Veselova L.Yu.♦

DOI: 10.25108/2304-1730-1749.iolr.2020.62.54-63
UDC 004.5:001.4

Terminological approaches for forming a conceptual apparatus in the field of cyber security

Abstract: In general cyber security is interpreted differently and there are many opinions regarding the definition and interpretation of a difficult term. At the same time, in connection with various approaches to understanding the nature of information today there is no single general scientific definition of this concept, which leads to the difficulty of defining the concept of cyber security as an object of administrative regulation. In order to gain an understanding of the existing terminological approaches to the formation of a conceptual framework in the field of cyber security the author considers the scientific works and approaches of both Ukrainian, and foreign scientists in the field of (information) cyber security. The positions of specialists are studied when analyzing the definition of the term "cyber security" and based on the legislative definition of the term "information security" it is concluded, that cyber security is a special case of information security, the appearance of which is due to the use of computer systems and/or telecommunication networks. Thus, the definition of cyber security is based on the dialectical connection of the categories of general and individual in the field of information security. Cyber security is considered as a unit in relation to information security, acts as a general. In addition, the proposed approach allows us to consider the problems of cybe rsecurity from the perspective of a developed theoretical and practical base of information security and create consistent models in these areas. In turn, at the national and international levels of activity in cyberspace it is extremely important to strengthen the role of administrative regulation of the cyber defense sphere, as well as introduce innovations in the field of cyber security and improve educational areas for training specialists in this field of activity.

Keywords: hybrid war; administrative regulation; information security; national security.

References

1. Asmus V.F. (Eds.) *Aristotel'. Sobraniesochinenij v 4-h tomah* [Aristotle. Collected works in 4 volumes]. Moscow, Misl' Publ., 1976, 402 p. [in Russian].

2. Babakin V.M. (2011) *Osoblyvosti mizhnarodnoho spivrobitnytstva pry rozsliduvanni kiberzlochyniv* [Special features of the international competition for the provision of technical services]. *Forum prava – Forumright, 4, 27-30.* Available at http:/Avww.nbuv.gov.ua/e-journals/FP/2011 -4/11 bvmprk.pdf (accessed 10.03.2020) [in Ukrainian].

3. Baranov O.A. *Pro tlumachennia ta vyznachennia poniattia «kiberbezpeka»* [About interpreting and defining «cybersecurity»]. *Pravovainformatyka – Legal Informatics,* 2014, 2 (42), pp. 132-138 [in Ukrainian].

♦ **Veselova Liliya Yuryevna –** PhD in Law, Associate Professor of the Department for Administrative Activity of Police of the Odessa State University of the Internal Affairs of Ukraine. E-mail: cvet-Liliya@ukr.net

4. Baranov O.A. (2005) *Informatsiine pravo Ukrainy: stan, problemy, perspektyvy* [Information law of Ukraine: state, problems, prospects]. Kiev, Vydavnychyidim "SoftPres" Publ., 2005, 316 p. [in Ukrainian].

5. Gribanov D.V. Pravovoe regulirovanie kiberneticheskogo prostranstva kak sovokupnosti informacionnyh otnoshenij [Legal regulation of cyberspace as a set of information relations]. PhD in Law Thesis. Ekaterinburg. 2003. Available at: http://law.edu.ru/book/ book.asp?bookID=126348. (accessed 12.03.2020). [in Russian].

6. Dal' V.I. *Tolkovyj slovar' zhivogo velikorusskogo yazyka* [Explanatory Dictionary of the Living Great Russian Language] (Vols. 1-4). Moscow, GIS Publ., 1955, 669 p. [in Russian].

7. Dvoreckij I.H. *Latinsko-russkij slovar'* [Latin-Russian dictionary]. Moscow, Rus. iz. Publ., 1986, 840 p. [in Russian].

8. Katerynchuk I.P. *Informatsiine zabezpechennia diialnosti pravo okhoronny khorhaniv Ukrainy: problemyteorii i praktyky*[Information support of law enforcement agencies in Ukraine: problems of theory and practice]. Odessa, ODUVS Publ., 2015, 392 p. [in Ukrainian].

9. Ozhegov S.I., Shvedova N.Yu. *Tolkovyj slovar' russkogo yazyka* [Explanatory dictionary of the Russian language]. Moscow, Azbukovnik Publ., 1999, 324 p. [in Russian].

10. Panchenko V.M. (2013) *Spivvidnoshennia poniat: informatsiina ta kibernetychna bezpeka* [The relation of concepts: information and cyber security]. Informatsiina bezpeka liudyny, suspilstva, derzhavy [Information security of man, society, state] 2, 20-23. Available at: http://nbuv.gov.ua/j-pdf/iblsd_2013_2_5.pdf. (accessed 10.03.2020). [in Ukrainian].

11. Pigolkin A.S. *Yazyk zakona* [Language of law]. Moscow, Yurid. lit. Publ., 1990, 192 p. [in Russian].

12. *Pro Osnovni zasady rozvytku informatsiinoho suspilstva v Ukrainina 2007-2015 roky: Zakon Ukrainy* [On the Fundamental Principles of Information Society Development in Ukraine for 2007-2015: Law of Ukraine] vid 9 sichnia 2007 roku No. 537-V. Available at: https://zakon.rada.gov.ua/laws/show/537-16. (accessed 12.03.2020). [in Ukrainian].

13. *Pro osnovni zasady zabezpechennia kiberbezpeky Ukrainy: Zakon Ukrainy* [On the basic principles of ensuring cybersecurity of Ukraine: Law of Ukraine] vid 5 zhovtnia 2017 roku No. 2163-VIII. Available at: https://zakon.rada.gov.ua/laws/show/2163-19. (accessed 12.03.2020). [in Ukrainian].

14. Korystina O.Ie. (Eds.) *Protydiia vidmyvanniu koshtiv: mizhnarodni standarty, zarubizhnyi dosvid, administratyvno-pravovi, kryminolohichni, kryminalno-pravovi, kryminalistychni zasady ta systema finansovoho monitorynhu v Ukraini* [Money Laundering: International Standards, Foreign Experience, Administrative Law, Criminology, Criminal Law, Forensic Principles and Financial Monitoring System in Ukraine]. Kiev : Skif Publ., 2015, 984 p. [in Ukrainian].

15. Dubchynskyi V.V. (Eds.) *Suchasnyi tlumachnyi slovnyk ukrainskoi movy* [Modern Ukrainian Dictionary of Interpretation]. Khvarkov: VD Shkola Publ., 2006, 1008 p. [in Ukrainian].

16. Tykhomyrov O.O. *Zabezpechennia informatsiinoi bezpeky yak funktsiia derzhavy* [Providing information security as a function of the state] PhD in Law thesis. Kyiv, 2011, 234 p. [in Ukrainian].

17. Shelomentsev V.P. (2010) *Bezpekaliudyny, suspilstva i derzhavy v Ukraini: kryminolohichnyi aspekt* [Human, Society and State Security in Ukraine: The Criminological As-

pect]. *Borotba z orhanizovanoiuzlochynnistiu i koruptsiieiu (teoriia i praktyka) – Combating Organized Crime and Corruption (Theory and Practice)*, 22, pp. 215-222 [in Ukrainian].

18. Shelomentsev V.P. (2013) *Osnovni napriamy i subiekty zabezpechennia kiberbezpeky* [Key areas and subjects for cybersecurity]. *Borotba z orhanizovanoiuzlochynnistiu i koruptsiieiu (teoriia i praktyka) – Combating Organized Crime and Corruption (Theory and Practice)*. No. 1(29), pp. 348-355 [in Ukrainian].

19. ShemshuchenkoYu.S., Ziubliuk M.P., Horbatenko V.P. *Yurydychna entsyklopediia* [Legal Encyclopedia] (Vols. 1-6). Yu.S. Shemshuchenko (Ed.). Kyiv: Ukrainska entsyklopediiaim. M.P. Bazhana Publ., 2003, 736 p. [inUkrainian].

20. Franscella J. Cyber security vs. CyberSecurity: When, Why and How to Use the Term. Available at: www.infosecisland.com/blogview/23287-Cybersecurity-vs-Cyber-Security-hen-Why-and-How-to-Use-the-Term.html (accessed 16.03.2020).

21. Klimburg A. National cyber security framework manual // NATO CCD COE Publications (December 2012). 2012. Available at: http://belfercenter.hks. harvard.edu/files/hathaway-klimburg-nato-manual–ch-1.pdf (accessed 16.03.2020).

22. Stubley D. What is CyberSecurity? Available at: www.7elements.co.uk/resources/blog /what-is-cyber-security (accessed 16.03.2020).

Веселова Л.Ю.♦

DOI: 10.25108/2304-1730-1749.iolr.2020.62.54-63
УДК 004.5:001.4

Терминологические подходы формирования понятийного аппарата в области кибербезопасности

Аннотация: В общем кибербезопасность трактуется по-разному и существует множество мнений относительно определения и толкования непростого термина. Вместе с тем, в связи с различными подходами к пониманию природы информации на сегодня нет единого общенаучного определения этого понятия, что приводит к сложности определения понятия кибербезопасности как объекта административно-правового регулирования. С целью получения представления о имеющихся терминологических подходах формирования понятийного аппарата в области кибербезопасности рассматриваются научные работы и подходы как украинских, так и зарубежных ученых в сфере (информационной) кибернетической безопасности. Изучаются позиции специалистов при анализе определения термина «кибербезопасность» и на основе законодательного определения термина «информационная безопасность» делается вывод о том, что кибербезопасность – это частный случай информационной безопасности, появление которого обусловлено использованием компьютерных систем и/или телекоммуникационных сетей. Таким образом, определение кибербезопасности основано на диалектической связи категорий общего и единичного в сфере информационной безопасности. Кибербезопасность рассматривается как единичное по отношению к информационной безопасности, выступает в качестве общего. Кроме того, предложенный подход позволяет рассматривать проблемы кибербезопасности с позиции относительно наработанной теоретической и практической базы информационной безопасности и создавать непротиворечивые модели в этих сферах. В свою очередь, на национальном и международном уровнях деятельности в киберпространстве крайне важно усиление роли административного регулирования сферы киберзащиты, а также внедрение инноваций в сфере кибербезопасности и совершенствование образовательных направлений при подготовке специалистов в этой сфере деятельности.

Ключевые слова: гибридная война; административно-правовое регулирование; информационная безопасность; национальная безопасность.

Вступление. В современном мире, который перенасыщен новейшими информационными технологиями, локальными и глобальными компьютерными сетями, все чаще встречаются термины с приставкой «кибер», в частности киберпространство, кибератака, киберпреступление, кибероружие, кибертерроризм и т.п., которые относятся к особо динамической специфической сфере деятельности человека, связанной с обменом и обработкой электронных данных в глобальных информационно-коммуникационных сетях [2].

Терминологическое определение указанных понятий вызвало противоречие не только среди ученых, но и среди практиков. Вместе с тем, неготовность действующей правовой ба-

♦ **Веселова Лилия Юрьевна** - кандидат юридических наук, доцент кафедры административной деятельности полиции Одесского государственного университета внутренних дел, Украина. E-mail: cvet-Liliya@ukr.net

зы, в части понятийно-терминологического аппарата кибербезопасности, вызывает необходимость в адекватном его формировании и в качественном его наполнении в соответствии с требованиями, которые предъявляются к юридической терминологии. Данная необходимость вызвана современными и перспективными возможностями нашего государства, особенностями национальной правовой системы, а также требованиями, предъявляемыми к языку закона. Основными из этих требований считается следующие: до терминологического аппарата – однозначность, адекватность, системность терминологии, а также единство ее использования; к дефинициям и толкованиям понятий – ясность и простота, точность и полнота, лаконичность, последовательность изложения [11, с. 18-34]. При таких условиях, важным является системный подход к формированию именно понятийно-терминологического аппарата в сфере кибербезопасности в соответствии с международными актами в части административно-правового регулирования обеспечения и организации кибербезопасности. Учитывая указанное, и с целью адекватного содержательного наполнения понятийно-терминологического аппарата административно правового регулирования обеспечения и организации кибербезопасности, следует обратиться к самому термину, дефиниция которого позволит исчерпывающе определить дискуссионный предмет исследования, круг проблем, которые могут быть при этом затронуты [8 , с . 23].

В статье рассматриваются научные работы таких ученых, как Ампера А., Бабакина В. Баранова А., Виннера Н., Франсело Д., Шеломенцева В. и др. В общем кибербезопасность трактуется по-разному и существует множество мнений относительно определения и толкования непростого термина. Вместе с тем, в связи с различными подходами к пониманию природы информации на сегодня нет единого общенаучного определения этого понятия, что приводит к сложности определения понятия кибербезопасности как объекта административно-правового регулирования. **Цель данной статьи** – получить представление о имеющихся терминологических подходах формирования понятийного аппарата в области кибербезопасности, после чего понять недостатки обозначенного вопроса и определить пути решения найденных проблем.

Результаты исследования. На сегодняшний день не существует единой трактовки понятия «кибербезопасность». Это вызвано тем, что термин «cybersecurity» все чаще и чаще используется в научном и правовом обороте. Вместе с тем, Д. Франсело, специалист по обеспечению безопасности в киберпространстве, отмечает, что многие руководители служб безопасности и просто эксперты по информационной безопасности до сих пор путаются в том, когда и как использовать этот термин [20]. «Кибербезопасность» является одной из разновидностей понятия – «безопасность», а потому для определения сути данного термина является логическим обратиться к толкованию дефиниции «безопасность», который происходит от английского «security» [19, с. 132]. В свою очередь, английское слово «security» происходит от латинского слова securitas (securus), которое имеет несколько значений, в частности: «беспечность», «душевный покой», «безопасность», «обеспеченность» [7, с. 695]. В переводе с древнегреческого термин «безопасность» переводится как «владение ситуацией» [1, с. 102]. В справочных словарях термин «безопасность» предлагается понимать как состояние, при котором не угрожает опасность кому/чему-либо [9, с. 38]; не вызывает беспокойства [15 ,с. 53]; отсутствие опасности, сохранность и надежность [6 с. 67]. Однако, такой этимологический подход к пониманию безопасности является упрощенным и не отражает реалий существования человеческого общества, которое существует в условиях постоянного нали-

чия угроз, реальных и потенциальных, известных и неизвестных, прогнозируемых и неожиданных [16, с. 75].

Многие из украинских ученых, анализируя нормативно-правовое обеспечение национальной и информационной безопасности, определяют кибербезопасность как защищенность жизненно важных интересов человека и гражданина, общества и государства, при которой обеспечивается устойчивое развитие общества, своевременное выявление, предотвращение и нейтрализация реальных и потенциальных угроз национальным интересам в сфере функционирования ИТС [21]. Изучая различные мнения и подходы при определении безопасности, по нашему мнению, интересна позиция В. Шеломенцева. Ученый предлагает под кибербезопасностью понимать состояние защищенности жизненно важных интересов и гражданина, общества и государства от внешних и внутренних угроз, связанных с использованием ресурсов киберпространства, при котором в государстве обеспечивается устойчивое развитие информационного общества [17, с. 220].

Что касается сущности кибербезопасности. Понятие имеет приставку «кибер», что происходит от слова «кибернетика». Слово греческого происхождения и в переводе означает «искусство руководителя», то есть «искусство управления, управление». Древнегреческий философ Платон первым начал использовать и ввел в оборот термин «кибернетика». В 1834 году французский ученый Андре Мари Ампер использовал термин для обозначения науки об управлении обществом, а в 1947 году Норберт Винер опубликовал книгу «Кибернетика», в которой ученый определил кибернетику как науку об управлении, коммуникации, обработки информации в технических системах, человеческом обществе и живых организмах. Основным тезисом исследования ученого было сходство информационных процессов управления и коммуникации в машинах, живых организмах и обществе, а следовательно, по мнению автора, кибернетика – это наука об управлении информацией [10]. В общем термин «кибербезопасность» вызвал интерес исследователей еще в середине 1990-х годов, а именно, когда правительство США начало активно исследовать проблемы киберпреступности [22]. В современных научных трудах понятие «кибербезопасности» рассматривается по нескольким направлениям, например в технологическом контексте – это процесс защиты киберпространства от реальных и потенциальных киберугроз; на философско-социологическом уровне – это совокупность условий функционирования субъекта в киберпространстве, обеспечивающие его оптимальное информационное развитие.

Кибербезопасность, по мнению некоторых украинских ученых – это защищенность надлежащего функционирования информационных и телекоммуникационных систем от нежелательных для пользователей нарушений процесса обработки данных и результатов такой обработки (киберугроз) [18, с. 350; 5].

На сегодня кибернетика – наука об управлении, связи и переработке информации, объектом исследования которой является кибернетические системы, рассматриваемые абстрактно (безотносительно к их реальной природе), что позволяет проводить исследования технических, биологических, социальных систем общими методами [5, с. 27]. В этом смысле кибернетическую систему следует рассматривать как совокупность ее взаимосвязанных элементов (объектов), которые способны запоминать, обрабатывать информацию и обмениваться ею с другими элементами и внешним миром.

Процесс подготовки управленческих решений, как и сам процесс управления, неразрывно связанны с информационными процессами. Невозможно представить без использова-

ния компьютерных систем и телекоммуникационных сетей современные системы управления. Особенно трудно представить системы управления с большими территориально-распределенными социотехническими системами, например, такими как системы управления энергетической инфраструктурой, воздушным и железнодорожным движением, банковскими и финансовыми системами, большими промышленно-производственными комплексами и т.п., без соответствующего современного информационного обеспечения. В связи с этим, большое количество специалистов и экспертов считают, что толкование кибербезопасности как проблемы, связанной с системами управления, будет пониматься как частичная проблема во всей проблематике кибербезопасности.

Проведенное исследование позволяет утверждать, что авторы полностью согласны с позицией профессора А. Баранова относительно толкования и определения понятия «кибербезопасность» [3], а использование компьютерных систем и телекоммуникационных сетей является основным квалифицирующим признаком и обязательным условием проблематики кибербезопасности.

Вместе с тем, рост современного общества неразрывно связан с предотвращением разнообразных угроз, которые усиливаются в период реформирования любой сферы жизнедеятельности общества [14]. Вопрос противодействия гибридным угрозам, в частности, информационным и кибернетическим, достаточно широко и комплексно охватывает проблемы национальной безопасности. Знание объекта возможных угроз, а также видов и типов возможного ущерба дают возможность для методологического определения объема юрисдикции понятия кибербезопасности. Кроме того, от знания и понимания зависит содержание стратегий кибербезопасности, объекты, подпадающие под меры по обеспечению кибербезопасности, уровень и перечень учреждений и органов, состав и объемы ресурсов, которые должны быть при этом задействованы. Таким образом, знание и понимание имеют высокую практическую ценность.

Учитывая целевое назначение компьютерных систем и телекоммуникационных сетей необходимо акцентировать внимание, что киберугрозы в первую очередь направлены на нарушение обращения информации. Угрозы могут быть связаны как с недостоверностью, несвоевременностью и неполнотой информации, так и с нарушением собственно обращения информации на любом из его этапов (создании, распространении, использовании, хранении и уничтожении информации), а также угрозы, связанные с несанкционированным использованием и распространением информации, нарушением ее целостности и конфиденциальности.

Итак, информация и ее оборот имеют непосредственное отношение к проблематике, связанной с кибербезопасностью, в частности, к обеспечению субъектов информационных отношений достоверной, своевременной и полной информацией, а также к недопущению несанкционированного использования и распространения информации, нарушение ее целостности и конфиденциальности.

Функционирование социальных и социотехнических систем, как правило, полностью базируется и зависит от качества, надежности и стабильности работы технических комплексов компьютерных систем и телекоммуникационных сетей, нарушение функционирования таких систем и сетей может привести к ухудшению или даже остановка социальных и социотехнических систем, элементами которых они являются. Поэтому такие комплексы должны надлежащим образом проектироваться, строиться, сдаваться в эксплуатацию, эксплуатироваться, сопровождаться проектантами и производителями и тому подобное. В данном аспек-

те выделяют отдельную группу киберугроз, вызванных недостатками в нормативно-правовом и нормативно-техническом обеспечении этих процессов, просчетами в их организации и реализации, которые могут привести к нарушению функционирования компьютерных систем и телекоммуникационных сетей в процессе их эксплуатации.

Сегодняшнее существование ставит достаточно высокие требования к созданию социальных и социотехнических систем. Элементы таких систем находятся на значительном расстоянии и на разных территориях. Поэтому с целью обеспечения их инфраструктурной устойчивости и достаточности обеспечения оптимального проектирования топологии территориально распределенных компьютерных систем и телекоммуникационных сетей является весьма важным фактором. Несоблюдение или невыполнение требований инфраструктурной устойчивости и достаточности территориально распределенных компьютерных систем и телекоммуникационных сетей может привести к ухудшению или даже остановки социальных и социотехнических их систем, элементами которых они являются.

Учитывая вышесказанное, можно сделать вывод, что среди проблем кибербезопасности есть проблема обеспечения инфраструктурной безопасности социальных и социотехнических систем, при работе которых используют компьютерные системы и телекоммуникационные сети, или другими словами, проблема, связанная с задачей возможного ущерба от негативных последствий использования информационных компьютерных технологий [4].

Вместе с тем, все возможные виды и типы ущерба, которые могут иметь место в результате нарушения кибербезопасности, сводятся к ущербу, который непосредственно несут социальные и социотехнические системы. Нарушения кибербезопасности приводит к снижению уровня защищенности жизненно важных интересов человека, общества и государства. Основная цель обеспечения кибербезопасности – это обеспечение состояния защищенности жизненно важных интересов человека, общества и государства. Основным критерием эффективности мероприятий по обеспечению кибербезопасности должны быть критерии, основанные на оценке качества функционирования социальных и социотехнических систем. Поэтому, проблема оценки состояния кибербезопасности должна прежде всего рассматриваться в неразрывной связи с оценкой возможного или нанесенного ущерба социальным или социотехническим системам как системам более высокого порядка.

В научной работе профессор А. Баранов «Информационное право Украины: состояние, проблемы, перспективы» [4] обосновывает и раскрывает определение термина «информационная безопасность». Обозначенный термин закреплен и на законодательном уровне. Так, Закон Украины «Об основных принципах развития информационного общества в Украине на 2007-2015 года» информационную безопасность определяет как состояние защищенности жизненно важных интересов личности, общества и государства, при котором предотвращается нанесение ущерба через: неполноту, несвоевременность и недостоверность информации, что используется; негативное информационное влияние; негативные последствия применения информационных технологий; несанкционированное распространение, использование и нарушение целостности, конфиденциальности и доступности информации [12]. В дальнейшем законодателем определены правовые и организационные основы обеспечения защиты жизненно важных интересов человека и гражданина, общества и государства, национальных интересов Украины в киберпространстве, полномочия и обязанности государственных органов, предприятий, учреждений, организаций, лиц и граждан, основных принципов координации их деятельности, а также базовых терминов в сфере кибербезопасности

[13]. В Законе Украины «Об основных принципах обеспечения кибербезопасности Украины» важным является и то, что (как и ранее упоминали в законе) также толкуются сами понятия «кибербезопасности», «киберзащиты» и «киберпреступности», уже более десяти лет используют в юридической практике.

Изучив позиции специалистов при анализе определения термина «кибербезопасность» и на основе законодательного определения термина «информационная безопасность» можно сделать вывод о том, что кибербезопасность – это частный случай информационной безопасности, появление которого обусловлено использованием компьютерных систем и/или телекоммуникационных сетей.

Выводы. Таким образом, определение кибербезопасности основано на диалектической связи категорий общего и единичного в сфере информационной безопасности. Кибербезопасность рассмотрена как единичное по отношению к информационной безопасности, выступает в качестве общего. Кроме того, предложенный подход позволяет рассматривать проблемы кибербезопасности с позиции относительно наработанной теоретической и практической базы информационной безопасности и создавать непротиворечивые модели в этих сферах. В свою очередь, на национальном и международном уровнях деятельности в киберпространстве крайне важно усиление роли административного регулирования сферы киберзащиты, а также внедрение инноваций в сфере кибербезопасности и совершенствование образовательных направлений при подготовке специалистов в этой сфере деятельности.

Библиография

1. Аристотель. Собрание сочинений в 4-х томах / Под ред. В.Ф. Асмус. Т. 3. - Москва: Мысль, 1976. - 402 с.

2. Бабакін В.М. Особливості міжнародного співробітництва при розслідуванні кіберзлочинів. *Форум права.* 2011. № 4. С. 27-30. [Электронный ресурс]. Режим доступа: http:/Avww. nbuv. gov. ua/e-journals/FP/2011 -4/11 bvmprk.pdf. (дата обращения: 10.03.2020).

3. Баранов О.А. Про тлумачення та визначення поняття «кібербезпека». *Правова інформатика*. -2014. - № 2 (42). - С. 132-138.

4. Баранов О.А. Інформаційне право України: стан, проблеми, перспективи. - Київ: Видавничий дім “СофтПрес”, 2005. - 316 с.

5. Грибанов Д.В. Правовое регулирование кибернетического пространства как совокупности информационных отношений: автореф. дис. … канд. юрид. наук. Екатеринбург, 2003. 23 с. [Электронный ресурс]. Режим доступа: http://law.edu.ru/book/ book.asp?bookID=126348 (дата обращения: 12.03.2020).

6. Даль В.И. Толковый словарь живого великоруського языка: в 4 т. / вступ. ст. А.М. Бабкина. - Москва: ГИС, 1955. (Набрано и напеч. со 2-го изд., 1880-1882 гг.), Т. 1: А - З. - LXXXVIII. - 669 с.

7. Дворецкий И.Х. Латинско-русский словарь: словарь. 3-е изд., исправ. - Москва: Рус. изд., 1986. - 840 с.

8. Катеринчук І.П. Інформаційне забезпечення діяльності правоохоронних органів України: проблеми теорії і практики: монографія. - Одеса : ОДУВС, 2015. - 392 с.

9. Ожегов С.И., Шведова Н.Ю. Толковый словарь русского языка. [4-е изд., доп.]. - Москва: Азбуковник, 1999. - 324 с.

10. Панченко В.М. Співвідношення понять: інформаційна та кібернетична безпека. Інформаційна безпека людини, суспільства, держави. 2013. № 2. - С. 20-23. [Электронный ресурс]. Режим доступа: http://nbuv.gov.ua/j-pdf/iblsd_2013_2_5.pdf. (дата обращения: 10.03.2020).

11. Пиголкин А.С. Язык закона. - Москва: Юрид. лит., 1990. - 192 с.

12. Про Основні засади розвитку інформаційного суспільства в Україні на 2007-2015 роки: Закон України від 9 січня 2007 року № 537-V. [Электронный ресурс]. Режим доступа: https://zakon.rada.gov.ua/laws/show/537-16 (дата обращения: 12.03.2020).

13. Про основні засади забезпечення кібербезпеки України: Закон України від 5 жовтня 2017 року № 2163-VIII. [Электронный ресурс]. Режим доступа: https://zakon.rada.gov.ua/laws/show/2163-19 (дата обращения: 12.03.2020).

14. Протидія відмиванню коштів: міжнародні стандарти, зарубіжний досвід, адміністративно-правові, кримінологічні, кримінально-правові, криміналістичні засади та система фінансового моніторингу в Україні. Підручник. За ред. Користіна О.Є.- Київ: Скіф, 2015.-984 с.

15. Сучасний тлумачний словник української мови: / [словник 65000 слів] заг. ред. В.В. Дубчинський. - Харьков: ВД «ШКОЛА», 2006. - 1008 с.

16. Тихомиров О.О. Забезпечення інформаційної безпеки як функція держави: дис. … канд. юрид. наук. - Київ, 2011. - 234 с.

17. Шеломенцев В.П. Безпека людини, суспільства і держави в Україні: кримінологічний аспект. // Боротьба з організованою злочинністю і корупцією (теорія і практика). - 2010. - № 22. - С. 215-222.

18. Шеломенцев В.П. Основні напрями і суб'єкти забезпечення кібербезпеки // Боротьба з організованою злочинністю і корупцією (теорія і практика). - 2013. - № 1(29). - С. 348-355.

19. Юридична енциклопедія: словник-довідник: В 6 т./ [укл.: Ю.С. Шемшученко, М.П. Зюблюк, В.П. Горбатенко та ін. / НАНУ.Ін-т держави і права ім. В.М. Корецького; Гол.ред. Ю.С. Шемшученко]. [Т. 5: П-С]. - Київ: Українська енциклопедія ім. М.П. Бажана, 2003. - 736 с.

20. Franscella J. Cybersecurity vs. CyberSecurity: When, Why and How to Use the Term. Available at: //www.infosecisland.com/blogview/23287-Cybersecurity-vs-Cyber-Security-hen-Why-and-How-to-Use-the-Term.html (accessed 16.03.2020)

21. Klimburg A. National cyber security framework manual // NATO CCD COE Publications (December 2012). 2012. Available at: http://belfercenter.hks. harvard.edu/files/hathaway-klimburg-nato-manual–ch-1.pdf (accessed 16.03.2020).

22. Stubley D. What is Cyber Security? Available at: //www.7elements.co.uk/resources/blog /what-is-cyber-security (accessed 16.03.2020).