УДК 004.056
DOI: 10.18384/2310-7227-2022-2-76-83

ГЛОБАЛИЗАЦИЯ И ЕЁ ВОЗДЕЙСТВИЕ НА ИНФОРМАЦИОННУЮ БЕЗОПАСНОСТЬ РОССИЙСКОЙ ФЕДЕРАЦИИ

Гурьянов Н. Ю.[1], Пальмов С. В.[2]
[1]Медицинский университет «Реавиз»
443001, г. Самара, ул. Чапаевская, д. 227, Российская Федерация
[2]Поволжский государственный университет телекоммуникаций и информатики
443010, г. Самара, ул. Льва Толстого, д. 23, Российская Федерация

Аннотация
Цель. Рассмотреть последствия глобализации в информационной сфере и оценить их влияние на информационную безопасность Российской Федерации.
Процедура и методы. В исследовании последовательно рассматриваются последствия глобализации в информационной сфере, а также связанные с ними проблемы и перспективы информационной безопасности РФ, включая противодействие угрозам информационного терроризма и инфогенным катастрофам. В ходе исследования комплексно применяются методы анализа и синтеза, диалектический, компаративный и прогностический методы.
Результаты. В исследовании показано, что в условиях глобализации возрастает число информационных угроз и пропорционально увеличивается нагрузка на службы информационной безопасности РФ. Самой значительной угрозой информационной безопасности РФ признаётся потенциальная возможность глобальных инфогенных катастроф, источниками которых могут стать сбои и нарушения в программных продуктах различных государств при осуществлении международных проектов.
Теоретическая и/или практическая значимость. В исследовании выявляются положительные (увеличение доступного объёма информации о технологиях и стимулирование разработки российского программного обеспечения) и отрицательные (рост киберпреступлений и зависимость от зарубежных программных продуктов) факторы, оказывающие влияние на информационную безопасность РФ. Последние анализируются в контексте их практической реализации – ещё не завершившейся пандемии COVID-19 и введённого западными странами режима беспрецедентного санкционного давления на Россию.

Ключевые слова: глобализация, инфогенная катастрофа, информационная безопасность, информационная сфера, информационный терроризм, киберпреступность

GLOBALIZATION AND ITS IMPACT ON THE INFORMATION SECURITY OF THE RUSSIAN FEDERATION

N. Guryanov[1], S. Palmov[2]
[1]Reaviz Medical University
ul. Chapaevskaya 227, Samara 443001, Russian Federation
[2]Povolzhskiy State University of Telecommunications and Informatics
ul. Lva Tolstogo 23, Samara 443010, Russian Federation

Abstract
Aim. To consider the consequences of globalization in the information sphere and assess their impact on the information security of the Russian Federation.

Methodology. The study consistently examines the consequences of globalization in the information sphere, as well as the related problems and prospects of information security of the Russian Federation, including countering the threats of information terrorism and infogenic disasters. In the course of the study, methods of analysis and synthesis, dialectical, comparative and prognostic methods are used complexly.

Results. The study shows that in the context of globalization, the number of information threats increases and the burden on the information security services of the Russian Federation increases proportionally. The most significant threat to the information security of the Russian Federation is recognized as the potential for the global infogenic catastrophes, the sources of which may be failures and violations in software products of various states in the implementation of international projects.

Research implications. The study identifies positive (increasing the available amount of information about technologies and stimulating the development of Russian software) and negative (the growth of cybercrime and dependence on foreign software products) factors affecting the information security of the Russian Federation. The latter are analyzed in the context of their practical implementation – the COVID-19 pandemic that hasn't yet ended and the regime of unprecedented sanctions pressure imposed on Russia by Western countries.

***Keywords*:** globalization, infogenic catastrophe, information security, information sphere, information terrorism, cybercrime

Введение

Под глобализацией традиционно понимается процесс усиления взаимозависимости, взаимопроникновения и взаимообусловленности экономических, политических, культурных и прочих экзистенциальных параметров мирового сообщества. Данный феномен весьма неоднозначно оценивается исследователями. Однако несмотря на то, что многие современные авторы настроены решительно против тенденций развёртывающейся всеобщей интеграции и унификации, в XXI в. глобализация воспринимается, скорее, как данность – как очередной, неизбежно наступающий этап в эволюции человечества [1, с. 63–64].

Признаки грядущей глобализации в полной мере стали проявляться ещё в XX столетии, в том числе через посредство трансформации английского языка в язык мирового общения. Изменения в валютных системах (повсеместное распространение доллара, создание евро, отмирание национальных валют) также подготовили почву для предстоящей глобализации, которая повлекла за собой кардинальные изменения в жизни общества, и в наибольшей степени в экономической сфере, а именно – в её транснационализации[1]. В свою очередь, это привело к формированию единого экономико-финансового и информационного пространства. В результате многие процессы хозяйственной жизнедеятельности переместились в сеть, и информация стала одним из ключевых факторов обеспечения безопасности государства. В этой связи информационная безопасность становится одним из важнейших элементов системы национальной безопасности любого современного государства.

В соответствии с Доктриной информационной безопасности Российской Федерации, информационная безопасность – «состояние защищённости личности, общества и государства от внутренних и внешних информационных угроз, при котором обеспечиваются реализация конституционных прав и свобод человека и гражданина, достойные качество и уровень жизни граждан, суверенитет, территориальная целостность и устойчивое социально-экономическое развитие Российской Федерации, оборона и безопасность государства»[2].

[1] Глобализация // Национальная энциклопедическая служба: [сайт]. URL: https://voluntary.ru/termin/globalizacija.html (дата обращения: 27.03.2022).

[2] Указ Президента РФ от 5 декабря 2016 г. N 646 «Об

Последствия глобализации в информационной сфере

С каждым годом информация в современном мире становится всё более доступной. С одной стороны, это может быть признано неоспоримым преимуществом: государство получает доступ к новейшим зарубежным технологиям и разработкам, а организациям обеспечивается возможность получения ценных сведений о конкурентах. Но, с другой стороны, свободно циркулирующая информация может оказаться заведомо ложной или искажённой, ставящей целью ввести в заблуждение её потенциальных пользователей. Последнее ведёт к девиациям общественного сознания, попыткам манипулировать им в сомнительных интересах разнородных политических и идеологических структур.

Кроме того, доступность информации привела к появлению одной из самых значимых проблем нашей современности – информационной избыточности, или перенасыщению информацией. В случае переизбытка информации пользователь может либо анализировать сведения, поступающие к нему из различных источников, либо принимать в качестве достоверной наиболее примитивную информацию, изложенную самым простым языком. В таких условиях очевидной является потребность в критической рефлексии или, как минимум, в сомнении в качестве любой получаемой информации.

Сомнение, как известно, выступает неотъемлемым элементом когнитивной активности человека, однако ввиду необходимости анализировать чрезмерный поток информации эффективность данной интеллектуальной процедуры существенно снижается. Это обстоятельство оказывает негативное и даже разрушительное воздействие на психическое и физическое здоровье пользователей сети. Имеет место также формирование у населения мнения и мировоззрения, выгодных заправляющим этим процессом третьим лицам, в том числе в плане привития требуемого отношения к власти, государственным структурам и пр. Открытость информации может положить начало информационным войнам. Таким образом, доступность информации является и значительной угрозой одновременно.

Не менее важной задачей, актуализирующийся ввиду избытка доступной информации, является сохранение сведений, составляющих государственную или коммерческую тайну, а также иной информации ограниченного доступа. Такая информация может быть не только украдена, но и вновь добавлена в базы данных в искажённом виде, что может привести к нарушениям в работе отдельных структур, дестабилизации политической и экономической ситуации в Российской Федерации. Предотвращение подобных эксцессов требует пристального внимания и больших усилий со стороны сотрудников служб информационной безопасности [6, p. 45].

Очевидно, что с технической точки зрения перемещение множества процессов в сеть создаёт перегрузку глобальной информационной системы в целом. Особенно заметной реализация данной угрозы стала в контексте недавних событий, а именно ограничительных мер, направленных на противодействие ещё не исчерпавшей себя коронавирусной инфекции, приведшей к пандемии и введению «всемирного карантина». Большинство компаний, не связанных напрямую с производством и сельским хозяйством, переводили своих работников на удалённый режим работы. Аналогичный процесс стартовал и в учебных заведениях, начавших внедрять дистанционный или смешанный формат обучения. Вследствие необходимости обрабатывать значительно больший объём данных, чем тот, на который рассчитан сетевой узел, учащались случаи сбоев программных продуктов [5, p. 570]. Между тем, в этой связи могут пострадать важнейшие системы жизнеобеспечения государства и населения.

Следует также признать, что наибольшую угрозу информационной безопасно-

утверждении Доктрины информационной безопасности Российской Федерации» // Гарант: [сайт]. URL: https://base.garant.ru/71556224 (дата обращения: 27.03.2022).

сти РФ, как и любого другого государства в эпоху глобализации, представляет собой возможность осуществления нового вида катастроф, наступающих по причине сбоев или нарушений в глобальных информационно-телекоммуникационных сетях. Эту разновидность катастроф принято называть инфогенной. Особая опасность связана с взаимозависимостью и взаимообусловленностью множества процессов. К примеру, сбои в системе информационного обеспечения авиационной и железнодорожной безопасности лишь одного государства при осуществлении международных рейсов способны парализовать транспортное сообщение. В случае реализации этой угрозы пострадает не только информационная сфера государства, но и все остальные элементы системы национальной безопасности.

Проблемы и перспективы информационной безопасности РФ

Необходимость интегрирования в мировые процессы высвечивает недостаточность уровня развития и внедрения отечественных разработок в области информационных технологий. В настоящее время в российской сфере IT наблюдаются зависимость от иностранных технологий и отсутствие конкурентоспособных отечественных продуктов. В связи с этим многие сферы национальных интересов РФ находятся в зависимости от предоставления зарубежными странами права пользования разработанными ими программами и техническим оборудованием[1]. При худшем сценарии это может привести к преднамеренной или непреднамеренной информационной блокаде России в случае ухудшения отношений со странами-экспортерами программного обеспечения.

Данная угроза стала реальностью в 2022 г., когда в условиях введённых против России масштабных санкций с ней отказались сотрудничать многие крупнейшие западные IT-компании. Речь идёт об отказе от продаж компьютерной техники и комплектующих, непредоставлении сервисных услуг по уже имеющемуся оборудованию, отключении от мировых платёжных систем и др. Проблемы могут возникать и в уже функционирующих системах, предоставленных России зарубежными производителями, т. к. как сохраняется возможность запуска вирусов и различных вредоносных программ в отечественные базы данных.

Ещё одной злободневной для России проблемой, связанной с необходимостью обеспечения исправного функционирования IT-сферы, является человеческий фактор, в частности, массовый отток из страны представителей данной отрасли, связанный с введением санкционного режима[2]. В целях их удержания в отношении IT-сферы был введён комплекс стимулирующих мер, многие из которых уже начали действовать, в том числе грантовая поддержка перспективных IT-проектов, льготное кредитование IT-организаций, повышение заработной платы и улучшение жилищных условий IT-специалистов, предоставление им отсрочки от призыва на военную службу и пр.[3].

2 марта 2022 г. «в целях обеспечения ускоренного развития отрасли информационных технологий в Российской Федерации»[4] был издан указ президента РФ, в который вошли постановления, направленные «на установление до 31 декабря 2024 г. для аккредитованных организаций налоговой ставки по налогу на прибыль организаций в размере 0 процентов; на упрощение процедур трудоустройства иностранных граждан, привлекаемых для ра-

[1] Указ Президента РФ от 5 декабря 2016 г. N 646 «Об утверждении Доктрины информационной безопасности Российской Федерации» // Гарант: [сайт]. URL: https://base.garant.ru/71556224 (дата обращения: 27.03.2022).

[2] IT-специалисты десятками тысяч уезжают из России // CNEWS: [сайт]. URL: https://www.cnews.ru/news/top/2022-03-22_poslableniya_ne_pomogayut (дата обращения: 27.03.2022).

[3] Указ Президента Российской Федерации от 02.03.2022 № 83 «О мерах по обеспечению ускоренного развития отрасли информационных технологий в Российской Федерации» // Президент России: [сайт]. URL: http://www.kremlin.ru/acts/bank/47593 (дата обращения: 27.03.2022).

[4] Там же.

боты в аккредитованных организациях, и получения этими гражданами вида на жительство; на установление налоговых льгот и преференций для аккредитованных организаций, получающих доходы от распространения (размещения) рекламы или оказания дополнительных услуг с использованием приложений и онлайн-сервисов этих организаций либо доходы, связанные с реализацией, установкой, тестированием и сопровождением отечественных решений в области информационных технологий; на освобождение аккредитованных организаций от налогового контроля, валютного контроля и других видов государственного контроля (надзора) и муниципального контроля на срок до трёх лет; на обеспечение консолидации и стимулирования закупок критически важных отечественных разработок в области информационных технологий, проводимых для обеспечения государственных и муниципальных нужд или проводимых отдельными видами юридических лиц, а также на упрощение порядка проведения таких закупок»[1].

Данный указ может восприниматься как важнейший шаг, предпринятый за последние десятилетия и направленный на оздоровление кадрового и технического потенциала, а также экономического подъёма российской IT-сферы. Положения указа являются важным стимулом для совершенствования программного обеспечения отечественного производства, увеличения финансирования данной сферы и наращивания отечественного IT-потенциала. А поскольку ИТ-сфера прямо или косвенно воздействует и на все прочие сферы российского общества, в том числе и на сферу информационной безопасности, в обозримом будущем следует ожидать её беспрецедентного подъёма в качестве закономерного результата предпринимаемых мер и их практической реализации.

[1] Указ Президента Российской Федерации от 02.03.2022 № 83 «О мерах по обеспечению ускоренного развития отрасли информационных технологий в Российской Федерации» // Президент России: [сайт]. URL: http://www.kremlin.ru/acts/bank/47593 (дата обращения: 27.03.2022).

Информационный терроризм как угроза информационной безопасности РФ

Активное использование в современном мире межгосударственных связей и новых технологий позитивно влияет на результаты работы правоохранительных органов в сфере раскрытия компьютерных преступлений. Этому способствует возможность оперативно связываться со спецслужбами иностранных государств с целью отслеживания каналов передачи информации, что повышает шансы на обнаружение преступников. Однако, вследствие возможности быстрого перемещения между государствами, неполного покрытия территорий системами фиксации (к примеру, видеонаблюдения), отсутствия отлаженной системы правовых норм в области информационных технологий и прочих затруднений с поимкой преступников, неуклонно растёт число киберпреступлений, связанных с нарушениями личных и экономических прав граждан РФ [3, с. 125–126]. На уровень киберпреступности также негативно влияет возможность действовать анонимно или под псевдонимом (никнеймом).

Как следствие, возможности новой информационно-цифровой эпохи расширяются не только у конструктивных, но и у разного рода террористических и экстремистских организаций. Последние активно используют механизмы информационного воздействия на индивидуальное, групповое и общественное сознание. В результате нарастает межнациональная и социальная напряжённость, происходит эскалация конфликтов по разным основаниям, разжигаются этническая и религиозная ненависть и вражда. Опасность информационного терроризма зачастую недооценивается, в результате чего, граждане порой и сами не осознают, что становятся его жертвами.

Информационный терроризм предполагает особое психологическое воздействие на сознание человека с помощью ресурсов информационной сети, которое направлено на внушение требуемых идей, пода-

вляющих собственное мнение, аналитическую способность и логическое мышление индивида [2, с. 113–114]. Основной целью информационных террористов является донесение заведомо ложной информации, которая впоследствии будет восприниматься потерпевшими как абсолютно достоверная. Главная опасность здесь кроется в том, что эта, как правило, негативная информация может повлечь за собой необратимые последствия, например, пошатнуть целостность государства, привести к смене правительства и пр. Особенно эффективным инструментом террористической пропаганды является обыгрывание социально-политических проблем общества с разжиганием межэтнической и национальной розни.

В настоящее время можно выделить несколько разновидностей информационного терроризма.

1. *Информационно-психологический терроризм*. Связан непосредственно с самой информацией и её распространением, т. е. основное давление здесь оказывается на психику человека. Например, для того, чтобы запустить негативный слух в СМИ или интернете, используются методы насилия или подкупа, целью которых являются операторы, разработчики или представители телекоммуникационных систем.

2. *Информационно-технический терроризм*. Данный вид связан с нанесением ущерба непосредственно самой технике или с её помощью. Например, создание различных вирусов или помех с помощью других программ с целью разрушения систем управления или перехват управления техническими объектами.

3. *Кибертерроризм*. Направлен на выведение из строя компьютерных систем и их взлома, нападения на компьютерные сети.

4. *Кибертеррористический акт*, который проводится с помощью различных компьютерных технологий и является при этом политически мотивированным. Как правило, целью всего этого является максимальное привлечение внимания к политическим требованиям, выдвигаемым террористами.

Последние два вида информационного терроризма являются продуктом недавнего времени и ведут свою историю с начала 90-х гг. XX века. Их появление было напрямую связано с ростом потребностей в сфере информационных технологий и с развитием самой глобальной сети. В настоящее время именно кибертерроризм считается самым опасным и масштабным видом информационных атак, т. к. как его крайне сложно обнаружить и предотвратить. Действия, совершаемые террористом, производятся удалённо через киберпространство. Они могут исходить даже с территории другого государства, что ещё больше усложняет ситуацию с выявлением киберпреступника [4, с. 98].

Таким образом, на сегодняшний день информационный терроризм становится угрозой не только для России, но и для всего цивилизованного мира. С каждым разом его всё сложнее предотвратить, т. к. технологии, используемые террористами, всё больше совершенствуются. Весомой проблемой является также и то, что террористические организации пользуются не только высококлассным информационным оборудованием, но и методикой ведения «сетевых войн». Последняя имеет целью подрыв целостности в обществе, его дестабилизацию путём распространения в информационной сети ложных сведений, которые оказывают морально-психологическое давление на граждан.

Ещё одним опасным последствием доступа террористических организаций к новым информационным технологиям является пропаганда экстремистской идеологии и вербовка в террористические группировки новых сторонников. В основном такими «новобранцами» становятся молодые, эмоционально нестабильные люди с подвижной психикой и неустановившейся системой ценностей. Вербовка молодёжи в экстремистские и террористические организации – одно из самых опасных последствий реализации угрозы информационной безопасности государства, поскольку, в свою очередь, создаёт угрозу всей системе национальной безопасности.

Заключение

Безусловно, глобализация имеет как положительное (например, увеличение доступного объёма информации о технологиях и стимулирование разработки российского программного обеспечения), так и отрицательное (например, рост киберпреступлений и зависимость от зарубежных программных продуктов) влияние на информационную безопасность Российской Федерации. Причём важно отметить, что в ходе проведённого анализа было выявлено больше недостатков, чем преимуществ.

В условиях глобализации и сопутствующего ей роста числа информационных угроз пропорционально увеличивается нагрузка на службы информационной безопасности РФ. В условиях кадрового дефицита в сфере информационных технологий реализация этой угрозы приводит к банкротству коммерческих организаций, утечкам из баз данных различных служб.

Введённый странами Запада режим жёсткого санкционного давления актуализирует потребность разработки собственного программного обеспечения, что необходимо не только для бесперебойного функционирования различных систем в случае невозвращения в Россию западных экспортеров программного обеспечения, но и для сохранения экономического и информационного суверенитета РФ.

Ввиду активизации деятельности экстремистских структур необходимо создание инструментов защиты пользователей от пропаганды терроризма и вовлечения в подобные организации. Насущной также является проблема ограниченных возможностей сетевых узлов для обработки данных и их перемещения по каналам в мировом информационном пространстве, т. к. даже кратковременный сбой в работе программ может привести как к нарушению жизненного ритма человека и компании, так и к потере данных важнейших в государственных структурах.

Самой же масштабной и значительной угрозой информационной безопасности Российской Федерации является потенциальная возможность наступления глобальных инфогенных катастроф, источниками которых могут стать сбои и нарушения в программных продуктах различных государств при осуществлении международных проектов.

Статья поступила в редакцию 31.03.2022.

ЛИТЕРАТУРА

1. Гурьянов Н. Ю., Гурьянова А. В. Цифровая глобализация в контексте развития цифровой экономики и цифровых технологий // Вестник Московского государственного областного университета. Серия: Философские науки. 2020. № 3. С. 63–69.
2. Гурьянов Н. Ю., Коротаева Т. В. Девиации когнитивных способностей человека под воздействием информационных технологий // Вестник Московского государственного областного университета. Серия: Философские науки. 2021. № 1. С. 111–118.
3. Гурьянова А. В., Тимофеев А. В. Социально-правовое регулирование Интернет-среды: проблемы, реалии, перспективы // Вестник Московского государственного областного университета. Серия: Философские науки. 2021. № 4. С. 125–133.
4. Тимофеев А. В., Комолов А. А. Киберпреступность как социальная угроза и объект правового регулирования // Вестник Московского государственного областного университета. Серия: Философские науки. 2021. № 1. С. 95–101.
5. Guryanova A. V., Petinova M. A., Guryanov N. Yu. Socio-economic Problems and Perspectives of Globalization in the Context of Coronavirus Pandemic // Economic Systems in the New Era: Stable Systems in an Unstable World. IES 2020. Lecture Notes in Networks and Systems. Vol. 160. Cham: Springer, 2021. P. 567–573.
6. Guryanova A. V., Stotskaya T. G., Khafiyatullina E. R. Information Security as a Condition for Sustainable Development in the Global World // Digital Technologies in the New Socio-Economic Reality. ISCDTE 2021. Lecture Notes in Networks and Systems. Vol. 304. Cham: Springer, 2022. P. 43–50.

REFERENCES

1. Gur'yanov N. Yu., Gur'yanova A. V. [Digital Globalization in the Context of Digital Economy and Digital Technologies Development]. In: *Vestnik Moskovskogo gosudarstvennogo oblastnogo universiteta. Seriya: Filosofskie nauki* [Bulletin of Moscow Region State University. Series: Philosophy], 2020, no. 3, pp. 63–69.
2. Gur'yanov N. Yu., Korotaeva T. V. [Deviations of Human Cognitive Abilities under the Influence of Information Technologies]. In: *Vestnik Moskovskogo gosudarstvennogo oblastnogo universiteta. Seriya: Filosofskie nauki* [Bulletin of Moscow Region State University. Series: Philosophy], 2021, no. 1, pp. 111–118.
3. Gur'yanova A. V., Timofeev A. V. [Socio-Legal Regulation of the Internet Environment: Problems, Realities, Prospects]. In: *Vestnik Moskovskogo gosudarstvennogo oblastnogo universiteta. Seriya: Filosofskie nauki* [Bulletin of Moscow Region State University. Series: Philosophy], 2021, no. 4, pp. 125–133.
4. Timofeev A. V., Komolov A. A. [Cybercrime as a Social Threat and an Object of Legal Regulation]. In: *Vestnik Moskovskogo gosudarstvennogo oblastnogo universiteta. Seriya: Filosofskie nauki* [Bulletin of Moscow Region State University. Series: Philosophy], 2021, no. 1, pp. 95–101.
5. Guryanova A. V., Petinova M. A., Guryanov N. Yu. Socio-economic Problems and Perspectives of Globalization in the Context of Coronavirus Pandemic. In: Economic Systems in the New Era: Stable Systems in an Unstable World. IES 2020. Lecture Notes in Networks and Systems. Vol. 160. Cham, Springer, 2021, pp. 567–573.
6. Guryanova A. V., Stotskaya T. G., Khafiyatullina E. R. Information Security as a Condition for Sustainable Development in the Global World. In: *Digital Technologies in the New Socio-Economic Reality. ISCDTE 2021. Lecture Notes in Networks and Systems. Vol. 304*. Cham, Springer, 2022, pp. 43–50.

ИНФОРМАЦИЯ ОБ АВТОРАХ

Гурьянов Николай Юрьевич – кандидат философских наук, доцент, доцент кафедры гуманитарных дисциплин Медицинского университета «Реавиз»;
e-mail: nik.guryanow@yandex.ru

Пальмов Сергей Вадимович – кандидат технических наук, доцент, доцент кафедры информационных систем и технологий Поволжского государственного университета телекоммуникаций и информатики;
e-mail: psvzo@yandex.ru

INFORMATION ABOUT THE AUTHORS

Nikolay Yu. Guryanov – Cand. Sci. (Philosophy), Assoc. Prof., Department of Humanities , Reaviz Medical University;
e-mail: nik.guryanow@yandex.ru

Sergey V. Palmov – Cand. Sci. (Technical Sciences), Assoc. Prof., Department of Information Systems and Technologies, Povolzhskiy State University of Telecommunications and Informatics;
e-mail: psvzo@yandex.ru

ПРАВИЛЬНАЯ ССЫЛКА НА СТАТЬЮ

Гурьянов Н. Ю., Пальмов С. В. Глобализация и её воздействие на информационную безопасность Российской Федерации // Вестник Московского государственного областного университета. Серия: Философские науки. 2022. № 2. С. 76–83.
DOI: 10.18384/2310-7227-2022-2-76-83

FOR CITATION

Guryanov N. Yu., Palmov S. V. Globalization and Its Impact on the Information Security of the Russian Federation. In: *Bulletin of Moscow Region State University. Series: Philosophy*, 2022, no. 2, pp. 76–83.
DOI: 10.18384/2310-7227-2022-2-76-83