УДК 342.951:351.82

АКТУАЛЬНЫЕ НАПРАВЛЕНИЯ СОВЕРШЕНСТВОВАНИЯ АДМИНИСТРАТИВНОГО УПРАВЛЕНИЯ СИСТЕМОЙ ОБЕСПЕЧЕНИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ СУБЪЕКТА РОССИЙСКОЙ ФЕДЕРАЦИИ: ПРОБЛЕМЫ И ПРЕДЛОЖЕНИЯ

Коды JEL: O31, O32, O38

Шахворостов Г. И., *кандидат технических наук, доцент, заведующий кафедрой государственного и муниципального управления, Российская академия народного хозяйства и государственной службы при Президенте РФ (филиал РАНХиГС), г. Воронеж, Россия*
E-mail: shakhvorostov@mail.ru
SPIN-код: 3352-6307

Кустов А. И., *кандидат физико-математических наук, доцент, кафедра государственного и муниципального управления, Российская академия народного хозяйства и государственной службы при Президенте РФ (филиал РАНХиГС), г. Воронеж, Россия*
E-mail: aikustov@mail.ru
SPIN-код: 3253-3604

Самсонов В. С., *кандидат экономических наук, доцент, кафедра естественно-научных и социальных дисциплин, Российская академия народного хозяйства и государственной службы при Президенте Российской Федерации (филиал РАНХиГС), г. Воронеж, Россия*
E-mail: svs1311@mail.ru
SPIN-код: 1427-8466

Жданов М. А., *магистрант, Российская академия народного хозяйства и государственной службы при Президенте Российской Федерации (филиал РАНХиГС), г. Воронеж, Россия*
E-mail: mzhdanov@mail.ru
SPIN-код: отсутствует

Поступила в редакцию 28.12.2021. Принята к публикации 17.01.2022

Аннотация

Предмет. *Система обеспечения информационной безопасности субъекта Российской Федерации.*

Тема. *Актуальные направления совершенствования системы обеспечения информационной безопасности субъекта Российской Федерации.*

Цели. *Разработка предложений по совершенствованию системы обеспечения информационной безопасности субъекта Российской Федерации.*

Методология. *Метод теоретического анализа, анализа нормативных правовых документов по теме исследования, изучения материалов научных и периодических изданий по теме исследования и метод сравнения.*

Результаты. *В рамках анализа и оценки системы обеспечения информационной безопасности субъекта Российской Федерации выявлено, что в настоящее время основные проблемные вопросы субъекта Российской Федерации в сфере обеспечения информационной безопасности связаны с фиксируемой в последние годы объективной тенденцией усложнения информационных угроз и все большего их смещения с федерального на региональный уровень. В связи с чем органам исполнительной власти, необходимо совершенствовать систему обеспечения информационной безопасности, обеспечивающую своевременное (оперативное) и скоординированное реагирование на интенсивно возникающие многогранные информационные угрозы. В целях реализации комплексного подхода к построению единой системы обеспечения информационной безопасности субъекта Российской Федерации предлагается ее совершенствование по следующим направлениям: модернизация структуры Ситуационного центра главы региона; совершенствование нормативно-правовой базы субъекта Российской Федерации в области обеспечения информационной безопасности; формирование единой оперативно координируемой системы обеспечения информационной безопасности*

субъекта Российской Федерации; автоматизация процессов выявления и нейтрализации угроз информационной безопасности.

Область применения. *Система исполнительных органов государственной власти субъектов Российской Федерации.*

Выводы. *В статье рассматриваются основные проблемы исполнительных органов государственной власти по обеспечению информационной безопасности в субъекте Российской Федерации. Описываются методы и механизмы организации управления исполнительных органов государственной власти, направленных на совершенствование системы обеспечения информационной безопасности субъекта Российской Федерации. Предложены направления совершенствования системы обеспечения информационной безопасности субъекта Российской Федерации, в части организации оперативного реагирования на информационные угрозы. Проведённое исследование демонстрирует, что развитие системы обеспечения информационной безопасности субъекта Российской Федерации требует комплексного подхода. В современных условиях эффективность реагирования на информационные угрозы во многом зависит от оперативности и согласованности действий исполнительных органов государственной власти субъектов Российской Федерации.*

Ключевые слова: *информационная безопасность, исполнительные органы государственной власти, субъект Российской Федерации, информационные технологии, нормативные правовые акты, Ситуационный центр региона, Центр управления регионом.*

UDC 342.951:351.82

CURRENT DIRECTIONS OF IMPROVING THE ADMINISTRATIVE MANAGEMENT OF THE INFORMATION SECURITY SYSTEM OF A SUBJECT OF THE RUSSIAN FEDERATION: PROBLEMS AND PROPOSALS

JEL Codes: O31, O32, O38

Shakhvorostov G. I., *candidate of Technical Sciences, head of the department of state and municipal administration, Russian Presidential Academy of National Economy and Public Administration (branch of RANEPA), Voronezh, Russia*
E-mail: shakhvorostov@mail.ru
SPIN-code: 3352-6307

Kustov A. I., *Candidate of Physical and Mathematical Sciences, department of state and municipal administration, Russian Presidential Academy of National Economy and Public Administration (branch of RANEPA), Voronezh, Russia*
E-mail: kustov@mail.ru
SPIN-code: 3253-3604

Samsonov V. S., *Candidate of Economic Sciences, associate professor of the Department of Natural Sciences and Social Disciplines, Russian Academy of National Economy and Public Administration under the President of the Russian Federation (branch of RANEPA), Voronezh, Russia*
E-mail: svs1311@mail.ru
SPIN-code: 1427-8466

Zhdanov M. A., *graduate student, Russian Presidential Academy of National Economy and Public Administration (branch of RANEPA), Voronezh, Russia*
E-mail: mzhdanov@mail.ru
SPIN- code: none

Annotation.
Subject. *Information security system of a constituent entity of the Russian Federation.*
Topic. *Areas of development of the system of rapid response to threats to information security of the constituent entity of the Russian Federation.*
Purpose. *Development of proposals for improving the information security system of the constituent entity of the Russian Federation.*

Methodology. *The method of theoretical analysis, the analysis of regulatory documents on the topic of research, the study of materials of scientific and periodicals on the topic of research and the method of comparison.*

Results. *As part of the analysis and assessment of the information security system of the constituent entity of the Russian Federation, it was revealed that at present the main problematic issues of the constituent entity of the Russian Federation in the field of information security are related to the change in the direction of threats from the federal to the regional level. In this connection, the executive authorities need to improve the information security system, which ensures a timely (prompt) and coordinated response to intensively emerging multifaceted information threats. In order to implement an integrated approach to building a unified information security system for a constituent entity of the Russian Federation, it is proposed to improve it in the following areas: modernization of the structure of the Situation Center of the head of the region; improving the regulatory framework of the constituent entity of the Russian Federation in the field of information security; formation of a unified operational response system threats to information security of the constituent entity of the Russian Federation; automation of processes for identifying and neutralizing information security threats.*

Application area. *The system of executive bodies of state power of the constituent entities of the Russian Federation.*

Conclusions. *The article examines the problems of the executive bodies of state power on information security in the constituent entity of the Russian Federation. Methods and mechanisms of management of executive bodies of state power, improvement of the information security system of the Russian Federation are described. The directions of improving the information security system of the constituent entity of the Russian Federation, in terms of organizing an operational response to information threats, are proposed. The study demonstrates that the development of the information security system of the constituent entity of the Russian Federation requires an integrated approach. In modern conditions, the effectiveness of the response to information threats largely depends on the promptness and consistency of the actions of the executive bodies of state power of the constituent entities of the Russian Federation.*

Keywords: *information security, executive bodies of state power, a constituent entity of the Russian Federation, information technology, regulatory legal acts, the Situational center of the region, the Center for regional management.*

DOI: 10.22394/1997-4469-2022-56-1-28-35

Введение

В условиях происходящего в наши дни технологического рывка распространение информационно-коммуникационных технологий является одним из важных факторов формирования новой политической реальности как в России, так и в мире в целом. Отмечается стремительная трансформация традиционных норм поведения в политической сфере, прежние из которых во многом себя изжили. Причем российские эксперты в этой области говорят о так называемой информационной геополитике (или геополитики эпохи информатизации), которая в условиях становления информационного общества, или в соответствии с терминологией Национальных проектов — «цифровой трансформации», потребует обновления стратегии развития России и ее регионов [1]. В связи с чем, все большую актуальность приобретает необходимость надежного обеспечения информационной безопасности личности, общества и государства, представляющее собой осуществление взаимоувязанных мер по прогнозированию, обнаружению, сдерживанию, предотвращению, отражению информационных угроз и ликвидации последствий их проявления.

В целях обеспечения информационной безопасности субъекта Российской Федерации формируется система (обеспечения информационной безопасности), в которую входят: государственные органы, а также подразделения и должностные лица государственных органов, органов местного самоуправления и организаций, уполномоченные на решение в соответствии с законодательством Российской Федерации задач по обеспечению информационной безопасности.

Одновременно в политике, как мировой, так и внутрироссийской увеличивается состав участников, способных применять средства информационного противоборства для достижения своих целей. Субъектами таких процессов теперь являются не только государства, но и «акторы вне суверенитета», которые в своей деятельности также активно пользуются преимуществами цифрового измерения (в частности, социальными сетями).

К основным группам негосударственных участников информационного противоборства современности российский эксперт в области информационной безопасности А. А. Смирнов причисляет [2]: террористические и экстремист-

ские организации; хакерские и активистские группы; сообщества журналистов-расследователей и гражданских активистов; средства массовой информации и блогеров; коммерческие организации неправительственные организации; отдельных лиц.

Оценка проблем информационной безопасности субъекта РФ

В настоящее время анализируя состояние информационной обстановки вокруг Российской Федерации, позволяет сделать о расширении масштабов и интенсивности вовлечения данных субъектов в информационное противоборство, а также постоянном проведении западными странами информационных действий, направленных на подрыв суверенитета, политической и социальной стабильности, а также территориальной целостности России [3].

В настоящее время уровень таких усилий значительно возрос, во многих случаях приобрел новое качество, при этом наблюдается тенденция смещения активности противоборства на региональный уровень. Отсюда, в том числе и активизация на региональном уровне протестов, деятельности экстремистских организаций и хакерских групп, связанных со спецслужбами иностранных государств.

Особенно выделяется стремление заинтересованных субъектов информационного пространства нарастить протестный потенциал в субъектах Российской Федерации. Основным информационным поводом последнего времени является прививочная кампания по вакцинированию населения от коронавирусной инфекции «Covid-19». В социальных сетях и мессенджерах активно распространяется дезинформация о «мировом заговоре и стремлении власть имущих загнать людей в цифровой концлагерь, а также нарушении основополагающих норм демократии и предоставлении права выбора населению». Проводится активная агитация народных масс к вовлечению в «ярые антипрививочники» и необходимости участия в протестных акциях «в борьбе за свои права».

При этом современные реалии показывают, что быстрота реакции на ту или иную угрозу (информационный повод, воздействие, событие) приобретает особое значение при обеспечении информационной безопасности. В этой связи здесь действует «презумпция виновности», т. е. тот, кого обвиняют, вынужден оправдываться (доказывать свою невиновность), а значит утрачивает инициативу.

Этот простой механизм хорошо отлажен и активно используется США и их союзниками для продвижения своих геополитических интересов. В его основе лежат простые психологические особенности общественного сознания: хорошо запоминается и принимается в качестве основной именно первоначальная версия; если кто-то оправдывается, значит он виноват.

Данная тенденция, все более ужесточает требования ко времени принятия решений (естественно в сторону максимального его сокращения) на организацию мероприятий информационного воздействия и защиты, выделяя оперативное реагирование, как ключевую часть общей системы обеспечения информационной безопасности.

В широком смысле под оперативным реагированием на угрозы информационной безопасности, следует понимать непрерывное отслеживание изменений информационной обстановки, своевременное выявление информационных угроз и принятие в кратчайшие сроки необходимых и исчерпывающих комплексных мер, как «наступательного», так и «защитного» характера, по их ослаблению (нейтрализации).

Анализ подходов к обеспечению информационной безопасности субъекта Российской Федерации

В настоящее время на недостаточном уровне определены основные интересы Российской Федерации и ее субъектов в информационной сфере по предметам совместного ведения, а также интересы субъектов Федерации по предметам их исключительного ведения, наиболее опасные угрозы этим интересам, направления и механизмы участия органов федеральной системы обеспечения информационной безопасности, органов государственной власти субъектов Российской Федерации, государственных, общественных и иных организаций и граждан, проживающих на территории субъекта Российской Федерации, в реализации мероприятий по противодействию этим угрозам, а также порядок координации данной деятельности.

Основная сложность определения и разграничения интересов страны и регионов обусловлена неформальным характером задачи выделения среди множества жизненно важных целей развития регионов таких, достижение которых в существенной степени зависит от информационной сферы и защита которых составляет предмет региональной информационной безопасности.

Представляется, что оптимальное решение выделенных проблем может быть найдено лишь на основе концентрации усилий органов государственной власти субъектов Российской Федерации, государственных и общественных

организаций региона, действующих в информационной сфере, хозяйствующих субъектов, специалистов при методической поддержке органов федеральной системы обеспечения информационной безопасности.

Региональная политика федеральной власти в области обеспечения информационной безопасности, должна формироваться исходя из необходимости защиты жизненно важных интересов Российской Федерации в информационной сфере по предметам совместного ведения Федерации и субъектов Федерации, а также оказания субъектам Федерации необходимой помощи в защите их жизненно важных интересов в информационной сфере.

Внутренняя региональная политика субъектов Российской Федерации в области информационной безопасности должна быть направлена прежде всего на определение системы целей и задач по предметам их исключительного ведения, к которым в информационной сфере следует отнести:

1. Региональную информацию, включая региональные информационные ресурсы, информационную инфраструктуру, системы массового информирования граждан, системы связи;

2. Культурное развитие регионов.

Достижение этих целей и решение задач с учетом специфики и возможностей конкретных субъектов российской Федерации целесообразно положить в основу их региональных систем обеспечения информационной безопасности.

При этом, возросшие масштабы и многогранность угроз информационной безопасности требует выстраивания эффективной системы выявления, прогнозирования и реагирования на них с обязательным привлечением потенциала всех заинтересованных сил и средств региона под руководством единого координирующего органа.

В целях создания в регионах органа управления Главы исполнительной власти по реагированию на различные угрозы, в соответствии с Указом Президента Российской Федерации от 25 июля 2013 года № 648 «О формировании системы распределенных центров, работающих по единому регламенту взаимодействия» в интересах оперативного управления регионом в субъектах Российской Федерации созданы Ситуационные центры.

В общем виде основными целями Ситуационного центра являются информационно-аналитическое обеспечение государственного управления и стратегического планирования, а также повышение эффективности государственного управления в мирное и военное время, в том числе при возникновении чрезвычайных (кризисных) ситуаций.

Основными задачами Ситуационного центра являются: мониторинг и анализ складывающейся ситуации, а также прогнозирование ее изменения, управление информационными потоками и визуализацией, а также информационное взаимодействие с ситуационными центрами, входящими в систему распределенных ситуационных центров.

Таким образом, ситуационный центр является инструментом Главы субъекта Российской Федерации по оперативному реагированию на изменения обстановки в мирное время и стабилизации обстановки при кризисных (чрезвычайных) ситуациях. И хотя уровень его взаимодействия со сторонними структурами по вопросам обеспечения информационной безопасности в настоящее время находится еще на недостаточно высоком уровне, возложение задач координации обеспечения информационной безопасности в субъекте именно на ситуационные центры является наиболее целесообразным.

Предложения по совершенствованию административного управления системой обеспечения информационной безопасности субъекта РФ

В целях реализации комплексного подхода к построению единой и эффективной системы обеспечения информационной безопасности целесообразно ее совершенствование осуществлять на основе Ситуационного центра по следующим направлениям:

1. Модернизация структуры Ситуационного центра.

2. Совершенствование нормативно-правовой базы субъекта Российской Федерации в области обеспечения информационной безопасности.

3. Формирование единой системы оперативного реагирования на угрозы информационной безопасности субъекта Российской Федерации.

4. Автоматизация процессов выявления и нейтрализации угроз информационной безопасности.

Необходимость модернизации структуры Ситуационного центра обосновывается отсутствием подразделений, в задачах которых предусмотрено проведение следующих мероприятий: мониторинга информационной обстановки и координация деятельности субъектов системы обеспечения информационной безопасности по оперативному реагированию на информационные угрозы; анализ и оценка эффективности выполненных мероприятий.

Для исправления данного положения предлагается в составе Ситуационного центра сформировать подразделение оперативного реагиро-

вания на угрозы информационной безопасности со следующими функциями, осуществляемыми в круглосуточном режиме:

— мониторинг, выявление и оценку угроз информационной безопасности;

— организация взаимодействия с субъектами системы обеспечения информационной безопасности региона, а также Российской Федерации в целом (по необходимости) по выявлению угроз и уточнения необходимых данных;

— подготовка информационно-справочных документов по выявленным информационным угрозам;

— организация оперативного реагирования на угрозы информационной безопасности субъекта Российской Федерации;

— контроль и оценка результатов проводимых мероприятий по нейтрализации (снижению) выявленных информационных угроз;

— подготовка предложений по совершенствованию системы оперативного реагирования на угрозы информационной безопасности субъекта Российской Федерации.

Кроме того, в целях выявления тенденций изменения информационной обстановки, направленности информационных угроз и выработки подходов к повышению эффективности мероприятий и мер реагирования в подразделении, необходимо сформировать структуру, осуществляющую:

— анализ, обобщение и осуществление экспертной оценки данных, характеризующих состояние информационной обстановки вокруг субъекта Российской Федерации и информационной политики, проводимой руководством региона;

— определение тенденций формирования угроз информационной безопасности субъекта Российской Федерации;

— прогнозирование развития существующих и появлении новых способов и средств информационного воздействия;

— представление руководству субъекта Российской Федерации информационно-аналитических материалов по информационной обстановке вокруг региона.

Введение подобного подразделения в состав Ситуационного центра позволит осуществлять оперативные, скоординированные по целям, задачам, месту и времени меры (наступательные и защитные) по нейтрализации (ослаблению) информационных угроз дежурными силами и средствами системы обеспечения информационной безопасности региона, в том числе с задействованием потенциала федеральных органов исполнительной власти.

Непосредственно состав, структура и функционал предлагаемого подразделения должны определяться исходя из специфики региона, в том числе масштабности и интенсивности внешних и внутренних угроз информационной безопасности.

В целях совершенствования нормативных правовых документов, учитывая необходимость внесения изменений в структуру центра управления регионом, актуальным становится вопрос о регламентации их деятельности, для чего необходимо уточнить Положение о Ситуационном центре. В котором будет детально описан функционал предлагаемого подразделения.

Исходя из предлагаемых выше изменений, в целях формирования единой системы оперативного реагирования на угрозы информационной безопасности субъекта Российской Федерации предлагается:

— функции координирующего органа возложить на Ситуационный центр Главы субъекта Российской Федерации в целях обеспечения единого руководства действиями элементов системы в информационно-телекоммуникационном пространстве;

— нарастить взаимодействие Ситуационного центра с элементами системы обеспечения информационной безопасности региона и Российской Федерации в целом;

— взаимоувязать деятельность элементов системы оперативного реагирования на угрозы информационной безопасности субъекта Российской Федерации с элементами обеспечения информационной безопасности межрегионального и федерального уровнями Российской Федерации.

Таким образом в целях формирования единой системы оперативного реагирования на угрозы информационной безопасности субъекта Российской Федерации предлагается взаимодействие по схеме, представленной на рисунке.

На схеме представлены федеральный, межрегиональный и региональный уровни. Субъект представлен региональным уровнем и является основной единицей информационного взаимодействия системы. Связующим и координирующим элементом субъекта является Ситуационный центр, информационный обмен которого осуществляется как по вертикали, так и по горизонтали.

Анализ существующих документов, регламентирующих взаимодействие ситуационных центров субъектов Российской Федерации показал, что не требуется формирование новых. [4, 5, 6, 7] Необходимо дополнить существующий Регламент функционирования и информационного обмена Ситуационного центра в части обмена информацией в сфере выявления и оперативной нейтрализации (снижения воздействия) угроз информационной безопасности субъекта российской Федерации.

Рис. Предлагаемая схема взаимодействия Ситуационного центра по вопросам оперативного реагирования на угрозы информационной безопасности

Для повышения эффективности функционирования Ситуационного центра в его работе необходимо использовать комплексы средств автоматизации, основанных на современных информационных технологиях.

В первую очередь информационные системы, направленные на сбор и анализ эмоциональной окраски во всем информационном пространстве (СМИ и социальные сети, теле- и радиовещания), а также систематизацию и иерархическое хранение данных, полученных из других органов.

Заключение

В условиях стремительно меняющейся информационной обстановки, применения заинтересантами все новых форм и методов информационно-психологического и информационно-технического воздействия, для обеспечения национальной безопасности Российской Федерации и ее регионов крайне важно перманентное совершенствование системы обеспечения информационной безопасности государства, способной оперативно и эффективно реагировать на возникающие вызовы и угрозы в информационной сфере. Основой эффективного применения сил и средств обеспечения информационной безопасности является координация их деятельности под единым управляющим органом. А также обеспечение данных сил автоматизированными средствами на основе современных информационных технологиях.

В статье рассмотрены предложения, повышающие эффективность оперативного реагирования на угрозы информационной безопасности, тем самым совершенствующие подходы к своевременной нейтрализации информационных угроз и функционирование системы обеспечения информационной безопасности субъекта Российской Федерации и государства в целом.

Информация о конфликте интересов

Мы, авторы данной статьи, со всей ответственностью заявляем о частичном и полном отсутствии фактического или потенциального конфликта интересов с какой бы то ни было третьей стороной, который может возникнуть вследствие публикации данной статьи.

СПИСОК ЛИТЕРАТУРЫ

1. *Модестов С. А.* Информационное противоборство как фактор геополитической конкуренции / С. А. Модестов. — Москва : Московский общественный научный фонд: Издательский центр научных и учебных программ, 1999. — 64 с.

2. *Смирнов А. А.* Негосударственные акторы в современных информационных войнах / А. А. Смирнов // Международная жизнь. — 2018. — № 5. — URL: https://interaffairs.ru/jauthor/material/2020. (дата обращения: 15.10.2021).

3. Российская Федерация. Президент РФ (2012—2018; В. В. Путин). Доктрина информационной безопасности Российской Федерации: Указ Президента РФ от 05.12.2016 г. № 646 // Информационно-правовое обеспечение Гарант [Электронный ресурс]. — Режим доступа:

http://base.garant.ru/71556224/ (дата обращения: 15.10.2021).

4. Российская Федерация. Президент РФ (2012—2018; В. В. Путин). Поручение Президента РФ Пр-354, от 01.03.2020 г. // Информационно-правовое обеспечение Гарант [Электронный ресурс]. — Режим доступа: http://base.garant.ru/72556611/ (дата обращения: 01.02.2021)

5. Российская Федерация. Президент РФ (2012—2018; В. В. Путин). О формировании системы распределительных ситуационных центров, работающих по единому регламенту взаимодействия : Указ Президента РФ от 25 июля 2013 г. № 648 // Информационно-правовое обеспечение Гарант [Электронный ресурс]. — Режим доступа: http://base.garant.ru/71556337/ (дата обращения: 11.07.2021).

6. Российская Федерация. Президент РФ (2012—2018; В. В. Путин). Вопросы взаимодействия и координации деятельности органов исполнительной власти субъектов Российской Федерации и территориальных органов федеральных органов исполнительной власти : Указ Президента РФ от 2 июля 2013 г. № 773 // Информационно-правовое обеспечение Гарант [Электронный ресурс]. — Режим доступа: http://base.garant.ru/7258834/ (дата обращения: 13.02.2021).

7. О взаимодействии и координации деятельности органов исполнительной власти субъектов Российской Федерации и территориальных органов федеральных органов исполнительной власти : Постановление Правительства РФ от 5 декабря 2005 г. № 725 // Информационно-правовое обеспечение Гарант [Электронный ресурс]. — Режим доступа: http://base.garant.ru/71663136/ (дата обращения: 12.06.2021).

LIST OF LITERATURE

1. *Modestov S. A.* Information confrontation as a factor of geopolitical competition / S. A. Modestov. — Moscow : Moscow Public Science Foundation: Publishing Center for Scientific and Educational Programs, 1999. — 64 s.

2. *Smirnov A. A.* Non-state actors in modern information wars / A. A. Smirnov // International life. — 2018. — No. 5. — URL: https://interaffairs.ru/jauthor/material/2020. (date of access: 15.10.2021).

3. Russian Federation. President of the Russian Federation (2012—2018; V. V. Putin). Doctrine of information security of the Russian Federation : Decree of the President of the Russian Federation of 05.12.2016 N 646 // Information and legal support of the Guarantor [Electronic resource]. — URL: -http: //base.garant.ru/71556224/ (date accessed: 15.10.2021).

4. Russian Federation. President of the Russian Federation (2012—2018; V. V. Putin). Instruction of the President of the Russian Federation Pr-354, dated 01.03.2020 // Information and legal support of the Guarantor [Electronic resource]. — URL: -http: //base.garant.ru/72556611/ (date of access: 01.02.2021).

5. Russian Federation. President of the Russian Federation (2012—2018; V. V. Putin). On the formation of a system of distribution situational centers operating according to a single interaction regulation : Decree of the President of the Russian Federation of July 25, 2013 No. 648 // Information and legal support of the Guarantor [Electronic resource]. — URL: -http: //base.garant.ru/71556337/ (date accessed: 07.11.2021).

6. Russian Federation. President of the Russian Federation (2012—2018; V. V. Putin). Issues of interaction and coordination of the activities of executive bodies of the constituent entities of the Russian Federation and territorial bodies of federal executive bodies : Decree of the President of the Russian Federation of July 2, 2013 No. 773 // Information and legal support of the Guarantor [Electronic resource]. — URL: -http: //base.garant.ru/7258834/ (date of access: 13.02.2021).

7. On interaction and coordination of the activities of executive bodies of the constituent entities of the Russian Federation and territorial bodies of federal executive bodies : Decree of the Government of the Russian Federation of December 5, 2005 No. 725 // Information and legal support of the Garant [Electronic resource]. — URL: -http: //base.garant.ru/71663136/ (date accessed: 12.06.2021).