УДК 342.951:351.82

Михнев И.П., Михнева С.В., Махова А.А., Лапшина А.Р.
Волгоградский институт управления (филиал) ФГБОУ ВО «Российская академия народного хозяйства и государственной службы при Президенте РФ», Волгоград,
e-mail: mkmco@list.ru, svet-mihneva@list.ru,
maxovaalexa@mail.ru, nastya.lapshina.999@mail.ru

ПОЛНОМОЧИЯ ФЕДЕРАЛЬНЫХ ОРГАНОВ ГОСУДАРСТВЕННОЙ ВЛАСТИ РОССИЙСКОЙ ФЕДЕРАЦИИ В ОБЛАСТИ ОБЕСПЕЧЕНИЯ БЕЗОПАСНОСТИ КРИТИЧЕСКОЙ ИНФОРМАЦИОННОЙ ИНФРАСТРУКТУРЫ

Ключевые слова: орган государственной власти, федеральный орган, полномочия, критическая информационная инфраструктура, информационная безопасность, компьютерные атаки, компьютерные инциденты.

В работе рассматриваются полномочия и компетенция органов государственной власти Российской Федерации в рамках их правового статуса в сфере обеспечения безопасности критической информационной инфраструктуры. Четкость и однозначность закрепления прав и обязанностей государственных органов, уполномоченных в сфере информационной безопасности, являются гарантиями эффективного обеспечения безопасности значимых объектов информационной инфраструктуры. Федеральный закон № 187-ФЗ впервые закрепил понятие и объекты критической информационной инфраструктуры, а также определил федеральные органы государственной власти, уполномоченные в этой сфере. Важную роль законодатель отводит Федеральной службе безопасности России, отвечающей за эффективность государственной системы обнаружения, предупреждения и ликвидации последствий компьютерных атак, и Федеральной службе технического и экспортного контроля России, обеспечивающей безопасность объектов критической информационной инфраструктуры. Учитывая схожесть функций данных федеральных органов государственной власти, компетенция их нуждается в тщательном анализе. В ряде федеральных органов исполнительной власти изменились некоторые функции и полномочия в сфере информационной безопасности. В частности, Федеральная Служба Безопасности на основании Указа Президента РФ уполномочена на создание государственной системы обнаружения, предупреждения и ликвидации последствий компьютерных атак на информационные ресурсы РФ. Однако, не все права и обязанности являются закрепленными, ряд полномочий вызывает двойственность правового положения некоторых федеральных органов государственной власти.

Mikhnev I.P., Mikhneva S.V., Makhova A.A., Lapshina A.R.
Volgograd Institute of Management – branch of the Russian Presidential Academy of National Economy and Public Administration, Volgograd,
e-mail: mkmco@list.ru, svet-mihneva@list.ru,
maxovaalexa@mail.ru, nastya.lapshina.999@mail.ru

THE POWERS OF THE FEDERAL AUTHORITIES OF THE RUSSIAN FEDERATION IN THE FIELD OF ENSURING THE SECURITY OF CRITICAL INFORMATION INFRASTRUCTURE

Keywords: authority state authority, federal authority, credentials, critical information infrastructure, information security, computer attacks, computer incidents.

The paper considers the competence and powers of the state authorities of the Russian Federation within the framework of their legal status in the field of ensuring the security of critical information infrastructure. The clarity and unambiguity of securing the rights and obligations of state bodies authorized in the field of information security are guarantees to effectively ensure the security of important information infrastructure facilities. For the first time, Federal Law No. 187-FZ fixed the concept and objects of critical information infrastructure, and also determined the federal government authorities authorized in this sphere. The legislator assigns an important role to the Federal Security Service of Russia, which is responsible for the effectiveness of the state system for detecting, preventing and eliminating the effects of computer attacks, and the Federal Technical and Export Control Service of Russia, ensuring the safety of critical information infrastructure facilities. Given the similarity of the functions of these federal authorities of state power, their competence requires careful analysis. Some functions and authorities in the field of information security have changed in a number of federal executive authorities. In particular, the Federal Security Service, on the basis of a presidential decree, is authorized to create a state system for detecting, preventing and eliminating the consequences of computer attacks on information resources of the Russian Federation. However, not all rights and obligations are enshrined, a number of powers cause the duality of the legal status of certain federal authority of state power.

Введение

Правовое регулирование деятельности субъектов информационных отношений сегодня направлено не только на защиту прав и законных интересов индивидуальных участников права, но, прежде всего, на обеспечение национальной безопасности в сфере информационных систем и технологий [1].

Тема критической информационной инфраструктуры достаточно актуальна на протяжении последних 10 лет. Международная арена межгосударственных отношений на сегодняшний момент характеризуется напряженностью и конфликтностью, усугубляемой информационной войной и столкновением интересов в сфере информационных систем и коммуникаций, сопровождающимся частыми компьютерными атаками и инцидентами. Таким образом, необходимость разработки новейших методов и способов защиты информации, комплекса мероприятий по обеспечению информационной безопасности диктуется требованиями современного информатизированного пространства. Недостаточно налаженная система информационной безопасности и низкая степень защиты информационной инфраструктуры (информационных систем, информационно-телекоммуникационных сетей, автоматизированных систем управления) могут повлечь за собой необратимые последствия для всего государства, события с хакерскими атаками в Иране 2010 года и в Западной Корее 2013 года яркое тому подтверждение [2].

Информационная безопасность стала важной сферой жизнедеятельности государства, поэтому ее обеспечение и защита информации сегодня признаются приоритетным направлением концепции национальной безопасности. Актуальность на общегосударственном уровне и своевременность защиты национальной информационной инфраструктуры России с учетом появления международных санкционных мер со стороны других стран в целом ускорили процесс принятия на федеральном уровне закона о ее безопасности, особенно в сфере здравоохранения, науки, транспорта, финансового сектора, в ракетно-космической промышленности, атомной энергетике и в других. Законодатель впервые четко определил понятие термина – критическая информационная инфраструктура, выделил ее субъекты, значимые объекты и способы их защиты [3].

Основными субъектами, осуществляющими деятельность по обеспечению информационной безопасности, являются федеральные органы государственной власти, которые обладают специальными полномочиями в рамках закрепленного правового положения, и выполняемыми в соответствии с ним функциями. Важное место в системе федеральных органов государственной власти, обладающих полномочиями в области обеспечения безопасности критической информационной инфраструктуры, занимают Президент РФ, Правительство РФ, Федеральная служба безопасности России, Федеральная служба по техническому и экспортному контролю. С принятием и вступлением в силу с 1 января 2018 года Федерального закона № 187-ФЗ от 26.07.2017 «О безопасности критической информационной инфраструктуры Российской Федерации» пополнился ряд полномочий данных федеральных государственных органов. В частности, для ФСБ России нововведением является создание и функционирование государственной системы обнаружения, предотвращения и ликвидации компьютерных атак и образование Национального координационного центра по компьютерным инцидентам, цель которого заключается в координировании мероприятий по реагированию на компьютерные инциденты и непосредственное участие в таких мероприятиях, организация и осуществление обмена информацией о компьютерных инцидентах между субъектами информационной безопасности, а также между субъектами и уполномоченными органами иностранных государств, международными организациями [4].

Сегодня в современных условиях можно подвести первые итоги состояния обеспеченности информационной безопасности в России, состояния защиты информации. Несмотря на принятый на федеральном уровне и вступивший в законную силу с 1 января 2018 года новый закон, предусматривающий безопасность критической информационной инфраструктуры, сегодня уже можно

обозначить достоинства введенных инноваций, а также выявить проблемные стороны правового регулирования, его пробелы и недостающие обоснования новых элементов. Таким образом, элементы информационного права, активно развиваясь, требуют соответствующего юридического сопровождения. А потому нуждаются, прежде всего, в научном осмыслении для правильности определения ряда понятий, выявления участвующих субъектов и определения их правового положения [5].

Полномочия федеральных органов исполнительной власти РФ в сфере обеспечения безопасности критической информационной инфраструктуры являются необходимым элементом их деятельности. От четкости их установления в соответствии с выполняемыми функциями зависит и степень обеспеченности защиты значимых объектов критической информационной инфраструктуры. Поэтому важность анализа закрепления и определения полномочий федеральных органов обусловлена выявлением степени правовой урегулированности сферы информационной безопасности и ее соответствия реальным потребностям и возможностям субъектов критической информационной инфраструктуры [6].

Цель исследования – опираясь на нормы и положения действующего законодательства, проанализировать полномочия федеральных органов государственной власти в сфере обеспечения безопасности критической информационной инфраструктуры.

Материал и методы исследования

Нормативно-правовую базу исследования составляют следующие нормативно-правовые акты: Конституция Российской Федерации 1993 года, Федеральный закон № 187-ФЗ от 26.07.2017 «О безопасности критической информационной инфраструктуры Российской Федерации», вступивший в силу с 1 января 2018 г, «Концепция государственной системы обнаружения, предупреждения и ликвидации последствий компьютерных атак на информационные ресурсы РФ» (утв. Президентом РФ 12.12.2014 № К 1274), Постановление Правительства РФ № 127 от 08.02.2018 г. «Об утверждении Правил категорирования объектов критической информационной инфраструктуры, а также перечня показателей критериев значимости объектов критической информационной инфраструктуры и их значений», Приказ ФСБ России № 366 от 24.07.2018 «О НКЦКИ», Приказ ФСБ России № 367 от 24.07.2018 «Об утверждении Перечня информации, представляемой в Государственную систему обнаружения, предупреждения и ликвидации последствий компьютерных атак на информационные ресурсы РФ и Порядка представления информации в государственную систему обнаружения, предупреждения и ликвидации последствий компьютерных атак на информационные ресурсы РФ», Приказ ФСБ России № 368 от 24.07.2018 «Об утверждении Порядка обмена информацией о компьютерных инцидентах и Порядка получения субъектами критической информационной инфраструктуры информации о средствах и способах проведения компьютерных атак и о методах их предупреждения и обнаружения» [7].

Методы исследования составили следующие: общенаучный метод диалектики научного познания, а также основанные на нем частно-научные методы, такие как сравнительно-правовой, структурно-функциональный, формально-юридический. При этом применялись анализ, синтез, индукция и дедукция для исследования [8].

Рассматриваемые вопросы находятся на стыке различных отраслей права. С одной стороны, такие юридические отраслевые науки как: конституционное и административное право, закрепляющие общие положения и статус государственных органов, а также информационное право, регулирующее деятельность участников информационных отношений [9].

Результаты исследования и их обсуждение

Правовое положение органов государственной власти представляет собой определенное место данных государственных субъектов в системе государственного и муниципального управления, выраженное совокупностью прав и обязанностей, или полномочий данных органов по осуществлению функций и решению основных задач госу-

дарства. Анализ полномочий федеральных органов предполагает обращение ко всей системе власти и управления Российской Федерации [10].

Государственное и муниципальное управление России представляет собой трехуровневое распределение государственных органов и органов местного самоуправления. Государственная власть РФ распространяется на федеральный уровень и на уровень субъектов федерации. Исходя из принципа разделения властей выделяются законодательные (представительные), исполнительные и судебные органы государственной власти как на федеральном, так и на региональном уровне. Органы местного самоуправления согласно статье 12 Конституции РФ не входят в систему органов государственной власти. Учитывая важность сферы безопасности критической информационной инфраструктуры, основные функции по обеспечению ее безопасности отводятся федеральной власти, прежде всего, Президенту РФ, Правительству РФ, ФСБ России и ФСТЭК России. В целях оптимального распределения и определения функций, полномочий, прав и обязанностей данных органов, исключения их дублирования законодатель закрепляет понятие критической информационной инфраструктуры, хотя правоприменительное использование этой категории на практике отмечалось и ранее [11].

В законодательной сфере критическая информационная инфраструктура (далее КИИ) – относительно новый термин, требующий некоторого пояснения. Согласно закону, под ней подразумеваются информационные системы, информационно-телекоммуникационные сети, автоматизированные системы управления, сети электросвязи, используемые для организации их взаимодействия. Ключевым условием отнесения системы к КИИ является ее использование государственным органом или учреждением в 12 обозначенных сферах, в частности: здравоохранения, науки, транспорта, финансовом секторе, ракетно-космической промышленности и других [12].

Обращаясь к категориальному аппарату, следует обозначить понятие полномочий органа государственной власти, поскольку в юридической науке выработаны различные подходы к смысловому значению и определению полномочий, выявлению соотношения этого понятия с компетенцией, функциями и задачами органа власти. Несмотря на широкий спектр определений данного термина, в целом полномочия можно определить как определенные законом возможности правового действия органа власти, его права, обязанности, а также задачи и функции, направленные на выполнение компетенции органов.

Прежде всего, ряд полномочий по обеспечению критической информационной инфраструктуры РФ закон закрепляет за Президентом РФ, который вырабатывает основу государственной политики в этой сфере, а также определяет два федеральных органа исполнительный власти – орган, уполномоченный в области обеспечения безопасности критической информационной инфраструктуры и орган, обеспечивающий функционирование государственной системы обнаружения, предупреждения и ликвидации последствий компьютерных атак на информационные ресурсы РФ, порядок создания и задачи этой системы [13].

В рамках своих полномочий для обеспечения безопасности критической информационной инфраструктуры Правительство РФ выполняет такие основные функции как категорирование, контроль, интегрирование электросвязи. В связи с этим, в полномочия его входит: 1) по категорированию – установление данных факторов и критериев значимости объектов критической информационной инфраструктуры с их значениями, а также порядок и сроки осуществления их категорирования; 2) определение порядка и процедуры осуществления госконтроля в области безопасности информационной инфраструктуры; 3) налаживание единой сети электросвязи РФ для функционирования объектов информационной инфраструктуры [14].

На основании Указа Президента РФ № 569 от 25 ноября 2017 «О внесении изменений в Положение о Федеральной службе по техническому и экспортному контролю, утвержденное Указом Президента РФ от 16 августа 2004 года № 1085» ФСТЭК России является федеральным органом исполнительной власти, уполномоченным в области обеспечения безопасности критической информацион-

ной инфраструктуры, противодействия техническим разведкам и технической защиты информации [15].

Анализ нормативно-правовой базы, закрепляющей функции, компетенцию и полномочия основных субъектов государственной власти в сфере информационной безопасности позволяет сформулировать следующие положения. Сферы деятельности двух ключевых федеральных органов для обеспечения информационной безопасности – ФСБ и ФСТЭК России разделены. Так, в полномочия ФСТЭК входит обеспечение безопасности критической информационной инфраструктуры, а ФСБ отвечает за функционирование государственной системы обнаружения, предупреждения и ликвидации последствий компьютерных атак на информационные ресурсы РФ (далее ГосСОПКА).

В рамках своего правового положения ФСТЭК несет ответственность за: ведение реестра объектов КИИ, проверку правильности их категорирования, разработку требований по безопасности для каждой категории объектов, осуществление государственного контроля. В свою очередь, юридический статус ФСБ предполагает ответственность за: оценку состояния защищенности, порядок реагирования на компьютерные инциденты, порядок ликвидации последствий компьютерных атак, порядок обмена информацией об инцидентах, разработку требований к ГосСОПКА [16].

Указ Президента РФ от 25.11.2017 № 569 установил федеральным органом исполнительной власти, уполномоченным в области обеспечения безопасности КИИ – Федеральную службу технического и экспортного контроля России. Данный орган обладает следующими полномочиями в рассматриваемой сфере: ведет реестр объектов критической информационной инфраструктуры; устанавливает требования по обеспечению их безопасности и к созданию систем безопасности их функционирования; разрабатывает меры совершенствования правового регулирования в области обеспечения безопасности критической информационной инфраструктуры и предлагает их Президенту РФ и Правительству РФ; утверждает форму соответствующих документов (например, направления сведений о результатах присвоения объекту критической информационной инфраструктуры одной из категорий значимости либо об отсутствии необходимости присвоения ему одной из таких категорий); осуществляет государственный контроль в области информационной безопасности [17].

Положения Федерального закона № 187-ФЗ «О безопасности критической информационной инфраструктуры в РФ» создают понятие – Государственная система обнаружения, предупреждения и ликвидации последствий компьютерных атак (ГосСОПКА), которая представляет собой территориально распределенный комплекс на федеральном уровне, на уровне федеральных округов и на региональном уровне (в субъектах федерации). Закрепляет основу для создания Национального координационного центра по компьютерным инцидентам (НКЦКИ), представляющего собой структуру, отвечающую за обеспечение координации деятельности субъектов критической информационной инфраструктуры и являющейся составной частью ГосСОПКА. Создан он Приказом ФСБ России 2018 г «О национальном координационном центре по компьютерным инцидентам» [18].

Еще одно полномочие, возложенное на ФСБ России Указом Президента РФ от 15 января 2013 г № 31с «О создании государственной системы обнаружения, предупреждения и ликвидации последствий компьютерных атак на информационные ресурсы РФ», по созданию государственной системы предупреждения компьютерных атак, которая должна контролировать степень защищенности критической информационной инфраструктуры РФ от компьютерных атак. При этом до сих пор не было однозначного понимания, кто должен конкретно подключаться к этой системе. Теперь четко закреплено законом, что должны подключаться к системе ГосСОПКА все субъекты критической информационной инфраструктуры. Таким образом ключевая идея закона № 187-ФЗ заключается в создании единого центра мониторинга и управления информационной безопасностью для информационных систем, важных государству. Так, ранее на ФСБ были возложены полномо-

чия по созданию системы обнаружения, предупреждения компьютерных атак на информресурсы России (информсистемы и информационно-телекоммуникационные сети), ликвидации данных атак. Теперь решено возложить на ФСБ функции по создании ГосСОПКА [19].

Еще одним Указом Президента РФ от 22 декабря 2017 г № 620 «О совершенствовании государственной системы обнаружения, предупреждения и ликвидации последствий компьютерных атак на информационные ресурсы РФ» возложены на Федеральную службу безопасности функции федерального органа исполнительной власти, уполномоченного в области обеспечения функционирования государственной системы выявления компьютерных атак. В связи с чем, полномочиями ФСБ в этой сфере являются: обеспечение и контролирование данной системы, научно-техническая политика в этой сфере, разработка документации по обеспечению безопасности с использованием суперкомпьютерных и грид-технологий, проведение экспертных криптографических, инженерно-криптографических и специальных исследований шифровальных средств. Также в полномочия ФСБ входит: создание Национального координационного центра по компьютерным инцидентам, координация деятельности субъектов информационной инфраструктуры по компьютерным атакам, оценка уровня безопасности информационной инфраструктуры [20].

Выводы

Анализ тенденций нормативных положений позволяет выделить основные направления деятельности государственного аппарата: Президент РФ разрабатывает основу государственной политики в этой сфере, органы законодательной власти определяют концептуальную нормативную основу ключевых направлений государственной политики в сфере информационной безопасности, закрепляют правовое положение основных субъектов КИИ, их права, обязанности и ответственность; а исполнительная власть определяет ключевые исполнительные органы, отвечающие за информационную безопасность, и обеспечивает непосредственно сам процесс защиты значимых объектов КИИ и ликвидации компьютерных атак [21].

В соответствии с действующим российским законодательством и Концепцией национальной безопасности РФ задача федеральных исполнительных органов государственной власти в области обеспечения информационной безопасности сегодня сводится к интегрированию всех субъектов информационных отношений с целью учета и контроля функционирования значимых объектов КИИ и ликвидации компьютерных атак. Итак, для обеспечения безопасности критической информационной инфраструктуры необходимо провести следующие работы: 1) категорирование объектов КИИ, 2) проектирование и внедрение системы обеспечения безопасности КИИ. Первая группа работ включает в себя такие этапы, как: создание комиссии по категорированию, составление перечня объектов КИИ и его согласование, отправка его в ФСТЭК, анализ угроз безопасности, категорирование объектов КИИ и информирование ФСТЭК, экспертиза работ по КИИ. Вторая группа включает в себя деятельность по проектированию и внедрению системы обеспечения информационной безопасности, а также разработка документации для субъектов объектов КИИ.

Таким образом, всем субъектам КИИ нужно не только провести массу продолжительных по времени и дорогостоящих мероприятий, но и создавать эффективные системы безопасности. Однако, обслуживание этих систем, их модернизация и совершенствование требует финансовых, трудовых и иных ресурсов [22].

Проблемы информационной безопасности, несмотря на их важность и возросшую активность компьютерных атак, многими организациями не рассматривались и не решались, в связи с чем, угрозы постоянно возрастали. Сегодня же закон обязывает всех субъектов соблюдать требования по обеспечению информационной безопасности. Таким образом, актуальность обеспечения безопасности всех важных сфер, в частности, здравоохранения, науки, транспорта и связи, финансовый сектор, ракетно-космическая и других закономерно предполагает взаимосвязь трех звеньев государственного управления: федерального, окружного и регионального.

Затрагиваемые в статье проблемы представляют важность для национальной безопасности, в частности, в сфере информационной безопасности и безопасности критической информационной инфраструктуры, и потому нуждаются как в научном обосновании, так и в законодательном урегулировании в целях соответствия правовых норм современным реалиям.

Библиографический список

1. Митячкина Е.С., Михнева С.В. Правовое регулирование положения главы местной администрации и муниципального служащего в Российской Федерации // Гуманитарные исследования. – 2016. – № 2 (58). – С. 157-162.

2. Михнев И.П., Сальникова Н.А., Кравец А.Г. Защита информации от несанкционированного доступа при анализе радиационных характеристик помещений спектрометрическим методом // Известия Волгоградского государственного технического университета. – 2018. – № 8 (218). – С. 105-109.

3. Сальникова Н.А., Михнев И.П. Проведение аттестации знаний студентов с помощью компьютерного тестирования // Известия Волгоградского государственного технического университета. Серия: Новые образовательные системы и технологии обучения в вузе. – 2007. – Т. 4. – № 7 (33). – С. 182-184.

4. Федеральный закон от 26 июля 2017 г. № 187-ФЗ «О безопасности критической информационной инфраструктуры Российской Федерации» // Российская газета. – Федеральный выпуск. – 2017. – № 7333 (167). – 31 июля.

5. Михнев И.П., Михнева С.В., Айвазян А.Г., Серкина Е.П. Правовое регулирование деятельности в сфере информационной безопасности в Российской Федерации: достижения, проблемы и перспективы развития // Вестник Алтайской академии экономики и права. – 2018. – № 6. – С. 227-233.

6. Mikhnev I.P., Mikhneva S.V., Salnikova N.A. Studies of radon activity in civil engineering and environmental objects // International Journal of Engineering & Technology. [S.l.]. – 2018. – Vol. 7. – № 2.23. – P. 162-166.

7. Приказ ФСБ России № 368 от 24.07.2018 «Об утверждении Порядка обмена информацией о компьютерных инцидентах и Порядка получения субъектами критической информационной инфраструктуры информации о средствах и способах проведения компьютерных атак и о методах их предупреждения и обнаружения» // Собрание законодательства РФ. – 2017. – № 31 (Ч. I). – Ст. 4736.

8. Михнев И.П., Сальникова Н.А., Мединцева И.П. Защита конфиденциальной информации от несанкционированного доступа при проектировании автоматизированных систем радионуклидной спектрометрии на базе сцинтилляционного гамма-спектрометра. В книге: Научное обозрение: коллективная монография / гл. ред. Э.Н. Рябинина. – Чебоксары, 2018. – С. 48-58.

9. Краткий обзор ИТ-технологий, используемых в юридической деятельности / Р.Г. Драпезо [и др.] // Вестник Кемеровского государственного университета. – 2013. – № 1(53). – С. 306-312.

10. Агафонова Л.И., Полякова Е.С. Правовое положение органов государственной власти. В сборнике: Конституция России: глобальное, национальное, региональное: материалы Международной научно-практической конференции. – 2018. – С. 112-116.

11. Михнева С.В., Митячкина Е.С. Ценностные характеристики местного самоуправления // Гуманитарные исследования. – 2017. – № 4 (64). – С. 248-253.

12. Крылов А.Н., Иванова Ю.О. Сферы использования критической информационной инфраструктуры в РФ. В сборнике: Конституция России: глобальное, национальное, региональное: матер. междунар. науч.-практ. конференции. – 2018. – С. 63-68.

13. Михнева С.В., Михнев И.П., Чернова А.П. Правовые основы определения юридического положения должностных лиц местного самоуправления и муниципальных служащих в Российской Федерации. В сборнике: Социально-экономические и правовые основы инновационного развития: сборник научных статей. – Пенза, 2018. – С. 104-111.

14. Иванова Ю.О., Крылов А.Н. Функции субъектов по защите критической информационной инфраструктуры в РФ // Муниципальная служба: правовые вопросы. – 2018. – № 4. – С. 33-35.

15. Федеральный закон от 27 июля 2006 г. № 149-ФЗ «Об информации, информационных технологиях и о защите информации» // Российская газета – Федеральный выпуск. – 2006. – № 4131 (0). – 29 июля.

16. Михнев И.П., Михнева С.В. Природные радионуклиды как источник фонового облучения населения Нижневолжского региона. В сборнике: Образование и наука: современные тренды: коллективная монография. Серия «Научно-методическая библиотека» / гл. ред. О.Н. Широков. – Чебоксары, 2018. – С. 151-166.

17. Доктрина информационной безопасности РФ (утв. Указом Президента РФ от 5 декабря 2016 г. № 646). «Собрание законодательства РФ». 12.12.2016. № 50. Ст. 7074.

18. Михнева А.И. Формирование местного самоуправления в Российской Федерации: организационно-правовые аспекты // Аллея науки. – 2018. – Т. 5. – № 4 (20). – С. 813-817.

19. Маруков А. Н. Компьютерные преступления: классификация и способы противодействия: учебное пособие. – М.: Логос, 2015.

20. Кленина В.И. Информационные технологии в профессиональной деятельности юриста // Ученые записки. – 2010. – № 7. – С. 99-102.

21. Михнев И.П. Информационная безопасность на просторах мобильного интернета // Образовательные ресурсы и технологии. – 2015. – № 4 (12). – С. 66-70.

22. Бачолин Н. Л. Информационное право. Основы практической информатики. – М.: Юринформцентр, 2012.