Of course, in the context we are talking about common interests of constituent entities and components of the social system. All kinds of differences in interests should be governed by information security. It should be noted that within the theory we share interests the security interests and development interests. Security interests, on the definition and the analogy with physics, are negative, they target a combination of social systems, preserve its consistency and in its ideal value level, they seek to minimize the activity (for example, interest have less accidents, diseases, etc). The development, on the contrary, we are called positive (in the scientific sense — similar to the physical), because they target the extension and termination of the social system, in your perfect value level, they are close to the maximum (for example, interest to have more money, territories etc). But, according to the principle of unity and struggle of opposites and the principle of the existence of the social system, these two interests can't develop without each other. They complement each other and coexist in a perfect balance, which we derive in the theory. Thus, the main principle of determining the balance of the law should be the principle of equilibrium of interests and threats.

The special theory of administrative-legal regulation of information security

of social systems (STALRISS) aims at modeling the security of the main principles of modeling of information security and means of scientific cognition of the laws of the simulation. The main means of cognition and analysis is to choose the method of reconstruction.

Approval of administrative-legal bases of reconstruction in the information security of social systems, which will be withdrawn when the development of the theory, contribute to the verification and receipt of new information. The feasibility of its application makes sense because the influence of time lost tracks and the quality of objects and phenomena. Reconstruction is the only method that ensures the reproduction and study the processes of circulation and use of information as a binder of social systems [10].

Analysis and evaluation of the models allow to identify causal relationships of processes of development of the social system and other phenomena in the middle and outside of the system and influence its development. The subjective side of the offense (mental relation of the person to socially dangerous act and its consequences in the form of intent or negligence) can also be studied through the analysis and evaluation models, identifying the most obvious explanation and that they have the relevant skills required to commit the offense in the information sphere [11].

The model of information security in each social system is a dynamic system. The system operates as a set of interacting elements that are combined in structural integrity with new properties different from the properties of each element of the social system alone. The system approach allows to analyze and identify the nature of relations between the selected model and the ultimate goal of applying this model to highlight the essential terms of objectives, types of these links, to establish patterns in the relationship between the elements forms a coherent system [12].

Models that are developed to create information security social systems are shared, because it's impossible to consider all the peculiarities of each situation. Only after receiving a number of models, selecting the more attractive, the contractor shall adapt the model and choose the path of achievement, for their social system or situation, then to issue it in the form of instructions or orders.

STALRISS takes into account the fact that advance modeling and forecasting of the chosen model, as well as creating a perfect (ultimate) goal has positive and negative sides. Focusing on ensuring the basic signs, sometimes insignificant and secondary (from the point of view task), you can skip those characteristics that are objectively substantial. For example, during a reconstruction (which, like physical research, is the source of experimental data during analysis and cognition), the link between objects can be misconceived and their dependence on consequences, resulting in inaccurate conclusions. Reconstruction, in the case of testing and research models, is used instead of the research trials with the original test with which it's impossible or impractical.

Development of models of information security for social systems should be based depending on the potential and existing threats. The list of threats

determined from the list of main interests of the social system. We argue that the occurrence of interest, at the same time there's the certain existing and potential threats to this interest that may be identified and addressed. Threats can be both internal and external. But these postulates too are to be investigated during the development of the theory.

Conclusions and prospects for further research. High rates of development of information technologies that generate new requirements of the security sector in General and information security in particular. The reform of the legislation governing activities in the field of information security must be based on proper scientific theories. What is urgent is the need to create a Common Security Theory (CST), which would explain and regulate a set of processes for ensuring the safety of society. At the same time, this is only possible after the creation and development of the laws of the Special theory of administrative-legal regulation of information security of social systems (STALRISS).

In the process of developing STALRISS and STBV is appropriate to use the analogy with the laws of physics, as nature demonstrates appropriate and effective mechanisms to achieve goals.

STALRISS should have a simple and clear structure. To use models of information security of social systems requires a clear procedure and regulation. The chosen mechanisms will aim at regulating the whole process, to entities that will use modeling, should know all the laws and formulas simulations, the order of their construction. Under development of STALRISS, the subjects

of it security needs to have a clear idea about the existing laws of their analogy, and the value for the selected model of information security.

REFERENCES

1. *Mitio Kaku* (2017), Fizyka buduscheho [Physics of the future], 5th ed, ANF, Moscow, Russian Federation.
2. *Hokinh S.* (2017), Najkorotsha istoriia chasu [The shortest history of time], KSD, Kharkiv, Ukraine.
3. *Adzhemohlu D. and Robinson D.* (2017), Chomu natsii zanepadaiut' [Why the nation will collapse], 2nd ed, Nash format, Kyiv, Ukraine.
4. *The Verkhovna* Rada of Ukraine (1996), Constitution of Ukraine, available at: http://zakon0.rada.gov.ua/laws/show/254%D0%BA/96-%D0%B2%D1%80
5. *The Verkhovna* Rada of Ukraine (1992), The Law of Ukraine "About information", available at: http://zakon0.rada.gov.ua/laws/show/2657-12 (Accessed 21 September 2017).
6. *The Verkhovna* Rada of Ukraine (1998), The Law of Ukraine "About the National Program of Informatization", available at: http://zakon2.rada.gov.ua/laws/show/74/98-%D0%B2%D1%80 (Accessed 22 September 2017)
7. *Kissinger H.* (2015), Myrovoj poriadok [World order], AST Publishers, Moscow, Russian Federation.
8. *Kormych B. A.* (2004), Informatsijna bezpeka: orhanizatsijno-pravovi osnovy: navchal'nyj posibnyk [Information security: organizational and legal bases: a tutorial], Kondor, Kyiv, Ukraine.
9. *Tsymbaliuk V.* (2004), "Information security of entrepreneurial activity: definition of the essence and content of the concept in the conditions of

Ukraine's entry into the information society (global cybercivilisation)" // Pidpryiemnytstvo, hospodarstvo, pravo. — Vol. 3. — P. 88–95.

10. *Maruschak A. I.* (2007) Informatsijne pravo: Dostup do informatsii : navchal'nyj posibnyk [Information law: Access to information: a tutorial], KNT, Kyiv, Ukraine.

11. *Nesteruk H. F., Osovetskoho L. H. and Nesteruk F. H.* (2003), "Adaptive model of neural network information security systems" // Perspektyvni informatsijni tekhnolohii ta intelektual'ni systemy. — Vol. 3. — P. 45–56.

12. *Lipkan V. A. Baskakov V. Yu.* (2013) Administratyvno-pravovyj rezhym informatsii z obmezhenym dostupom v Ukraini : monohrafiia. [Administrative-legal regime of restricted access information in Ukraine: monograph], FOP Lipkan, Kyiv, Ukraine.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. *Митио Каку*. Физика будущего. — 5-е изд. — М., 2017. — 584 с.

2. *Гокінг С.* Найкоротша історія часу. — Харків: КСД, 2017. — 159 с.

3. *Аджемоглу Д., Робінсон Д.* Чому нації занепадають. — 2-ге вид. — К.: Наш формат, 2017. — 440 с.

4. *Конституція* України від 28 червня 1996 року // Відомості Верховної Ради України. — 1996. — № 30. — Ст. 141.

5. *Про інформацію*: Закон України від 02.10.1992 р. № 2657-XII [Електронний ресурс]. — Режим доступу: http://zakon5.rada.gov.ua/laws/show/2657-12

6. *Про Національну* програму інформатизації: Закон України від 04.02.1998 р. № 74/98-ВР [Електронний ресурс]. — Режим доступу: http://zakon5.rada.gov.ua/laws/show/74/98-вр

7. *Киссинджер Г.* Мировой порядок. — М.: AST Publishers, 2015. — 512 с.

8. *Кормич Б. А.* Інформаційна безпека: організаційно-правові основи: навч. посіб. — К. : Кондор, 2004. — 382 с.

9. *Цимбалюк В.* Інформаційна безпека підприємницької діяльності: визначення сутності та змісту поняття за умов входження України до інформаційного суспільства (глобальної кіберцивілізації) // Підприємництво, господарство, право. — 2004. — № 3. — С. 88–95.

10. *Марущак А. І.* Інформаційне право: Доступ до інформації : навч. посіб. — К. : КНТ, 2007. — 532 с.

11. *Нестерук Г. Ф., Осовецького Л. Г., Нестерук Ф. Г.* Адаптивна модель нейромережевих систем інформаційної безпеки // Перспективні інформаційні технології та інтелектуальні системи. — 2003. — № 3. — С. 45–56.

12. *Ліпкан В. А., Баскаков В. Ю.* Адміністративно-правовий режим інформації з обмеженим доступом в Україні : монографія / В. А. Ліпкан, В. Ю. Баскаков. — К. : ФОП Ліпкан, 2013. — 342 с.