Т. Ю. Галкина [T. Yu.Galkina]
Е. С. Гундарь [E. S. Goundar]

УДК 323.2

ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ КАК ФАКТОР НАЦИОНАЛЬНОЙ БЕЗОПАСНОСТИ И КОНКУРЕНТОСПОСОБНОСТИ ГОСУДАРСТВА

INFORMATION SAFETY AS A FACTOR OF NATIONAL SAFETY AND COMPETITIVE ABILITY OF THE STATE

ФГАО ВОУ Северо-Кавказский федеральный университет, г. Ставрополь, Россия

Аннотация. *Представлено авторское исследование содержания информационной безопасности в Российской Федерации, организационных структур информационной безопасности на Украине, во Франции, Германии, Великобритании и США. Проведено сравнительное изучение структурных компонентов информационной безопасности в указанных странах с 2000-х гг.*

Государства, определяющие политическую повестку в мире, стремятся обеспечить доминирование в информационной сфере и навязать свое видение другим игрокам мирового порядка. Всплеск интереса к информационной безопасности в РФ обусловлен тем, что страна достигла определенного прорыва во многих сферах жизнедеятельности общества, в том числе, политической, экономической (в том числе, после введения санкций по отношению к Российской Федерации значительно выросла доля производства отечественных товаров и предоставления услуг населению – импортозамещение), и, конечно, информационной. Доктрина информационной безопасности Российской Федерации 2016 г. показывает выход указанных проблем на уровень межгосударственного противостояния. Национальная безопасность страны невозможна без качественной реализации информационной безопасности как граждан, так и страны в целом.

Методы и материалы исследования. *В статье охарактеризованы тенденции развития информационной безопасности в Российской Федерации после разработки, утверждения и внедрения в стране Доктрины информационной безопасности в 2000 г. и утверждения новой Доктрины информационной безопасности 2016 г. Авторами применялся системный, сравнительный и структурно-функциональный подходы для исследования элементов национальной и информационной безопасности в Российской Федерации, США, Франции, Германии, а также на Украине, были сделаны выводы о качественной стороне этих процессов.*

Результаты *исследования акцентируют внимание на активном, но все же недостаточном развитии в России новой системы информационной безопасности (изменились как методы, так и масштабы информационных и хакерских угроз для нашей страны), ее качественным изменением, связи с развитием человеческого капитала, социальной и другими видами безопасности. В Российской Федерации сложилось государственное понимание того, что недостаточно иметь технологии и программное обеспечение. Важно иметь подготовленных специалистов, готовых к реализации задач будущего.*

Заключение *подтверждает авторские выводы о том, что обеспечить конкурентоспособность страны в информационном противоборстве, в первую очередь, могут необходимые и достаточные действия по формированию современной отечественной экономики, созданию новых высокотехнологичных рабочих мест, обеспечению роста благосостояния общества в целом, и, прежде всего, способность своевременно и эффективно реагировать на возникающие опасности и угрозы. Это подразумевает: становление и улучшение инфраструктуры российского информационного пространства; установление контроля за финансовыми потоками Интернет-торговли; реализация разъяснительных проектов среди населения об основах информационной безопасности; становление российской промышленности услуг информатизации и сохранение информационных ресурсов от неразрешённого доступа, обеспечение защищенности информационных и телекоммуникационных структур, как уже существующих, так и которые будут создаваться на территории Российской Федерации; привлечение гражданского общества к разработке критериев эффективности, закладываемых в основу «цифрового управления».*

Ключевые слова: безопасность, информационная безопасность, национальная безопасность, государственное управление, эффективность, мировой доминирование, кибербезопасность, социальная безопасность.

Abstract. *The authors' study of the content of information security in the Russian Federation, organizational structures of information security in Ukraine, France, Germany, the UK and the USA is presented. A comparative study of the structural components of information security in these countries since the 2000s has been carried out.*

The states that determine the political agenda in the world seek to ensure dominance in the information sphere and impose their vision on other players of the world order. The surge in interest in information security in the Russian Federation is due to the fact that the country has achieved a certain breakthrough in many areas of society's life, including political, economic (including after the

introduction of sanctions against the Russian Federation, the share of domestic goods and services import substitution to the population), and, of course, informational. The Doctrine of Information Security of the Russian Federation 2016 shows the emergence of these problems at the level of interstate confrontation. The national security of the country is impossible without the high-quality implementation of information security for both citizens and the country as a whole.

Methods and materials of the study. *The article describes the trends in the development of information security in the Russian Federation after the development of the Information Security Doctrine in the country in 2000 and the approval of the new Information Security Doctrine in 2016. The authors used a systematic, comparative and structural-functional approach to studies of elements of national and information security in the Russian Federation, USA, France, Germany, as well as in Ukraine, conclusions were made about the quality this side of these processes.*

The results *of the study focus on the active, but still insufficient development of the new information security system in Russia (both the methods and the scale of information and hacker threats for our country have changed), its qualitative change, and links with human capital development, social and other types of security in the Russian Federation, there is a state understanding that it is not enough to have technology and software. It is important to have trained professionals ready to fulfill the tasks of the future.*

Conclusion *confirms the author's conclusions that the country's competitiveness in informational confrontation, in the first place, can be necessary and sufficient actions to create a modern domestic economy, create new high-tech jobs, ensure the growth of the welfare of society as a whole, and, above all, the ability respond promptly and effectively to emerging dangers and threats. This implies: the formation and improvement of the infrastructure of the Russian information space; establishing control over the financial flows of online trading; implementation of explanatory projects among the population on the basics of information security; the formation of the Russian industry of information services and the preservation of information resources from unauthorized access, ensuring the security of information and telecommunication structures, both existing and to be created in the territory of the Russian Federation; involvement of civil society in the development of performance criteria that form the basis of "digital governance".*

Key words: security, information security, national security, government, efficiency, global domination, cyber security, social security.

Введение. Развитие Концепции информационной безопасности – современная, актуальная, задача, для разрешения которой в разных государствах выделяется существенная ресурсная база. Современный мир пронизан информационным противоборством, нацеленным на упрочение своих и ослабление других национальных, экономических и политических интересов.

Пристальное внимание политологов, философов, психологов к казалось бы технологической теме информационной безопасности обусловлено ее проникновением во все сферы человеческой деятельности. Согласно концепции А. Маслоу каждый нормальный взрослый человек в современном мире, «представитель нашей культуры прилагает все усилия, чтобы жить в безопасном, стабильном, организованном, предсказуемом мире, в мире, где существуют раз и навсегда установленные нормы и правила, где нет опасности» [1].

Материалы и методы исследования. Проведем сравнительное исследование развития системы информационной безопасности среди стран, активных на политической арене. Анализу подвергнем структуру и нормативную базу, ориентированную на информационную безопасность. Авторы использовали системный, сравнительный и структурно-функциональные подходы при изучении системы информационной безопасности в Российской Федерации, США, Франции, Германии, а также на Украине.

Результаты исследования. Во многих современных государствах уже произошли в полном объеме изменения связанные с информационными технологиями, совершился резкий взлет в производстве, накоплении, обработки, передаче и переработке информации. Но в действительности это означает, что информационное поле все чаще используется в корыстных целях для реализации политических, экономических и общественных целей.

В Германии создано Федеральное управление по информационной безопасности (BSI), основанное на многолетнем опыте Федеральной разведывательной службы Германии. Для усиления деятельности в части информационной безопасности в 2011 г. был создан Национальный центр кибербезопасности (NCAZ).

Информационная безопасность как комплексная программа реализуется в США, в первую очередь, Агентством Национальной безопасности и Разведывательным сообществом США (17 отдельных правительственных учреждений). С 2011 г. в соответствии с доктриной национальной безопасности США был построен и в 2013 г. введен в действие первый в мире дата-центр, позволяющий обрабатывать «все виды коммуникаций».

Ориентация на тотальное мировое доминирование прослеживается через рассуждения аналитиков «Вашингтон Пост» о том, что информационное развитие привело к тому, что тактика сдерживания гораздо более

проблематична, чем в «холодную войну», из-за того, что они назвали «проблемой атрибуции». «В ядерной войне, было бы легко выяснить, кто запустил ядерное оружие и принять ответные меры. В сфере информации – это совсем не просто. Злоумышленники часто скрываются за техническими средствами. И даже когда криминалистические методы могут быть использованы для отслеживания атаки (скажем, на IP-адрес в Китае), зачастую невозможно определить, работали ли хакеры, например, на китайское правительство или вооруженные силы, или работали на их собственный аккаунт.

Если Вы не знаете, кто атаковал Вашу компьютерную систему, Вы не можете нанести ответный удар по ним. Даже если у вас есть достаточно хорошее представление о том, кем был злоумышленник, вы не сможете доказать это, а другие государства могут не поверить в ваши претензии и осудить вас как агрессора. Если вы не знаете, кто на вас напал, вы не можете угрожать, чтобы наказать их; и вы не можете легко удержать их от нападения на вас» [2].

В Великобритании (GCHQ) подразделение информационной безопасности включает группу подразделений, в том числе, Национальный центр кибербезопасности. Центр внедрения современных технологий стратегических коммуникаций НАТО (НАТО StratCom COE) был основан также в Латвии в 2014 г.

Первоначально «информация» понималась как сведения, которые передаются от человека к человеку, любым удобным для него способом: письменным, устным, а также с помощью различных технических средств, например, сигналов.

Говоря иными словами, информация носит надежный и разносторонний характер, являясь полисемантичным понятием. Эту мысль можно аргументировать словами Н. Винера, основателя кибернетики: «Информация есть информация, а не энергия и не материя».

Согласно укоренившейся философской точки зрения, информация живет и находится автономно от человека и является характерной особенностью материи, а общепринятое определение безопасности в этой сфере - защищенность от воздействия угроз.

При всем этом начальным пунктом при рассмотрении опасностей информационной безопасности считается установление элемента информационной безопасности, который является опасным, секретным и создает уязвимость.

Информационной безопасности как зоне ответственности каждого гражданина посвящены современные учебные пособия [3]. Во многих странах издаются пособия, нацеливающие обучать персонал грамотности информационной безопасности [4].

Президентом РФ В.В. Путиным неоднократно озвучивалась задача по формированию нового поколения квалифицированных специалистов, способных к реализации национальных и политических интересов в информационном поле. Одновременно в местных и федеральных органах государственной власти происходит поиск места и роли информационного будущего.

В современной России формирование информационной безопасности сопряжено с развитием таких составляющих, как наукоемкие технологии, цифровая экономика, развитие промышленности и импортозамещения, сохранение традиций, идентичности, в целом развитие культуры общества.

Защита информации необходима во всех сферах: от военной до социальной. Например, в аграрной сфере планируется генное редактирование, создание «умных хранилищ», роботизация, автоматизированные режимы ухода за растениями и ветеринарного контроля. В соответствии с концепцией устойчивого развития агропромышленного комплекса до 2030 г., беспилотными станут комбайны и сеялки, - заявила вице-президент РАН И. Донник в Совете Федерации 18 мая 2018 г. Председатель Комитета Государственной Думы РФ по финансовому рынку А. Аксаков прогнозирует, что в экономической сфере, в связи с увеличением объема рынка Интернет-торговли в России (с 405 млрд. руб. в 2012 г. до 920 млрд. руб. в 2016 г.), в России существенно увеличилась доля безналичных расчетов, в будущем возможен отказ от «живых денег» [5].

В 2016 г. Указом Президента РФ подписан Указ об утверждении Доктрины информационной безопасности РФ, заложившей новый этап развития отечественной информационной безопасности. До 2016 г. информационная безопасность регламентировалась Доктриной 2000 г., в которой основное внимание было уделено созданию правовых регламентов и обоснованию тесной взаимосвязи стремительного развития информационных систем и национальной безопасности РФ. С 2000 г. по 2016 нормативно-правовая база по обеспечению информационной безопасности охватила все субъекты РФ.

По сравнению с Доктриной 2000 года в новом документе смещен акцент с «обеспечения свободного доступа любого гражданина к информационным ресурсам и технологиям связи к обеспечению безопасности взаимодействия людей с информационным пространством. Отдельно озвучена необходимость развития отечественной отрасли информационных технологий, поскольку сильная зависимость от иностранных продуктов и разработок повышает уровень влияния от иностранных игроков.

Следующий момент – стратегия обеспечения информационной безопасности РФ в глобальной сети Интернет. В новой Доктрине 2016 г. сделан акцент на «правдивом донесении информации о нашей стране, описан комплекс мер по соблюдению и достижению национальных интересов РФ в Интернете, а также по обеспечению и защите граждан в цифровом пространстве» [6]. В документе внимание уделено киберпреступлениям бытовой, социальной и информационно-культурной сфере, в кредитно-финансовой сфере. Отдельно указана информационная угроза террористических групп и девальвация системы ценностей молодежи «сетевыми» акторами. Если традиционная парадигма ведения информационного противоборства основана на характеристике «владение ценной информацией», то в информационной войне побеждает не тот, кто владеет информацией, а кто может ее убедительнее преподнести.

Российская Федерация неоднократно выступала с предложением создания международного органа, регулирующего деятельность Интернет-пространства, функционирующего по уровню и принципам ООН.

Безусловно, национальная безопасность должна иметь эффективные меры, против «информационно-психологического воздействия иностранных спецслужб», а также организаций, «осуществляющих разведку» российских государственных органов, научных организаций и предприятий оборонно-промышленного комплекса» и т.д.

Особенно четко актуальность выявлена после принятия Европарламентом резолюции о стратегической коммуникации ЕС для противодействия пропаганде против нее со стороны третьих лиц 2016/2030(INI). Данная резолюция формулирует стратегию и методы борьбы с пропагандой против ЕС России и, как ни странно, одновременно ИГИЛ. В резолюции однозначно определяется факт информационной войны между РФ и ЕС. Понимание Европейским парламентом информационной войны исходит из исторического противостояния времен холодной войны, получившего в современное время форму гибридной войны.

Основными целями деятельности российских СМИ и инфокоммуникационных технологий в странах ЕС в резолюции названы: «подрыв согласованности внешней политики ЕС», «угроза суверенитету государств-членов ЕС», «инвестирование Кремлем в дезинформацию и пропаганду в псевдо-новостные агентства и мультимедиа услуги», «наличие намерения поддерживать политический экстремизм», «широкая подрывная деятельность по ослаблению сотрудничества ЕС» [7].

С одной стороны, данная резолюция подтверждает существенно возросший уровень российских технологий в рассматриваемой сфере, однако по мнению российских специалистов как никогда остро стоят технологии «информационной войны». Возрастает угроза компьютерных атак на объекты значимой инфраструктуры, от социальных объектов политических структур до ядерных объектов.

Исследование основ информационной защищенности показывает, что проблема безопасности в информационной сфере является проблемой единой. С одной стороны, информационная защищенность подразумевает, как минимум, предоставление трех ее образующих – общедоступность, единство и секретность сведений. С другой точки зрения, данными и информативными системами в полном смысле «пронизаны» достаточно многие сферы политики, и воздействие данных в политику всегда наращивается. В последний период появилось и получило активное распространение явление «фейковых новостей» (пример, дело Скрипалей), «фейковых политиков» (Б. Джонсон в Великобритании и др.).

Также проблему для нормального функционирования экономики в общих чертах, представляют преступления, связанные непосредственно, с компьютерами, с проникновением правонарушающих элементов в сети и компьютерные системы кредитных организаций и банков.

Несовершенность правовой базы, которая определяет ответственность субъектов за неполноту или утаивания сведений об их рыночной деятельности, о свойствах производимых ими услуг и товаров, об инвестициях, о результатах их деятельности, затрудняет правильное функционирование экономических субъектов.

Немаловажный экономический ущерб политическим и экономическим субъектам может быть нанесен благодаря оглашению информации третьим лицам, в которой может содержаться коммерческая или даже государственная тайна. Среди основных процессов: систематизирование сбора, хранении, передачи и обработки

налоговой, биржевой, финансовой информации, - самыми опасными являются копирование, искажение благодаря случайным и (или) преднамеренным нарушениям методикам работы с информацией, неправомерного доступа к ней.

Данное действие также касается исполнительной власти, которое уполномочено распространять и формировать информацию о внешней деятельности государства. Так, казалось бы шуточное «пранк-расследование» в разное время осуществившее разведку информации «от первого лица» у президента Украины П. Порошенко, сенатора США Дж. Маккейна и генсека НАТО Й. Столтенберга, а авторы и исполнители (А. Столяров и В. Кузнецов), стали неотъемлемой частью альтернативной публичной дипломатии нашей страны и были избраны членами Экспертного совета по развитию информационного общества и СМИ в структуре Молодежного парламента при Государственной Думе РФ.

Законодательные мероприятия в области информационной защищенности ориентированы в формирование в государстве законодательной основы, упорядочивающей и регламентирующей действия субъектов взаимоотношений.

Согласно формированию нормативной основы информационной безопасности, среди приоритетов национальной безопасности страны - исследование новейших, либо исправление имеющихся законов, утверждений, распоряжений и руководств, а кроме того формирование эффективной концепции регулирования, контролирования реализации отмеченных регламентирующих документов. До начала 2010 – хх гг. телевидение, Интернет и другие средства массовой информации в своем роде являлись лишь «информационной витриной» активности местного самоуправления и государственной власти, в целом политического имиджа государства [8, с. 45-46].

В Российской Федерации разработана и утверждена Программа правительства по цифровой экономике до 2024 г. и ряд федеральных проектов, в том числе, федеральный проект «Цифровая трансформация государственного управления», выбраны пилотные проекты для цифровизации местного самоуправления (республиках Мордовия, Чувашия, Марий Эл, Брянская и Тамбовская области, Тюменская область и Пермский край). Основная цель данного проекта – повышение, как самой эффективности государственного управления, так и доверия граждан к органам власти.

Заключение. В сущности, в современном информационном обществе постоянно нарастают процессы совершенности политических решений, увеличивается транспарентность работоспособности власти, а народ и их общественные организации получают намного больше возможностей участвовать в регулировании обществом, что, в том числе, обеспечивает и социальную безопасность.

В целом социальная безопасность обеспечивается следующими показателями:

– для того, чтобы удовлетворить нужду людей, необходимо улучшить качество жизни общества;

– острота реагирования общества и государства на кризисные случаи;

– обновление отживших социальных институтов и структур и адаптация их под новые условия;

– увеличение социально-психологической осведомленности власти, общества;

– преодоление искажения системы отношений.

Активные пользователи за счет создания и продвижения социальных сетей, всё более интенсивно общаются между собой, стараясь обойти стороной, государственный контроль и государственное участие.

Следует отметить, что подобная деятельность проводится почти постоянно, так как область информационных технологий формируется быстро, в соответствии с этим возникают новейшие аспекты взаимоотношений, как в государственной, так и негосударственной сферах. С 2000 года (год принятия в Окинаве Хартии об информационной безопасности) существенно изменилось содержание угроз, методов информационной безопасности [9]. Современные международные агенты влияния, в том числе провоцирующие «размывание духовно-нравственных ценностей» граждан РФ должны почувствовать результаты реально действующей Доктрины информационной безопасности РФ.

В 2019 г. продолжается обсуждение законопроекта об управлении Рунета. Роскомнадзор будет следить и за тем, чтобы минимум внутрироссийского трафика шел по зарубежным сетям, а в критических ситуациях управление сетями будет брать на себя специальный центр. Федеральный закон от 01.05.2019 № 90-ФЗ «О внесении изменений в Федеральный закон «О связи» и Федеральный закон «Об информации, информационных технологиях и о защите информации» нормативно усилил защиту национальной системы информационной безопасности.

Важным моментом долгое время являлось и неудовлетворительное состояние защиты информации у организаций и предприятий областей национальной промышленности, обеспечивающей средства связи и телекоммуникации, использовавших пакет зарубежных средств, что к настоящему времени уже создало угрозу технологической подчинённости Российской Федерации от зарубежных государств. Практика импортозамещения позволила снизить эту угрозу, в том числе, от стран Европейского Союза [10, P. 1018-1020].

Несомненно, обеспечить конкурентоспособность страны в информационном противоборстве, в первую очередь, могут необходимые и достаточные действия по формированию современной отечественной экономики, созданию новых высокотехнологичных рабочих мест, обеспечению роста благосостояния общества в целом, и, прежде всего, способность своевременно и эффективно реагировать на возникающие опасности и угрозы. Это подразумевает

– становление и улучшение инфраструктуры российского информационного пространства;

– установление контроля за финансовыми потоками Интернет-торговли;

– реализация разъяснительных проектов среди населения об основах информационной безопасности;

– становление российской промышленности услуг информатизации и сохранение информационных ресурсов от неразрешённого доступа, обеспечение защищенности информационных и телекоммуникационных структур, как уже существующих, так и которые будут создаваться на территории Российской Федерации;

– привлечение гражданского общества к разработке критериев эффективности, закладываемых в основу «цифрового управления».

ЛИТЕРАТУРА

1. Maslow A. Motivation and Personality/ Trans. from English. SPb.: Peter. 2006. 352 p.

2. Политология кибербезопасности. // The Washington Post. [Электронный ресурс]. URL: https://www.washingtonpost.com/news/monkey-cage/wp/2014/02/20/the-political-science-of-cybersecurity-iii-how-international-relations-theory-shapes-u-s-cybersecurity-doctrine/?noredirect=on&utm_term=.b77f825fedcc (Дата обращения: 10.02.2019).

3. Straub D. W., Goodman S., Baskerville R. L. Information Security: Policy, Processes, and Practices. Advances in Management Information Systems. N.Y., 2008. 288 p.

4. Bogatenkov S. Implementation of information security during the personnel training in Russia // Modern European Researches. 2014. № 3. С. 12-15.

5. Расчеты наличными за онлайн-покупки уйдут в прошлое» // Парламентская газета. 30.11.2017. URL: https://www.pnp.ru/economics/raschyoty-nalichnymi-za-onlayn-pokupki-uydyot-v-proshloe.html. (Дата обращения: 15.07.2019).

6. Указ Президента Российской Федерации от 05.12.2016 № 646 «Об утверждении Доктрины информационной безопасности Российской Федерации» // Официальный интернет-портал правовой информации [Электронный ресурс]. URL: http://publication.pravo.gov.ru/Document/View/0001201612060002 (Дата обращения: 10.02.2019).

7. On EU strategic communication to counteract propaganda against it by third parties // European Parliament [Электронный ресурс]. URL: http://www.europarl.europa.eu/doceo/document/A-8-2016-0290_EN.html (Дата обращения: 11.05.2019).

8. Койбаев Б. Г. Политический имидж государства в современном глобальном информационном пространстве // Вестник Северо-Осетинского государственного университета имени Коста Левановича Хетагурова. Владикавказ: Изд-во СОГУ, 2013. № 1. С. 45-48.

9. Summit 2000. Okinawa: Government of Japan, July 22 // URL: http://www.g8.utoronto.ca/summit/2000okinawa/gis.htm).

10. Galkina E. V., Ogneva V. V., Bolkhovitina T. S., Moiseev V. V. Problems of Relations between Russia and European Union under Conditions of Sanctions // The European Proceedings of Social & Behavioural Sciences EPSBS. Tomsk: Future Academy, 2017. Vol. XXXV. № 119. P. 1018-1026.

REFERENCES

1. Maslow A. Motivation and Personality/ Trans. from English. SPb.: Peter. 2006. 352 p.

2. Politologiya kiberbezopasnosti. // The Washington Post. [Ehlektronnyy resurs]. URL: https://www.washingtonpost.com/news/monkey-cage/wp/2014/02/20/the-political-science-of-cybersecurity-iii-how-international-relations-theory-shapes-u-s-cybersecurity-doctrine/?noredirect=on&utm_term=.b77f825fedcc (Data obrashcheniya: 10.02.2019).

3. Straub D. W., Goodman S., Baskerville R. L. Information Security: Policy, Processes, and Practices. Advances in Management Information Systems. N.Y., 2008. 288 p.

4. Bogatenkov S. Implementation of information security during the personnel training in Russia // Modern European Researches. 2014. № 3. С. 12-15.

5. Raschety nalichnymi za onlayn-pokupki uydut v proshloe» // Parlamentskaya gazeta. 30.11.2017. URL: https://www.pnp.ru/economics/raschyoty-nalichnymi-za-onlayn-pokupki-uydyot-v-proshloe.html. (Data obrashcheniya: 15.07.2019).

6. Ukaz Prezidenta Rossiyskoy Federatsii ot 05.12.2016 № 646 «Ob utverzhdenii Doktriny informatsionnoy bezopasnosti Rossiyskoy Federatsii» // Ofitsial'nyy internet-portal pravovoy informatsii [Ehlektronnyy resurs]. URL: http://publication.pravo.gov.ru/Document/View/0001201612060002 (Data obrashcheniya: 10.02.2019).

7. On EU strategic communication to counteract propaganda against it by third parties // European Parliament [Ehlektronnyy resurs]. URL: http://www.europarl.europa.eu/doceo/document/A-8-2016-0290_EN.html (Data obrashcheniya: 11.05.2019).

8. Koybaev B. G. Politicheskiy imidzh gosudarstva v sovremennom global'nom informatsionnom prostranstve // Vestnik Severo-Osetinskogo gosudarstvennogo universiteta imeni Kosta Levanovicha Khetagurova. Vladikavkaz: Izd-vo SOGU, 2013. № 1. S. 45-48.

9. Summit 2000. Okinawa: Government of Japan, July 22 // URL: http://www.g8.utoronto.ca/summit/2000okinawa/gis.htm).

10. Galkina E. V., Ogneva V. V., Bolkhovitina T. S., Moiseev V. V. Problems of Relations between Russia and European Union under Conditions of Sanctions // The European Proceedings of Social & Behavioural Sciences EPSBS. Tomsk: Future Academy, 2017. Vol. XXXV. № 119. P. 1018-1026.

Доля соавторов

Галкина Татьяна Юрьевна (аннотация, введение, материалы и методы исследования, заключение) – 50 % авторского текста статьи,

Гундарь Елена Сергеевна (методы исследования, обработка результатов исследования, часть заключения) – 50 % авторского текста статьи.

С благодарностью научному руководителю, доктору политических наук Галкиной Елене Вячеславовне!

ОБ АВТОРАХ

Галкина Татьяна Юрьевна, аспирант кафедры зарубежной истории, политологии и международных отношений Гуманитарного института Северо-Кавказского федерального университета, anusha58@rambler.ru, 355009, г. Ставрополь, ул. Пушкина, 1

Galkina Tatiana Yuryevna, PhD student of the Department of foreign history, political science and international relations, Humanities Institute of the North Caucasus Federal University, anusha58@rambler.ru, 355009, 1, Pushkina street, Stavropol.

Гундарь Елена Сергеевна, Кандидат политических наук, доцент кафедры зарубежной истории, политологии и международных отношений, Гуманитарного института Северо-Кавказского федерального университета, 24-04@mail.ru, 355009, г. Ставрополь, ул. Пушкина, 1

Goundar Elena Sergeevna, Candidate of Political Sciences, PhD of the Department of foreign history, political science and international relations, Humanities Institute of the North Caucasus Federal University, 24-04@mail.ru, 355009, 1, Pushkina street, Stavropol.

Дата поступления в редакцию: 01.02.2019 г.
После рецензирования: 12.04.2019 г.
Дата принятия к публикации: 26.05.2019 г.