



Электронный научный журнал  
Южного федерального  
университета

УПРАВЛЕНИЕ В  
ЭКОНОМИЧЕСКИХ  
И СОЦИАЛЬНЫХ  
СИСТЕМАХ

2022

№4(14)

ISSN 2686-9802

Online scientific journal  
Southern Federal University



MANAGEMENT IN  
ECONOMIC AND  
SOCIAL SYSTEMS

2022

No 4(14)

ISSN: 2686-9802



Институт управления в экономических,  
экологических и социальных системах

# УПРАВЛЕНИЕ В ЭКОНОМИЧЕСКИХ И СОЦИАЛЬНЫХ СИСТЕМАХ

Электронный научный журнал

№ 4 (14), 2022

<http://journal-mes.ru>

Издание зарегистрировано Федеральной службой по надзору в сфере связи,  
информационных технологий и массовых коммуникаций (Роскомнадзор)

Свидетельство о регистрации: Эл № ФС 77-74261 от 23.11.2018 г.

Учредитель: Федеральное государственное автономное образовательное  
учреждение высшего образования “Южный федеральный университет”

ISSN 2686-9802

## ● Главный редактор

Горелова Г.В. - д-р техн. наук, профессор,  
Южный федеральный университет  
(Таганрог, Россия)

## ● Заместитель главного редактора

Павлов П.В. - д-р экон. наук, д-р юрид. наук,  
профессор, Южный федеральный университет  
(Таганрог, Россия)

## ● Ответственный секретарь

Бабикова А.В. - канд экон. наук, доцент,  
Южный федеральный университет  
(Таганрог, Россия)

## ● Ответственный редактор

Кобец Е.А. - канд экон. наук, доцент,  
Южный федеральный университет  
(Таганрог, Россия)

## ● Редакционная коллегия

Андреесен Д.-Э.	профессор, Остфолдский университет (Халден, Норвегия).
Бакаларчик С.	PhD, профессор, Лодзинский технологический университет, Глава Комитета по инновациям и развитию при ЕС (Лодзь, Польша).
Гомес Дж. Ф.С.	PhD, профессор, Университет Лиссабона, Лиссабонская школа экономики и менеджмента (Лиссабон, Португалия).
Гушев В.А.	PhD, профессор, Софийский университет Святого Климента Орхидского (София, Болгария).
Лутовац М.	д-р техн. наук профессор, Объединенный университет Никола Теслы (Белград, Сербия).
Станиславский Р.	PhD, профессор, Лодзинский технологический университет (Лодзь, Польша).
Вертакова Ю.В.	д-р экон. наук, профессор Курский филиал Финансового университета при Правительстве РФ (Курск, Россия).
Клочков В.В.	д-р ист. наук, доцент, Южный федеральный университет (Таганрог, Россия).
Костенко М.А.	канд. юрид. наук, доцент, Южный федеральный университет (Таганрог, Россия).
Кочергина Т.Е.	д-р экон. наук, профессор, Российская таможенная академия (Ростов-на-Дону, Россия).
Малько А.В.	д-р юрид. наук, профессор, Заслуженный деятель науки РФ, Институт государства и права Российской академии наук (г. Саратов, Россия).
Макареня Т.А.	д-р экон. наук, доцент, Южный федеральный университет (Таганрог, Россия).
Рачипа А.В.	д-р социол. наук, профессор, Южный федеральный университет (Таганрог, Россия).
Рыльская М.А.	д-р юрид. наук, профессор, Финансовый университет при Правительстве РФ (г. Москва, Россия).
Саак А.Э.	д-р техн. наук, доцент, Южный федеральный университет (Таганрог, Россия).
Таранов П.В.	д-р экон. наук, профессор, Ростовский государственный экономический университет (РИНХ) (Ростов-на-Дону, Россия).

Периодичность выпуска: 4 раза в год.

Языки: русский, английский.

Посвящен исследованиям: экономики и управления,  
права и общества.

Основное содержание: результаты оригинальных  
научных исследований и аналитические обзоры.

В журнале публикуются статьи проблемного и  
научно-практического характера по следующим  
научным направлениям:

05.13.01 Системный анализ, управление и обработка  
информации (по отраслям);

08.00.00 Экономические науки;

12.00.00 Юридические науки;

22.00.00 Социологические науки.

Авторы: ведущие ученые в области социально-  
гуманитарных наук, преподаватели, аспиранты,  
магистранты, представители бизнеса.

Основная аудитория: преподаватели, обучающиеся  
вузов, руководители органов власти,  
представители бизнеса.





# MANAGEMENT IN ECONOMIC AND SOCIAL SYSTEMS

Online scientific journal

No 4 (14), 2022

<http://journal-mes.ru>

The journal is registered by the Federal Service for Supervision of Communications,  
Information Technology and Mass Communications (Roskomnadzor)

Registration certificate: ЭЛ № ФС 77-74261 from 23.11.2018

Founder: Federal State Education Institution of Higher Education  
“Southern Federal University”

ISSN 2686-9802

## ● Editor-in-chief

Gorelova G.V. - Doctor of Technical Sciences,  
professor, Southern Federal University  
(Taganrog, Russia)

## ● Deputy of the editor-in-chief

Pavlov P.V. - Doctor of Economics, Doctor of  
Law, professor, Southern Federal University  
(Taganrog, Russia)

## ● Executive secretary

Babikova A.V. - Candidate of Economics (PhD),  
associate professor, Southern Federal University  
(Taganrog, Russia)

## ● Executive editor

Kobets E.A. - Candidate of Economics (PhD),  
associate professor, Southern Federal University  
(Taganrog, Russia)

## ● Editorial board

Andreassen J-E	Professor, Østfold University Colledge / Hogskolen i Østfold (Halden, Norway).
Bakalarczyk S.	PhD, Professor, Lodz University of Technology, Head of EU Committee for Innovation and Development, (Lodz, Poland).
Gomes Jg. F.S.	PhD, professor, associate professor of Lisbon school of Economics & Management Universidade de Lisboa (Lisbon, Portugal)
Gushev V.A.	PhD, Professor, Sofia Unoversity ST. Kliment Ohridski (Sofia, Bulgaria).
Lutovac M.	Doctor of Technical Sciences, Professor, University "Union Nikola Tesla" (Belgrade, Serbia)
Stanisławski R.	PhD, Professor, Lodz University of Technology (Lodz, Poland).
Klochkov V.V.	Doctor of History, associate professor, Southern Federal University (Taganrog, Russia).
Kostenko M.A.	Candidate of Law (PhD), associate professor, Southern Federal University (Taganrog, Russia).
Kochergina T.E.	Doctor of Economics, Professor, Russian Customs Academy (Rostov-on-Don, Russia).
Mal'ko A.V.	Doctor of Law, Professor, Honored Scientist of the Russian Federation, Institute of State and Law Russian Academy of Sciences (Saratov, Russia).
Makarenya T.A	Doctor of Economics, Professor, Southern Federal University (Taganrog, Russia).
Rachipa A.V.	Doctor of Sociological Science, Professor, Southern Federal University (Taganrog, Russia).
Ryl'skaya M.A.	Doctor of Law, Professor, Financial University under the Government of the Russian Federation (Moscow, Russia).
Saak A.E.	Doctor of Technical Sciences, associate professor, Southern Federal University (Taganrog, Russia)
Taranov P.V.	Doctor of Economics, Professor, Rostov State Economic University (Rostov-on-Don, Russia).
Vertakova Yu.V.	Doctor of Economics, Professor, Kursk Branch of the Financial University under the Government of the Russian Federation (Kursk, Russia)

Release frequency: 4 issues per year

Languages: Russian, English.

Dedicated to research: economics and management,  
rights and societies.

Main content: original results research and analytical  
reviews. The journal publishes articles of problem and  
scientific and practical nature of the following  
scientific areas:

05.13.01 System analysis, management and processing  
information (by industry);

08.00.00 Economic Sciences;

12.00.00 Jurisprudence;

22.00.00 Sociological Sciences.

Authors: leading scientists in the field of humanities,  
teachers, graduate and master students, business representatives.

Main audience of the journal: teachers, students enrolled at  
universities, heads of government, business representatives.

# СОДЕРЖАНИЕ

Защитина Е. К.	Теории оценки успешности мировой экономики с позиции развития системы образования	5
Zashchitina E. K.	Theories for assessing the success of the world economy from the standpoint of the development of the education system	
<hr style="width: 10%; margin: 0 auto;"/>		
Защитина Е. К., Павлов П. В.	Современные тренды развития мировой экономики	13
Zashchitina E. K., Pavlov P. V.	Modern development trends of the world economy	
<hr style="width: 10%; margin: 0 auto;"/>		
Петков Д. А.	Текущее положение России в ЕАЭС и БРИКС	20
Petkov D. A.	Current position of Russia in the EAEU and BRICS	
<hr style="width: 10%; margin: 0 auto;"/>		
Привалова Е. Е.	Особенности ведения бизнеса в рамках достижения целей устойчивого развития	26
Privalova E. E.	Peculiarities of doing business within the framework of achieving the sustainable development goals	
<hr style="width: 10%; margin: 0 auto;"/>		
Ткаченко Ю. Г., Дружинина В. Д.	Анализ влияния экономических санкций на деятельность организаций (на примере Ростовской области)	32
Tkachenko Yu. G., Druzhinina V. D.	Analysis of the impact of economic sanctions on the activities of organizations (example of the Rostov region)	
<hr style="width: 10%; margin: 0 auto;"/>		
Филатова Е. В., Селезнева П. М.	Национальная безопасность в информационную эпоху	41
Filatova E. V., Selezneva P. M.	National security in the informational era	
<hr style="width: 10%; margin: 0 auto;"/>		
Aleinikova Yu. V., Kazanskaya A. Yu.	Open opportunities for Russian business to enter the global market: PESTEL analysis of the UAE and Turkey	47
Алейникова Ю. В., Казанская А. Ю.	Открытые возможности выхода российского бизнеса на глобальный рынок: PESTEL анализ ОАЭ и Турции	

Научная статья  
УДК 378

## НАЦИОНАЛЬНАЯ БЕЗОПАСНОСТЬ В ИНФОРМАЦИОННУЮ ЭПОХУ

Филатова Е. В.<sup>1</sup>, Селезнева П. М.<sup>2</sup>

<sup>1</sup> Южный федеральный университет,  
канд. юрид. наук., доцент

<sup>2</sup> Южный федеральный университет,  
студент

В статье дается общая характеристика основных положений и принципов Доктрины информационной безопасности Российской Федерации, определяется ее значение и приоритетные направления совершенствования правового регулирования в информационной сфере. Высказывается мнение о необходимости разработки специализированного информационно-поискового тезауруса, а также систематизации всех терминов в информационной сфере по принципу вертикальной и горизонтальной классификации. Акцентируется внимание на целесообразности расстановки приоритетов по степени важности, решаемых Доктриной информационной безопасности задач. Методологией исследования выступили общенаучные и частнонаучные методы, особое место среди которых занимают конкретно-социологический и метод моделирования. Сделан вывод о необходимости гармонизации интересов государства, гражданского общества и личности в сфере национальной безопасности. В сфере информационной безопасности эффективная терминологическая политика позволяет делиться набором знаний, формировать, использовать и разрабатывать терминологию технической направленности среди программистов, технических специалистов, с одной стороны, и правоведов, с другой.

*Ключевые слова:* информационная безопасность; национальная безопасность; информационная сфера; обеспечение информационной безопасности; Доктрина информационной безопасности; информационные угрозы.

Original article

## NATIONAL SECURITY IN THE INFORMATIONAL ERA

Filatova E. V.<sup>1</sup>, Selezneva P. M.<sup>2</sup>

<sup>1</sup> Southern Federal University,  
Candidate of Law (PhD), Associate professor

<sup>2</sup> Southern Federal University,  
Student

The article provides a general description of the main provisions and principles of the Doctrine of Information Security of the Russian Federation, establishing its meaning and determining the priority areas for improving legal regulation in the information sphere. An opinion is expressed about the need to develop a specialized information retrieval thesaurus, as well as to systematize all terms in the information sphere according to the principle of vertical and horizontal classification. Attention is focused on the expediency of setting priorities according to the degree of importance solved by the Information Security Doctrine of tasks. The research methodology was general scientific and scientific methods, a special place among which is occupied by concrete sociological and modeling methods. The conclusion is made about the need to harmonize the interests of the state, civil society, and the individual in the field of national security. In the field of information security, an effective terminological policy allows you to share a set of knowledge, form, use and develop technical terminology among programmers, technical specialists, on the one hand, and lawyers, on the other.

*Keywords:* information security; national security; information sphere; ensuring information security; information security Doctrine; information threats.

В настоящее время невозможно представить свою жизнь без информационных технологий, а также без электронной обработки информации. В связи с этим, все больше граждан проводят значительную часть своего свободного времени в сети Интернет. Данное виртуальное пространство стало важной и неотъемлемой частью жизни людей, в связи с чем, мы можем

смело сказать, что сеть Интернет является зеркальным отражением нашего реального мира. Однако, с прогрессом и развитием персональной компьютерной техники зарождается и киберпреступность. Соответственно, киберпреступность и кибермошенничество являются одними из глобальных опасностей для Российской Федерации и для всего мира, в целом. В связи с этим большое количество ученых, правоведов и юристов уделяют особое внимание проблеме обеспечения информационной безопасности. На основании вышеизложенного отметим, что целью данной работы является изучение сущности Доктрины информационной безопасности Российской Федерации, утвержденной Указом Президента Российской Федерации от 5 декабря 2016 года № 646 (далее – Доктрина), так как данный документ, на наш взгляд, является одним из ключевых и основополагающих во всей системе обеспечения кибербезопасности. Видим острую необходимость проанализировать и сравнить, как сопоставляются задачи и цели обеспечения информационной безопасности в данном нормативном правовом акте с реальным их воплощением и реализацией в жизни.

Сферу информационной безопасности регулируют большое количество нормативно-правовых актов, среди которых: Доктрина информационной безопасности Российской Федерации [1], Федеральный закон «Об информации, информационных технологиях и о защите информации» [2], Федеральный закон «О связи» [3], Федеральный закон «О безопасности критической информационной инфраструктуры Российской Федерации» [4], Стратегия национальной безопасности Российской Федерации [5]. Данный список не является исчерпывающим, его дополняют ряд иных нормативных актов.

Проанализировав научную литературу, можно согласиться с мнением ученых о том, что Доктрина является центральным документом стратегического планирования, который стал основой для формирования и развития государственной политики и общественных отношений в сфере информационной безопасности. Так, уже в первой статье Доктрины указано, что она «представляет собой систему официальных взглядов на обеспечение национальной безопасности Российской Федерации в информационной сфере» [1]. Более того, она является основой для формирования общественных отношений и государственной политики в данной сфере. Необходимо отметить, что основополагающими национальными интересами в информационном пространстве являются: обеспечение и защита конституционных прав и свобод человека и гражданина, устойчивого и бесперебойного функционирования информационной инфраструктуры; развитие в Российской Федерации отрасли информационных технологий и электронной промышленности; содействие формированию системы международной информационной безопасности и доведение до российской и международной общественности достоверной информации о государственной политике Российской Федерации. Более того, Доктрина описывает состояние информационной безопасности и виды информационных угроз в различных областях нашего государства: общественная и государственная безопасность, наука, экономика, образование, технологии и так далее.

В ходе исследования были изучены различные подходы ученых к анализу Доктрины. Так, например, Н. М. Курбатов [6] и М. А. Капустина [7] расценивают данный документ, как концептуальную основу правового регулирования информационной сферы. Более того, в своих работах они высказывают мысль о том, что данная Доктрина является самым важным актом по формированию, развитию общественных отношений и государственной политики в сфере кибербезопасности нашей страны. Совершенно в другом направлении исследуют Доктрину Р. А. Абдусаламов, Л. В. Магдилова и Д. А. Рагимханова [8]. Сравнивая редакции Доктрины 2000 года и 2016 года, авторы приходят к выводу о том, что новая Доктрина, отражая интересы Российской Федерации, имеет перед собой цель привлечь нашу страну к более открытым, интенсивным и равноправным отношениям на мировой арене информационного пространства с иностранными государствами. Для этого в Доктрине уделено особое внимание развитию национальной системы управления российским сегментом сети Интернет. Однако, ученые считают, что без ущерба для нашей страны этой цели можно добиться только благодаря готовности отстаивать свой суверенитет и национальные интересы.



В научной статье А. Н. Прокопенко и А. А. Страхова приведены различные примеры антироссийской деятельности иностранных СМИ, общественных организаций, которые выпускают негативные материалы с ложной информацией о политике нашей страны, тем самым дискриминируя и дискредитируя нашу страну в международном сообществе. Противоположную позицию в своих научных трудах высказывает К. О. Полыхань [9], считая, что Доктрина делает акцент на наращивание информационного воздействия в целях размывания духовных и нравственных ценностей населения Российской Федерации. В особенности это оказывает огромное влияние на молодежь и детей в нашей стране. Более того, К. О. Полыхань осознает, что данная угроза появляется и распространяется за рубежом. Однако наши органы обязаны оказывать ей противодействие различными способами. Таким образом, можно прийти к выводу о том, что мнения научного сообщества по данному вопросу разительно отличаются.

Ряд правоведов говорят о том, что Доктрина является основополагающим нормативно-правовым актом в сфере информационной безопасности, вокруг которой уже в свою очередь выстраиваются другие правовые акты. Другие ученые высказывают свое мнение о том, что Доктрина не является системой официальных взглядов. Она только является официальным документом для привлечения нашей страны к более открытым отношениям с другими странами на мировой арене. Также многие ученые ведут активные споры по поводу пунктов, касающихся обеспечения духовной безопасности в информационном пространстве нашей страны. Так, некоторые правоведы высказывают свое мнение о том, что Доктрина оказывает негативное влияние на население нашей страны, размывая сложившиеся в Российской Федерации нравственные ценности. По нашему мнению, Доктрина является основным документом стратегического планирования в сфере информационной безопасности, поскольку она представляет собой систему официальных взглядов на обеспечение национальной безопасности Российской Федерации в указанной сфере. Более того, Доктрина указывает основополагающие угрозы международной информационной безопасности, цели и задачи государственной политики, основные направления реализации государственной политики и ее механизмы в области информационной безопасности.

В целях всестороннего и более глубокого изучения проблем информационной безопасности нами были использованы статистические материалы, полученные компанией «СёрчИнформ», где представлен аналитический обзор обеспеченности механизма реализации информационной безопасности с последующими выводами и рекомендациями. Компания «СёрчИнформ» провела анонимный опрос в 2019 году в российских компаниях и организациях информационных технологий, нефтегазовом секторе, кредитно-финансовой сфере, промышленности и транспорте, торговле, здравоохранении и других отраслях. В этом анонимном опросе приняли участие 1052 человека, которые являются специалистами подразделений информационной безопасности, эксперты и руководители организаций из коммерческой (76%), государственной (22%) и некоммерческой сфер (2%). Одним из главных выводов, который можно сделать на основании статистических материалов, заключается в том, что сама природа и динамика инцидентов показывает, что 77% компаний считают внутренние инциденты более опасными, чем внешние. Виновниками инцидентов информационной безопасности в большей мере являются рядовые сотрудники (73%), чем руководители компаний (27%). В результате приведенных данных было выявлено, что 59% российских компаний и организаций столкнулись в 2019 году с утечкой информации. Более того, были выявлены случаи «откатов» – 40%, промышленного шпионажа или работы в пользу конкурентов – 33%, явного саботажа – 17%, а также другие случаи правонарушений, связанных с проблемами информационной безопасности – 10%.

На основе анализа приведенных статистических материалов мы можем сделать следующий вывод: общая картина по обеспечению информационной безопасности показывает, что число утечек информации имеет тенденцию к их снижению. Однако, это касается только тех компаний, где действительно эффективно занимаются вопросами информационной безопасностью. При этом общее число инцидентов остаётся на критически высоком уровне,



как в Российской Федерации, так и в мире в целом.

Следующий вывод: оперативная информация и достоверные комментарии о случившемся в прессе или публичной сфере помогает нивелировать негативный эффект и смягчить как удар по своему имиджу, так и по финансовому и репутационному ущербу.

Несмотря на все вышеупомянутые сложности, нам бы хотелось выделить ключевую задачу в данном направлении: гармонизация интересов государства, гражданского общества и личности. Использование статистических данных позволило нам показать, что основная часть экспертного сообщества (77%) считают внутренние угрозы информационной безопасности более опасными, чем угрозы внешние. И это полностью коррелируется с одной из главных задач, поставленных Доктриной: обеспечение устойчивого и бесперебойного функционирования инфраструктуры Российской Федерации, в первую очередь критической.

Для повышения эффективности коммуникации между государством и обществом, нивелирования юридических и правовых ошибок в условиях развития информационного общества, необходимо решить следующие задачи в области информационной безопасности.

Во-первых, российское законодательство в информационной сфере нуждается в разработке классификаций понятий, терминов и систематизированного понятийного аппарата, характеризующего информационное пространство как в целом, так и его отдельные компоненты. Однако, стоит помнить, что в нормативных правовых актах информационной сферы огромную роль играют представители технических наук, а не юристы и правоведа. Большинство терминов в данной сфере приходят к нам из-за рубежа, и в последствии трансформируется. В связи с этим, проявляется сложность в адаптации нового термина в существующие правовые рамки. Так, термин «сайт» появился одним из первых в нашем законодательстве, однако его определение появилось намного позже. Из-за этого многие юристы не понимали в полном объеме, что именно он обозначает. В результате суды выносили решения, используя следующую формулировку «сайт конфисковать». В настоящее время сложно представить такие решения. Определение понятия сайт появилось только в Федеральном законе «Об информации, информационных технологиях и о защите информации» [2] в 2012 году. Также активно в юридической литературе используется термин «провайдер». Он употребляется, когда необходимо определить, кто должен был отвечать за контент в Интернете. Однако полное и исчерпывающее легальное определение в нашем законодательстве отсутствует. Существует определение термина «оператор связи», но его нельзя отождествлять с провайдером. Позднее появилось официальное определение понятия «провайдер хостинга», однако определение самого хостинга при этом отсутствует. Конечно, следует отметить, что данные определения имеются, например, в нормативных правовых актах города Москвы. Но, в то же время, понятия до сих пор остаются нераскрытыми и не позволяют соотнести провайдера хостинга с оператором связи и иными субъектами данной области права.

Видим актуальность в разработке информационно-поискового тезауруса, комплексного справочного словаря, который позволит аккумулировать в себе весь понятийный аппарат данной области в рамках отдельного комплекса стандартов. Для этого весь проработанный и классифицированный понятийный аппарат необходимо соотнести с терминами и определениями, которые уже закреплены в нормативных правовых актах и нормативно-технических документах для того, чтобы избежать ошибок и путаниц. Определяя механизм правового регулирования информационного пространства, недостаточно только выстроить систему отношений, которые подлежат регулированию. Необходимо также дать четкое определение понятий. Ведь юридическая терминология в любой сфере отношений характеризуется прежде всего: ясностью и понятностью слов и словосочетаний, одинаковые термины в нормативных правовых актах должны употребляться в одном и том же значении.

Для систематизации всех терминов в информационной сфере можно воспользоваться следующей классификацией: вертикальной и горизонтальной. Так, во главе вертикальной терминологии должен находиться основополагающий закон нашего государства. В нем закреплены термины широкого и обобщенного значения. Данные термины отличаются

простотой и общепонятностью в обществе, поскольку они широко распространены и часто употребляются не только в юридических науках, но и в обычной жизни. Однако, такие термины очень часто являются многозначными и допускаются их различное толкование среди правоведов, юристов и ученых. К данным терминам можно отнести: закон, государство, безопасность, государственная безопасность, безопасность личности, права и свободы личности, тайна переписки, телефонных переговоров, почтовых, телеграфных и иных сообщений, частная жизнь и другие.

Горизонтальная терминология, в свою очередь, охватывает виды отраслевой и межотраслевой терминологии. Так, под межотраслевой терминологией следует понимать терминологию, которая используется в нескольких отраслях законодательства. К данным терминам в информационной сфере можно отнести: документ, государственная тайна, информация, защита информации, Интернет, нарушитель, информационная безопасность, злоумышленник, мошенничество и многие другие. Отраслевая терминология в отличие от межотраслевой закрепляет понятий аппарат исключительно в особой отрасли законодательства, то есть образует пространство, которое не соотносится ни с межотраслевыми терминологическими полями, ни с общеправовыми. К таким терминам относятся: вирус, сайт, провайдер хостинга, кибервзломщик, киберпреступность, хакер, сетевая атака, информационная система, оператор информационной системы, доменное имя, поисковая система, идентификация, аутентификация. Данная классификация поможет законодателям и правоприменителям нивелировать проблемы формирования понятийного аппарата в информационной сфере, которые в настоящее время существуют в Российской Федерации. Ведь именно из-за отсутствия четкой систематизации данной терминологии и единого нормативного правового акта происходит рассредоточение терминов в данной сфере. Более того, в настоящее время не редкостью является ситуация, когда законодатель закрепляет одно и то же понятие и устанавливает за ним различные и отличные друг от друга дефиниции в разных законодательных актах.

Таким образом, для формирования понятийного аппарата и систематизации законодательства в сфере информационной безопасности необходимо прежде всего обеспечить высокий уровень терминологической политики. Она создается с целью регулирования терминологии в каждой сфере, в том числе и в информационной сфере, и формируется на стадиях принятия различных решений в языковой и правовой сферах. В результате создания эффективной терминологической политики и ее планирования создается большое количество языковых ресурсов, которые в последствии оказывают весомую поддержку для информационного представления знаний в конкретной предметной области. Более того, она помогает беспрепятственно коммуницировать специалистам из разных сфер и предметных областей. В сфере информационной безопасности эффективная терминологическая политика позволяет делиться набором знаний, формировать, использовать и разрабатывать терминологию технической направленности среди программистов, технических специалистов, с одной стороны, и правоведов, с другой. Более того, развитие данной политики позволяет осуществлять документирование, регистрацию, обработку, передачу знаний, терминологии, внедрение данной терминологии в практику, создавать ее толкование и локализацию.

Решение поставленных задач, позволит, усовершенствовать нормативно-правовую базу в данной сфере, повысить уровень грамотности людей, а также позволит организациям предотвращать преступления в области информационных технологий.

#### **Список источников:**

1. Доктрина информационное безопасности Российской Федерации утвержденная Указом Президента Российской Федерации от 5 декабря 2016 года № 646 // Российская газета. 2016.
2. Федеральный закон от 27.07.2006 г. № 149-ФЗ «Об информации, информационных технологиях и о защите информации» // Российская газета. 2006. № 4131.
3. Федеральный закон от 07.07.2003 г. № 126-ФЗ «О связи» // Российская газета. 2003. № 3249.

4. Федеральный закон от 26.07.2017 г. № 187-ФЗ «О безопасности критической информационной инфраструктуры Российской Федерации» // Российская газета. 2017. № 167.
5. Указ Президента РФ от 02.07.2021 г. № 400 "О Стратегии национальной безопасности Российской Федерации" // Собрание законодательства РФ. 2021. № 27. Ст. 5351.
6. Курбатов Н. М. Изменения в нормативном правовом регулировании обеспечения безопасности критической информационной инфраструктуры Российской Федерации // Экономика и право. 2019. № 3. С. 401–409.
7. Капустина М. А. Доктрина информационной безопасности России: правовое обеспечение национальных интересов Российской Федерации в информационном пространстве // Стратегические коммуникации в бизнесе и политике. 2018. № 4. С. 21–29.
8. Абдусаламов Р. А., Магдилова Л. В., Рагимханова Д. А. К вопросу о совершенствовании доктринальных положений в области обеспечения информационной безопасности // Юридический вестник. 2017. № 4. С. 165–169.
9. Польшань К. О. Проблемы и особенности состояние информационной безопасности в соответствии с Доктриной информационной безопасности Российской Федерации // Устойчивое развитие науки и образования. 2019. № 5. С. 154–160.

**References:**

1. Doktrina informatsionnoe bezopasnosti Rossiiskoi Federatsii utverzhdennaya Ukazom Prezidenta Rossiiskoi Federatsii ot 5 dekabrya 2016 goda № 646 // Rossiiskaya gazeta. 2016.
2. Federal'nyi zakon ot 27.07.2006 g. № 149-FZ «Ob informatsii, informatsionnykh tekhnologiyakh i o zashchite informatsii» // Rossiiskaya gazeta. 2006. № 4131.
3. Federal'nyi zakon ot 07.07.2003 g. № 126-FZ «O svyazi» // Rossiiskaya gazeta. 2003. № 3249.
4. Federal'nyi zakon ot 26.07.2017 g. № 187-FZ «O bezopasnosti kriticheskoi informatsionnoi infrastruktury Rossiiskoi Federatsii» // Rossiiskaya gazeta. 2017. № 167.
5. Ukaz Prezidenta RF ot 02.07.2021 g. № 400 "O Strategii natsional'noi bezopasnosti Rossiiskoi Federatsii" // Sovanie zakonodatel'stva RF. 2021. № 27. St. 5351.
6. Kurbatov N. M. Izmeneniya v normativnom pravovom regulirovanii obespecheniya bezopasnosti kriticheskoi informatsionnoi infrastruktury Rossiiskoi Federatsii // Ekonomika i pravo. 2019. № 3. S. 401–409.
7. Kapustina M. A. Doktrina informatsionnoi bezopasnosti Rossii: pravovoe obespechenie natsional'nykh interesov Rossiiskoi Federatsii v informatsionnom prostranstve // Strategicheskie kommunikatsii v biznese i politike. 2018. № 4. S. 21–29.
8. Abdusalamov R. A., Magdilova L. V., Ragimkhanova D. A. K voprosu o sovershenstvovanii doktrinal'nykh polozhenii v oblasti obespecheniya informatsionnoi bezopasnosti // Yuridicheskii vestnik. 2017. № 4. S. 165–169.
9. Polykhan' K. O. Problemy i osobennosti sostoyanie informatsionnoi bezopasnosti v sootvetstvii s Doktrinoi informatsionnoi bezopasnosti Rossiiskoi Federatsii // Ustoichivoe razvitie nauki i obrazovaniya. 2019. № 5. S. 154–160.

**Для цитирования:**

Филатова Е. В., Селезнева П. М. Национальная безопасность в информационную эпоху // Электронный научный журнал «Управление в экономических и социальных системах». 2022. № 4 (14). URL: <http://www.journal-mes.ru>

**For citation:**

Filatova E.V., Selezneva P. M. National security in the information era // Online scientific journal «Management in economic and social systems». 2022. no. 4 (14). URL: <http://www.journal-mes.ru>

**Сведения об авторах:**

*Филатова Елена Витальевна*, кандидат юридических наук, доцент Института управления в экономических, экологических и социальных системах, Южный федеральный университет, г. Таганрог, Россия  
 Контактная информация: [evfilatova@sfedu.ru](mailto:evfilatova@sfedu.ru)

*Селезнева Полина Михайловна*, студент Института управления в экономических, экологических и социальных системах, Южный федеральный университет, г. Таганрог, Россия.  
 Контактная информация: [pselezneva@sfedu.ru](mailto:pselezneva@sfedu.ru)

**Bio Notes:**

*Filatova Elena Vitalevna*, Candidate of Law, Associate professor of the Institute of Management in Economic, Ecological and Social Systems, Southern Federal University, Taganrog, Russia.

Contact information: [evfilatova@sfedu.ru](mailto:evfilatova@sfedu.ru)

*Selezneva Polina Mikhailovna*, student of the Institute of Management in Economic, Ecological and Social Systems, Southern Federal University, Taganrog, Russia.

Contact information: [pselezneva@sfedu.ru](mailto:pselezneva@sfedu.ru)

Статья поступила в редакцию 19.12.2022; одобрена после рецензирования 22.12.2022; принята к публикации 23.12.2022.

The article was submitted 19.12.2022; approved after reviewing 22.12.2022; accepted for publication 23.12.2022.



© 2022, Южный федеральный университет