ФЕДЕРАЛЬНОЕ СОБРАНИЕ РОССИЙСКОЙ ФЕДЕРАЦИИ

Развитие информационно-коммуникационного сотрудничества на пространстве ОДКБ

Издание Государственной Думы
2019

ФЕДЕРАЛЬНОЕ СОБРАНИЕ РОССИЙСКОЙ ФЕДЕРАЦИИ

ГОСУДАРСТВЕННАЯ ДУМА

Развитие информационно-коммуникационного сотрудничества на пространстве ОДКБ

Издание Государственной Думы
Москва • 2019

УДК 327(47+57)
ББК 66.4(0),6
Р17

Под общей редакцией

председателя Комитета Государственной Думы по делам СНГ,
евразийской интеграции и связям с соотечественниками
Л. И. Калашникова

Составители:

Кротов М. И., руководитель аппарата Комитета Государственной Думы по делам СНГ, евразийской интеграции и связям с соотечественниками,

Середа А. А., заместитель руководителя аппарата Комитета Государственной Думы по делам СНГ, евразийской интеграции и связям с соотечественниками,

Воробьев О. А., главный советник аппарата Комитета Государственной Думы по делам СНГ, евразийской интеграции и связям с соотечественниками,

Сааков А. А., главный советник аппарата Комитета Государственной Думы по делам СНГ, евразийской интеграции и связям с соотечественниками

Р17 **Развитие информационно-коммуникационного сотрудничества на пространстве ОДКБ.** – М.: Издание Государственной Думы, 2019. – 112 с.

УДК 327(47+57)
ББК 66.4(0),6

© Аппарат Государственной Думы, 2019

Содержание

Выступления участников

СТЕНОГРАММА
«круглого стола» Комитета Государственной Думы
по делам Содружества Независимых Государств,
евразийской интеграции и связям с соотечественниками на тему
«Развитие информационно-коммуникационного сотрудничества
на пространстве ОДКБ»

Здание Государственной Думы. Зал 137.
20 июня 2019 года. 16 часов.

Калашников Л. И. Давайте, коллеги, начнём.

Дело в том, что наш сегодняшний день немножко был переформатирован. Сегодня идёт «прямая линия» Президента России. И мы отменили пленарное заседание Государственной Думы. Тем не менее я должен сказать, что подавляющее большинство примет участие в работе «круглого стола», вот только у В. А. Шаманова график сломался, А. А. Панкин, заместитель министра иностранных дел, должен сейчас подъехать. И я думаю, что к нам другие товарищи будут присоединяться.

Уважаемые коллеги, дорогие друзья!

В соответствии с поручением Председателя Государственной Думы Вячеслава Викторовича Володина мы сегодня проводим этот «круглый стол».

Исполняющий обязанности генерального секретаря ОДКБ Валерий Анатольевич Семериков обратился с просьбой провести такой «круглый стол» и мы на неё с удовольствием откликнулись. Тема его «Развитие информационно-коммуникационного сотрудничества на пространстве ОДКБ».

Отмечаю высокий уровень представительства не только лидеров политических партий, комитетов, но и экспертного сообщества. Я думаю, это поспособствует успеху сегодняшнего «круглого стола», посвящённого рассмотрению путей усиления России и других стран ОДКБ в информационно-коммуникационном взаимодействии.

Времени не очень много прошло со времени формирования ОДКБ, его институтов, его правовых форм. И, конечно же, у нас ещё отсутствует системное правовое регулирование сферы информационного противоборства, а мы видим, что сегодня оно выходит на первый план. И каждый день нас «радуют» те, кого кто-то называет партнёрами (в кавычках), кто-то соперниками, исходя из того, как их характеризует политическая деятельность. Я их в своих выступлениях всегда представлял как наших, конечно же, далеко не партнёров, а, прежде всего, противников, и особенно в сфере безопасности. И всё время убеждаюсь в своей правоте. Но некоторые по-прежнему считают их партнёрами, в том числе и представители некоторых наших кругов, не только исполнительских, министерских, но и политических.

Однако ясно, что эта сфера, в том числе, регулирование этой сферы информационного противоборства, просто уже не терпит этой пустоты. И нам её, конечно же, надо заполнять, защищать. Надеюсь, что этим целям и многим другим, о которых я ещё не сказал, послужит наш сегодняшний «круглый стол».

В этой связи я хотел бы передать слово для ведения председателю постоянной комиссии Парламентской ассамблеи ОДКБ по вопросам обороны и безопасности, члену Комитета Государственной Думы по безопасности и противодействию коррупции Выборному Анатолию Борисовичу.

Пожалуйста, Анатолий Борисович, вам слово.

Выборный А. Б. Благодарю, уважаемый Леонид Иванович!

Уважаемые коллеги, прежде всего, позволю себе напомнить, что Организация Договора о коллективной безопасности – это единственная организация на постсоветском пространстве, которая является гарантом обеспечения коллективной и неделимой безопасности.

Как вы знаете, 30 лет назад межэтнические и многие другие конфликты стали причиной распада Советского Союза и так называемого парада суверенитетов. Каждая страна объявила о своей независимости, и как следствие – не стало единого экономического, политического и главным образом – оборонительного пространства.

Другими словами, тогда мы в один миг стали немного слабее с военной точки зрения. Однако, к счастью, в своё время была образована Организация Договора о коллективной безопасности. В настоящее время государствами – членами ОДКБ являются: Армения, Беларусь, Казахстан, Кыргызстан, Таджикистан и Россия. Затем в целях именно оперативной проработки модельных законодательных актов, гармонизации национальных законодательств, для решения уставных задач организации была образована Парламентская ассамблея ОДКБ.

И сегодня в целях развития системы информационно-коммуникационного сотрудничества на пространстве ОДКБ, проработки соответствующих модельных законодательных актов мы впервые рассматриваем данную тему, поскольку, как уже сказал Леонид Иванович, это пространство необходимо, с одной стороны, заполнять совершенно другим контентом и работать на опережение: перейти от оборонительной повестки в этой сфере, может быть, даже к наступательной, с позитивной точки зрения. И главное – вырабатывать механизмы превенции, о которых мы даже раньше и не говорили.

Более подробно об этом я позволю себе рассказать в своём выступлении в порядке очерёдности, а сейчас с удовольствием предоставляю слово Валерию Анатольевичу Семерикову, исполняющему обязанности Генерального секретаря ОДКБ.

Пожалуйста, Валерий Анатольевич.

Семериков В. А. Спасибо.

Добрый день!

Уважаемый Леонид Иванович, разрешите выразить вам искреннюю признательность за организацию «круглого стола» на столь актуальную и злободневную сегодня тему. Эта проблема в последнее время занимает всё более заметное место в повестке дня нашей организации, что вполне закономерно, поскольку информация и информационные технологии играют возрастающую роль как в жизни рядовых граждан наших стран, так и в деятельности их государственных и общественных институтов.

На актуальность задачи коллективного противодействия деструктивному воздействию на интересы государств – членов ОДКБ обратил особое внимание министр иностранных дел Российской Федерации Сергей Викторович Лавров в ходе заседания Совета министров иностранных дел 22 мая этого года. Попытки западных СМИ исказить отношения между партнёрами

по ОДКБ Сергей Викторович Лавров охарактеризовал как «акты информационной агрессии».

Уважаемые участники «круглого стола», развитие информационно-коммуникационных технологий привело к превращению в XXI веке информации в важнейший стратегический ресурс, вполне сопоставимый по значению с финансово-экономическим, военным, либо сырьевым потенциалом государств. В силу этого становится понятным стремление геополитических оппонентов России и её союзников по ОДКБ воспользоваться нынешней хаотизацией глобального миропорядка и розней систем международного права для закрепления за собой лидерства в информационной сфере.

Попытки России и её союзников переломить эту тенденцию и побудить Запад совместно разработать правовую регламентацию деятельности государств в информационной сфере успеха, к сожалению, пока не приносят. Показательно в этом плане, что 17 декабря 2018 года Генеральная ассамблея ООН большинством голосов приняла российскую резолюцию «Противодействие использованию информационно-коммуникационных технологий в преступных целях». Соавторами резолюции выступили партнёры России по ОДКБ. «За» проголосовали 94 государства, против – 59, воздержались – 33. В ходе голосования Соединённые Штаты Америки и страны Европейского союза наглядно продемонстрировали, что не намерены выносить тему борьбы с киберпреступностью на площадку Организации Объединённых Наций.

Между тем, процессы, происходящие в глобальном информационном пространстве, имеют прямую проекцию на ситуацию в зоне ответственности ОДКБ. Стремительное развитие и внедрение информационно-коммуникационных технологий во все сферы жизнедеятельности современного общества несут с собой не только прогресс и процветание, но и порождают новые по своей природе вызовы и угрозы его безопасности, требующие своевременного и адекватного реагирования.

В этих условиях наши государства вынуждены предпринимать конкретные меры для защиты своих интересов в информационном пространстве. Наиболее полно они отражены в принятой в 2016 году Стратегии коллективной безопасности ОДКБ до 2025 года и в Соглашении о сотрудничестве государств – членов ОДКБ в области обеспечения информационной безопасности.

Сегодня в формате нашей организации активно действуют механизмы практического взаимодействия в указанной области. Так, в рамках проводимых в формате Организации операций постоянного действия «ПРОКСИ» реализуются скоординированные мероприятия по противодействию преступности в сфере информационных технологий.

Весомым вкладом в коллективные усилия наших государств по борьбе с вызовами и в их коллективную безопасность в условиях роста информационных угроз призвана стать реализация принятого на прошедшей в ноябре 2018 года в Астане сессии Совета коллективной безопасности плана мероприятий по развитию скоординированной информационной политики в интересах государств – членов Организации договора.

Механизмы деструктивного информационного воздействия на личность общества и государства постоянно совершенствуются, а масштабное манипулирование сознанием принимает угрожающий характер.

Через информационное пространство осуществляется целенаправленная дискредитация конституционных основ государств и их властных структур, размывание национального менталитета и самобытности, вовлечение людей

в экстремистскую и в террористическую деятельность, разжигание межнациональной и межконфессиональной вражды, формирование радикального и протестного потенциала.

С учётом этого, в общем спектре вызовов угроз безопасности государств – членов ОДКБ, на одно из центральных мест постепенно выдвигается угроза их информационному суверенитету.

В последнее время на национальном уровне в государствах – членах ОДКБ происходит всё более очевидное осознание масштабов этой угрозы и необходимости выработки комплекса мер противодействия ей.

Эта задача, в частности, нашла отражение в утверждённой Президентом Российской Федерации 5 декабря 2016 года Доктрине информационной безопасности Российской Федерации, а также в принятой постановлением Совета Безопасности Республики Беларусь 18 марта этого года Концепции информационной безопасности Республики Беларусь и в утверждённой 3 мая постановлением Правительства Кыргызстана Концепции информационной безопасности Киргизской Республики до 2023 года.

Аналогичные по смыслу нормы и принципы закреплены в национальном законодательстве и других государств нашей организации. С учётом этого весьма своевременной и актуальной представляется задача гармонизации национального законодательства государств-членов в части, касающейся противодействия угрозам и их суверенитету в информационной сфере, а также разработка правовых актов на эту тему в формате ОДКБ.

Оптимальной площадкой для решения этой задачи могла бы, на наш взгляд, стать Парламентская ассамблея ОДКБ, обладающая для этого необходимым опытом и соответствующим экспертным потенциалом.

Опыт деятельности спецслужб государств – членов Организации свидетельствует о том, что из всех коммуникационных технологий именно компьютерные являются основным средством создания и поддержания деятельности террористических и религиозно-экстремистских организаций.

По данным «Лаборатории Касперского», в 2018 году четыре из шести государств – членов ОДКБ: Белоруссия, Армения, Киргизия и Казахстан – вошли в состав 20 государств мира с наибольшим числом пользователей, подвергшихся атакам через сеть «Интернет».

Особую тревогу вызывает активное использование для распространения в информационном пространстве фальсифицированной, недостоверной и запрещённой информации из социальных сетей, которая в коммуникационной сфере является лидером по охвату аудитории.

Учитывая высокий уровень интернет-проникновения в государства – члены ОДКБ, можно отметить, что социальные сети ныне служат средой, где разворачивается серьёзная борьба за умы в первую очередь молодёжи, для которой сеть «Интернет» выступает в качестве главного, а зачастую единственного источника информации, формирующей её мировоззрение.

Опыт Российской Федерации и её партнёров по ОДКБ говорит о том, что при умелом и грамотном подходе работа государственных структур в социальных сетях способна обеспечить положительные результаты.

На это, в частности, указывает практика широкого задействования цифровой дипломатии в деятельности министерств иностранных дел Российской Федерации и Республики Беларусь, а также других государств – членов ОДКБ, активно использующих социальные сети для донесения до целевой аудитории актуальной, правдивой и разносторонней информации о ситуации на постсоветском пространстве и крупнейших мировых событиях.

Во многом основываясь на этом опыте, Секретариатом ОДКБ ныне осуществлён масштабный выход в социальные сети, заведены и активно используются аккаунты организации в социальных сетях. Установлены контакты и налажено взаимодействие с администрациями социальных сетей, а также с интернет-компаниями.

Рассчитываем на то, что сотрудничество с этими провайдерами будет способствовать расширению информационного поля и увеличению численности потребителей актуальной и правдивой информации о деятельности ОДКБ как в государствах – членах Организации, так и в третьих странах.

Говоря о необходимости более активного присутствия государства в интернет-пространстве, следует подчеркнуть, что одним из основных средств противодействия деструктивному информационному влиянию должна выступить активная высокотехнологичная и целенаправленная деятельность государственных СМИ. Современные принципы выстраивания сложной слаженной работы государств – членов ОДКБ, государственных СМИ и экспертного сообщества, а также потенциал структур самой организации раскрывается в разрабатываемом ныне в формате ОДКБ проекте документа, нацеленного на противодействие деструктивному информационному воздействию на государства – члены ОДКБ.

Уважаемые участники «круглого стола», рассчитываем на открытый и содержательный обмен мнениями о перспективах развития информационно-коммуникационного сотрудничества на пространстве ОДКБ. Исходим из того, что он послужит вкладом в налаживание конструктивного взаимодействия между всеми участниками этого процесса – властными структурами, средствами массовой информации, провайдерами, регуляторами и органами самой организации в интересах отстаивания информационного суверенитета наших государств.

Спасибо за внимание.

Выборный А. Б. Благодарю вас, Валерий Анатольевич.

Действительно сегодня сформировался мощный запрос на оздоровление информационного поля и даже на площадке экспертно-консультативного совета Парламентской ассамблеи ОДКБ высказываются разные предложения на этот счёт, в том числе, например, создание беспилотного параллельного национального и даже наднационального интернет-пространства в рамках ОДКБ, которое обеспечит и позитивный контент, и защиту от провокационных и фейковых вопросов, минимизацию экстремистской, террористической, националистической и другой деструктивной идеологии.

И я уверен, что сегодня и по этим, и другим многим вопросам, конечно же, участники «круглого стола» будут высказывать свою точку зрения.

Сейчас я с удовольствием предоставляю слово председателю Комитета Государственной Думы по информационной политике, информационным технологиям и связи Леониду Леонидовичу Левину.

Пожалуйста, Леонид Леонидович.

Левин Л. Л. Добрый день, коллеги! Уважаемый Леонид Иванович, Валерий Анатольевич, Анатолий Борисович, дорогие друзья, коллеги!

Организация Договора о коллективной безопасности является одним из важнейших институтов поддержания законности, безопасности и правопорядка на пространстве Содружества Независимых Государств. Наши страны связывает не только общая история и экономические связи, но и понимание общего стратегического пути, обусловленного историческим наследием, географическими позициями, схожестью менталитета граждан.

Эффективность формата ОДКБ как международной региональной организации подтверждается примерами успешного сотрудничества в реализации совместных проектов, направленных на отражение угроз, имеющих глобальный трансграничный характер.

Усилия военных и правоохранительных ведомств стран-участниц, направленных на борьбу с наркотрафиком, проникновением террористических элементов, на противодействие распространению экстремизма, координируется из единого центра. Это позволяет гибко распоряжаться имеющимися материальными человеческими ресурсами, эффективно решая поставленные задачи.

В эру цифровой трансформации, которую сейчас проходит всё человечество, коммуникационные технологии, сети передачи данных и киберпространство принципиальным образом меняют все процессы, протекающие в обществе. Бизнес и государственное управление, образование и здравоохранение, средства массовой информации и правоохранительные органы – во всех этих областях широко внедрены интернет-технологии. Однако повсеместное проникновение цифровых технологий открывает перед международной преступностью новые технологические возможности, а трансграничность и анонимность сети – способность уходить от ответственности.

Сегодня на международных площадках высказываются призывы к выработке единых для всех правил взаимодействия с глобальной сетью, однако прогресс в этом направлении идёт слишком медленно, и законодатели развитых стран мира сейчас сконцентрированы на совершенствовании национальных норм права.

С учётом успешного опыта реализации международных программ в подходе к регулированию сети «Интернет» именно ОДКБ может выступить как координационный центр приведения правовых систем стран-участниц к единым стандартам. Это может стать существенным шагом для повышения уровня эффективности противодействия угрозам как в национальных сегментах сети «Интернет», так и на общеевразийском пространстве.

К настоящему моменту в Российской Федерации действует развёрнутое законодательство, позволяющее эффективно противодействовать различным видам противоправного контента, оперативно реагировать на возникающие киберугрозы и поддерживать стабильную работу информационных систем, которые развёрнуты на территории нашей страны и обеспечивают работу органов государственного управления, финансовых институтов и стратегически важных объектов.

Вместе с тем, другие страны – участницы ОДКБ также обладают собственными наработками и опытом выстраивания безопасного и доверенного цифрового пространства для своих граждан. В этом контексте Организация Договора о коллективной безопасности может выступить в качестве экспертно-аналитического центра для выработки предложений по межгосударственным законодательным инициативам в сфере регулирования информационно-коммуникационных технологий.

Ещё одной из сфер, где, на наш взгляд, ОДКБ имеет возможность реализовать свой потенциал как межрегиональный координатор, является общая коммуникационная политика, реализуемая на современных цифровых платформах.

Информационное взаимодействие государства и граждан, протекающее в различных форматах и на различных площадках, предназначено для реше-

ния самых разных задач. В то же время актуальное информирование населения и противодействие попыткам манипулирования общественным мнением для государственных структур является одним из приоритетов, направленных на обеспечение стабильности в обществе.

Сегодня наша общая задача заключается в том, чтобы, опираясь на наработанный опыт взаимодействия между нашими странами, последовательно развивать координацию межгосударственных связей, включающую не только силовое и правоохранительное сотрудничество, но и научно-технические инициативы, строительство общей телекоммуникационной инфраструктуры, а также центров мониторинга и управления киберпространством.

Уважаемые коллеги, сегодняшняя наша встреча на площадке Государственной Думы является важным этапом на пути выработки решений для определения общей информационно-коммуникационной политики на пространстве Евразийского экономического союза, и поможет обеспечить нашим странам синергию в реализации успешных цифровых инициатив. Надеемся, что и наши предложения войдут в эти заключительные итоговые документы, которые будут выработаны по итогам нашего сегодняшнего заседания. Спасибо.

Выборный А. Б. Благодарю Вас, Леонид Леонидович.

Действительно трудно поспорить с тем предложением, что иногда те вызовы и угрозы, с которыми мы сталкиваемся не только в России, но и в других странах, опережают правовое регулирование.

Вы знаете, совсем недавно на одной из площадок в рамках «Парламентской газеты» мы обсуждали вопросы противодействия терроризму. Некоторые эксперты прямо говорят, что законодательная база катастрофически отстаёт.

У нас появились новые вызовы. Появились, например, такие, как обработка несовершеннолетних террористическими аниматорами, которые с ранних лет, с 5, 7, 10 лет «влюбляют» их в себя, не в себя даже, а в террористическую деятельность. Эти аниматоры не обучают детей владению оружием, нет. Они просто фанатично ориентируют их на то, что спустя 10, 15 или 20 лет, когда те будут, например, главными инженерами атомных станций, придёт время выполнить ту миссию, ради которой они пришли на эту Землю. Вот это и многие-многие другие подобные вещи требуют от нас – законодателей, экспертов – учитывать опасность таких случаев и ориентироваться на то, чтобы предотвратить их.

Уважаемые коллеги, спасибо, ещё раз, Леонид Леонидович. И я слово предоставляю заместителю министра обороны Российской Федерации, начальнику Главного военно-политического управления Андрею Валерьевичу Картаполову. Пожалуйста, Андрей Валерьевич.

Картаполов А. В. Спасибо большое, Анатолий Борисович.

Уважаемые коллеги! С большим удовлетворением принял приглашение выступить сегодня на «круглом столе» по столь актуальной проблематике.

В современном мире информация становится стратегическим национальным ресурсом, одним из основных богатств государства. Однако быстрое совершенствование информационно-коммуникационных технологий повлекло, помимо несомненных преимуществ, и появление ряда серьёзных проблем.

Важнейшей из них стала необходимость обеспечения политической безопасности личности, общества, государства и всех его институтов, потому что в современных конфликтах методы борьбы стремительно смещаются в стороны комплексного применения: информационных, политических, экономических

и других невоенных мер. При этом стираются сами границы между состоянием войны и состоянием мира.

Я хотел бы обратить ваше внимание на такие характерные черты противоборства в информационно-коммуникационной среде, как всесторонний характер использования современных информационно-коммуникационных технологий целью тотального контроля сознания: от создания фейковых новостей до конструирования ложных реальностей, конструирования ложных социальных проблем, противоречий и тому подобных вещей с целью разрушения единства социально-политических систем и отношений как внутри государства, так и между государствами.

Нашими партнёрами во главе с Соединёнными Штатами организуется поддержка нетрадиционных религиозных структур, независимых в кавычках изданий и медиа-ресурсов, а также недальновидных или откровенно враждебно настроенных политических деятелей, популярных медийных личностей и представителей культуры и искусства. При этом основные усилия направляются на разрушение цивилизационной, государственной, идеологической, культурной, религиозной и тому подобной идентичности как нашего государства, так и наших партнёров по ОДКБ.

При этом главным объектом поражения в этом противоборстве являются не сами люди, а определённые типы сознания: общественное, индивидуальное. Причём поражение общественного сознания влечёт за собой разрушение общества в целом. Примером этому служат события на Украине, в Ливии, в Сирии, и мы массу других подобных примеров знаем. Подобные сценарии прорабатываются и в отношении государств – членов ОДКБ.

Но главной мишенью для Соединённых Штатов и их союзников безусловно остаётся Российская Федерация. Именно против нас развязана полномасштабная информационная война, которая сделала особенно очевидной растущую конфронтацию ценностных систем России и Запада. Мы буквально охвачены целой сетью специальных натовских центров в Прибалтике, Польше, Румынии, Болгарии и других странах Северо-Атлантического альянса, с территории которых активно действуют различные так называемые неправительственные организации. Их назначение – пропагандистское идеологическое воздействие на наших граждан, прямая дискредитация России, позиционирование её как авторитарной страны с диким агрессивным невежественным населением и властью, которая не считается с нормами международного права.

Кроме того, в сети «Интернет» широко реализуются проекты американских спецслужб, такие как «графика», «металл...», «эхо Рунета», нацеленные на прямое манипулирование общественным сознанием, прежде всего молодёжи. Осуществляется ряд программ, направленных на формирование у молодёжи активной протестной активности и недовольства властями страны. Наиболее значимыми из этих сетей являются социальные сети и фонд «Свободная Россия».

С помощью современных масс-медиа и сетевых форм работы наши партнёры стремятся переформатировать индивидуальное, групповое, массовое сознание населения России и стран – участниц ОДКБ в нужном для себя ключе, при этом очень активно используется такой вид идеологического оружия как фальсификация истории и итогов Второй мировой и Великой Отечественной войны, вклада народов СССР в общую победу над фашизмом. Сохраняется опасность распространения различного толка экстремистской идеологии, осно-

ванной на идеях радикального ислама и неонацизма. Всё больше места эти идеи находят себе на просторах сети «Интернет», где к ним особенно восприимчивы молодые люди.

Серьёзную опасность представляют граждане, вернувшиеся из районов, контролируемых экстремистами в Ираке, в Сирии, участвующие в ведении боевых действий, остающиеся действенными носителями крайних радикальных взглядов. И сегодня это проблема не только России, но и стран южного фланга ОДКБ.

Россия, выполняя задачи по борьбе с терроризмом в Сирии, по разгрому экстремистских движений и группировок, делает всё возможное, чтобы не допустить распространения этой идеологии и её ползущей экспансии на север, то есть к нам в дом, в дома наших соседей и друзей.

Я хотел бы выразить благодарность депутатам Государственной Думы за весомую поддержку и принятие очень необходимого нам закона по организации военно-политической работы номер 118 от 29 мая. Мы в ближайшее время ожидаем решение об организации военно-политической работы также и в других войсках и в воинских формированиях и органах. И убеждён, что наш опыт будет полезен и для ОДКБ, потому что именно военно-политическая работа призвана воспитывать у военнослужащих иммунитет к такому воздействию.

Уважаемые участники «круглого стола»! Вчера в Министерстве обороны Российской Федерации завершилась научно-практическая конференция, выступая на которой, Сергей Кужугетович Шойгу, министр обороны Российской Федерации, Герой России, обратил внимание на то, что негативное информационно-психологическое воздействие – это, по сути, оружие массового поражения. Его способы становятся всё более действенными и изощрёнными. Появилась возможность через информационно-коммуникационное пространство, организованное и скоординированное в масштабах целых государств и даже их сообществ, влиять не только на того, кого они считают своим противником, но и на своих партнёров. В таких условиях неспособность государств – членов ОДКБ обеспечить надёжную защиту своих национальных и духовных ценностей приведёт к разложению государственных институтов, в том числе Вооружённых Сил и поставит под сомнение историческую перспективу любого общества.

Поэтому сегодня особую актуальность приобретают вопросы формирования активной и согласованной информационной политики государств – членов ОДКБ. Развитие общего информационного пространства, создание совместного потенциала по противодействию информационным угрозам в отношении прав и свобод граждан в интересах государства и общества, защищённости информационных ресурсов и коммуникационных систем как национальных, так и в целом в составе организации.

Успешное решение задачи информационного воздействия и противодействия информационной агрессии необходимое, как нам видится, условие дальнейшего развития Организации Договора о коллективной безопасности в качестве организации, способной проводить эффективную политику по укреплению региональной безопасности в целом.

Уже говорили сегодня, что наиболее восприимчивой к любой информации и соответственно самой уязвимой частью общества является подрастающее поколение. Вопросам формирования у подрастающего поколения качеств гражданина и патриота, преданного идеалам служения своему народу и Отечеству, Министерством обороны Российской Федерации уделяется самое пристальное

внимание. В этих целях по инициативе министра обороны Российской Федерации и при поддержке Президента Российской Федерации создано Всероссийское детско-юношеское военно-патриотическое общественное движение Юнармия. За более чем три года своего существования оно стало ведущим военно-патриотическим молодёжным общественным объединением в стране. И сегодня оно объединяет в своих рядах более полумиллиона юношей и девушек во всех субъектах Российской Федерации, а также молодых россиян, проживающих в Белоруссии, Казахстане, Киргизии, Таджикистане, Армении, и даже в Соединённых Штатах. Движение стало узнаваемо и востребовано в молодёжной среде.

Вот одним из приоритетных проектов является создание современного многофункционального интернет-портала движения Юнармия для предоставления ребятам возможности самообразования и общения, получения информации из интернет-ресурсов Минобороны России и организации партнёра движения. Полагаем, что подобные интернет-порталы могут быть созданы и у наших партнёров на основе их молодёжных движений.

Очевидно, что проблема информационно-коммуникационной безопасности носит комплексный характер, её решение требует системного использования законодательных, организационных, технологических, административных и иных мер обеспечения безопасности, в том числе, блокирования распространения в нашем общем информационном пространстве негативных материалов о странах ОДКБ, целенаправленно искажающих их традиции и историю.

Я хочу выразить уверенность, что Государственная Дума и законодательные органы других государств и организаций выработают общие подходы к решению задач обеспечения духовного суверенитета на пространствах Организации Договора о коллективной безопасности, доминирования в информационной сфере общих духовно-нравственных ценностей наших народов.

Позвольте пожелать нашим парламентариям эффективного и системного взаимодействия в сфере развития информационно-коммуникационного сотрудничества на просторах ОДКБ в интересах укрепления информационной безопасности наших государств.

Благодарю за внимание.

Выборный А. Б. Благодарю вас, Андрей Валерьевич.

Что касается законотворческого процесса, научно-практической конференции, то, продолжая вашу мысль, позволю напомнить, что не так давно на базе Генеральной прокуратуры Российской Федерации (это было в ноябре прошлого года) по инициативе Федеральной службы безопасности, наших комитетов, Парламентской ассамблеи ОДКБ мы провели научно-практическую конференцию. Она касалась развития модельного законодательства как инструмента обеспечения безопасности и противодействия новым вызовам и угрозам.

Как вы знаете, законотворческий процесс каждого государства достаточно насыщен в рамках ОДКБ. Ретроспективный анализ показывает, что правовое регулирование за время деятельности Парламентской ассамблеи ОДКБ дало свои очевидные результаты. К настоящему времени принято порядка 70 нормативно-правовых актов в рамках развития модельного законодательства.

Так вот, опуская многие вещи, я бы хотел остановиться на некоторых выводах этой конференции. Среди ряда вопросов обозначены некоторые проблемные вопросы.

Мы обсуждали вопросы, в том числе, особенности и перспективы научно-методического, информационно-аналитического и экспертного обеспечения процессов разработки, принятия и реализации модельного законодательства.

В целях оценки актуальности этих вопросов и путей их решения, тех проблем, которые обозначены, проведён экспертный опрос. Кто участвовал в экспертном опросе? Это работники федеральных органов власти и судебной системы, и исполнительной власти, законодательной власти, сотрудники Конституционного Суда, Верховного Суда, также представители порядка 30 ведущих образовательных организаций. И эксперты пришли к четырём основным выводам.

Первый – наиболее серьёзными проблемами, которые влияют на оперативность и эффективность разработки и использования модельных актов, является несовершенство систем информирования о принятых модельных актах, так называемой «обратной связи» с национальными парламентами по вопросам имплементации их положений, в том числе взаимодействие разработчиков этих актов с экспертами заинтересованных организаций.

Если потребуется, я буду расшифровывать каждый пункт. Но я думаю, что понятно, о чём идёт речь. Второй вывод – наиболее эффективными мерами развития организации подготовки модельных актов является повышение оперативности процедур их согласования, к примеру, используя современные цифровые технологии, а также создание и использование единой базы данных, в том числе со сведениями об экспертах, их компетенции, квалификации в области разработки модельных актов.

Третий – с точки зрения повышения качества модельных актов наибольшую поддержку экспертов получили такие меры как, например, усиление адресности их положений с учётом конкретных потребностей и правового регулирования государств – членов ОДКБ. Недавно, например, мы рассматривали модельный акт с точки зрения переброски наших войск из одного государства в другое. И проведение специальных правовых, научных и аналитических исследований на этот счёт.

И последний вывод. Наиболее действенными мерами по повышению эффективности использования положений модельных актов... Я почему подчёркиваю эти вещи? Потому что иногда разработка модельных актов идёт год, два, а то и три. И к моменту принятия модельного акта он уже по сути морально устарел. Динамика жизни настолько скоротечна, что иногда требуется принятие модельного акта в течение полугода. Если мы в течение полугода не принимаем тот или иной акт, уже требуется совершенно другой, который, по сути, будет отклонять все предыдущие.

Так вот, требуется создание в национальных парламентах унифицированной системы учёта и предоставления в секретариат Парламентской ассамблеи результатов имплементации положений модельных актов, включение в регламент деятельности национальных парламентов положений, раскрывающих конкретный порядок и устои их использования, а также разработка и внедрение методических и практических рекомендаций по имплементации положений модельных актов в национальные законодательства.

По сути, если мы в целом говорим об этих проблемах, о которых говорят эксперты, с точки зрения развития модельных актов, то все проблемы сводятся к информационно-коммуникационному характеру.

Уважаемые коллеги, слово предоставляю заместителю руководителя Федерального агентства по делам Содружества Независимых Государств, со-

отечественников, проживающих за рубежом и по международному гуманитарному сотрудничеству Михаилу Дмитриевичу Брюханову. Пожалуйста, Михаил Дмитриевич.

Брюханов М. Д. Спасибо огромное.

Уважаемые выступающие, благодаря вашим таким развёрнутым и полным выступлениям я могу опустить теоретическую часть и несколько дать количественных характеристик работы Россотрудничества в информационно-коммуникативной среде.

Наша задача, наша основная цель – это усиление гуманитарного влияния государства в зарубежных странах. Решаем мы эту задачу в 16 часовых поясах, ведём работу по достижению этой цели, в 81 стране, сейчас действует 98 центров. Приближённость к аудитории позволяет нам готовить качественный контент, актуализированный для тех людей, кого мы считаем своей целевой аудиторией.

Приоритет мы уделяем собственному контенту и стараемся делать так, чтобы он был максимально актуальным и максимально приближённым к происходящему. Например, у нас вчера начала работу летняя школа русской сценической речи в Грузии, куда приехали в том числе артисты русскоговорящих театров с Украины. Вообще небывалое событие. И мы стараемся очень деликатно во всех соцсетях, особенно в тех странах, откуда приехали участники этой летней школы, эту информацию продвигать, обсуждать. И мы видим абсолютно позитивное отношение в соцсетях, практически отсутствие негативных комментариев. И вот такой контент для нас особо ценен и особо важен.

Огромный наш потенциал, над которым ещё придётся очень сильно работать, чтобы превратить его в наши достижения, это две программы, которые Россотрудничество проводит в соответствии с указами Президента России. Одна программа называется «Новое поколение»: мы ежегодно привозим на ознакомительные поездки около 1500 молодых иностранных посетителей, специалистов из различных сфер народного хозяйства государств мира. Они встречаются со своими коллегами, посещают различные летние студенческие лагери. Посещают редакции средств массовой информации, парламент. Огромная ведётся работа. И потом уезжают. Уезжают 99 процентов с позитивным прекрасным настроением, с открытыми глазами, комментарии дают самые восторженные. Самое главное нам их потом не потерять. Самое главное нам их потом акцептовать в наши сети, чтобы они писали, чтобы они были проводниками каких-то наших идей, чтобы они были нашей и вовлечённой аудиторией.

Вторая программа: по поручению Правительства Российской Федерации Россотрудничество ежегодно набирает на бесплатные квоты для обучения в Российской Федерации 15 тысяч студентов из зарубежных государств. Они учатся здесь пять лет, а после выпуска уезжают в свои страны, где формируют управленческие, политические, культурные элиты. Это огромный потенциал, который надо использовать. Признаюсь честно, пока люди скорее самоорганизуются в различные ассоциации выпускников. Мы их как бы догоняем и пытаемся эту работу построить без давления, но активно и наступательно. Есть чем заняться. На этом направлении гордиться пока нечем, но я думаю, что раз мы видим проблемы, значит мы их решим. И это превратится в наш с вами общий ресурс.

Огромный потенциал гуманитарного влияния лежит именно в доведении справедливой позиции по разным рисковым темам, которые мы с вами можем

прогнозировать. Хороший пример могу привести, как слаженно с Министерством иностранных дел Российской Федерации Россотрудничество отработало по теме пакта Молотова-Риббентропа, который будет в сентябре-августе обсуждаться. Заранее были собраны так называемые вопросники-ответники, ведущие учёные российского государства написали эти темы. Эти темы будут разосланы нашим представителям, нашим специалистам – тем, кто ведёт работу в соцсетях, и кто ведёт работу в живом общении. И в посольствах это, естественно, будет всё использоваться. И я думаю, что эта работа позволит нам не исказить исторические факты и представить их в реальном свете, чтобы историческая правда была выше всей отрицательной пены, которую сейчас будут пытаться наши партнёры использовать.

Вот что я хотел рассказать о тех практических задачах, которые решает Россотрудничество при работе в сети «Интернет».

Выборный А. Б. Спасибо, Михаил Дмитриевич.

Действительно сохранить память о прошлом, чтобы понимать, где мы сейчас находимся, чтобы обеспечить не только наше, но и будущее поколение правдивой информацией. Это крайне важно. Спасибо за вашу работу.

Кстати, вот там, где вы говорили о том, что нет критики в социальных сетях, это, честно говоря, вызывает беспокойство, потому что любой контент, он обязательно найдёт как позитивный отклик, так и отрицательный. Но у вас хороший пример, у вас есть только позитивные.

Благодарю вас ещё раз.

Слово предоставляется исполняющему обязанности ответственного секретаря Парламентской ассамблеи ОДКБ Сергею Валерьевичу Поспелову.

Пожалуйста, Сергей Валерьевич, вам слово.

Поспелов С. В. Уважаемый Анатолий Борисович, уважаемые коллеги!

Спасибо большое, во-первых, за возможность выступить.

Действительно, Парламентская ассамблея ОДКБ является, наверное, на сегодняшний день основным разработчиком вместе со своими партнёрами, с которыми мы это делаем в рамках консультативного совета, в рамках наших комитетов, законодательства на пространстве ОДКБ. В том числе, включая партнёров нашей организации, а у нас наблюдателями являются Сербия и нижняя палата Афганистана, они тоже участвуют в этой большой работе.

И хотел бы рассказать о некоторых законодательные актах, которые были уже созданы на пространстве ОДКБ и на пространстве СНГ. Также хочу затронуть тему СНГ, потому что те страны, которые входят в ОДКБ, они по большей части за исключением наших наблюдателей являются участниками стран СНГ.

Вот хотел бы обратить внимание на первый слайд[1]. *(Демонстрируется слайд.)* Если можно следующий.

Это те документы, которые уже созданы на пространстве СНГ, которые уже были приняты, это модельные законы, рекомендации, проекты стратегий. Безусловно, они в разной степени имплементированы в то или иное законодательство стран, но могу сказать, что процент достаточно высокий. Вот последняя аналитика, которую мы подготовили в прошлом году. В этом году мы продолжаем данную работу. Конечно, требуется более системная работа, потому что можно формально имплементировать тот или иной законодательный акт, но он, безусловно, имеет свою специфику в законодательстве той или иной страны.

---

[1] Здесь и далее иллюстративный материал не приводится.

Также нужно учитывать факт, что развитие информационной сферы, Леонид Иванович о ней сегодня говорил, практически ежедневно ставит перед нами задачи об изменении законодательства. Если вчера ещё никто не мог подумать, что социальные сети могут в один день изменить ситуацию в стране, то сегодня ни для кого это совершенно не секрет. Ещё вчера мы не думали о том, что так называемая биг-дата или те информационные следы, которые человек оставляет в социальных сетях, в сети «Интернет», просто пользуясь смартфоном, даже отправляя sms, представляют какую-либо значимость. Сегодня же эта информация становится не только предметом охоты коммерческих предприятий, которые занимаются с её помощью продажей товаров, но и, вот коллеги из Минобороны России подтвердят, является, в том числе, одним из инструментов гибридных войн.

Соответственно, те модельные рекомендации, которые у нас сегодня созданы на пространстве СНГ, легли в основу продолжения работы. Для тех, кто не знает, работа в рамках Парламентской ассамблеи ОДКБ ведётся согласно нашей программе законотворческой деятельности, которую мы составляем вместе с нашими партнёрами, вместе с ОДКБ, с другими службами, которые участвуют в разработке данного законодательства. Экспертный совет, который возглавляет Анатолий Борисович, в эту программу будет также предлагать дополнения.

Мы сегодня подходим к завершению той программы, которая была принята на 2016–2020 годы, и с 2020 года будет составляться новая программа. Могу тоже сказать, что мы ждём ваших предложений и рекомендаций в рамках той работы, которую мы с вами вместе уже осуществляем.

И буквально несколько слов о тех важных законодательных актах, которые приняты на текущий момент и которые сейчас находятся в работе.

В 2013 году были приняты рекомендации по правовому регулированию эксплуатации открытых телекоммуникационных сетей и предупреждению их использования в террористических и иных противоправных целях. Это важный документ.

В 2014 году был разработан модельный регламент административных процедур, осуществляемых уполномоченными органами в сфере обеспечения информационной безопасности государств – участников СНГ и модельный закон о критически важных объектах информационно-коммуникационной инфраструктуры. Это документ, который внёс изменения в закон «Об информации, информатизации и защите информации».

В текущем году подготовлен проект «Стратегия и обеспечение информационной безопасности государств – участников СНГ», на сегодняшний день он находится на этапе утверждения на высшем межгосударственном уровне.

И также хотел бы сказать, что существует, но сейчас в работе находятся – рекомендации по сближению и гармонизации законодательства стран – участниц ОДКБ по защите государственных секретов и глоссарий основных понятий в законодательстве о государственной тайне государств – членов ОДКБ.

Ещё два важных документа, о которых я хотел бы сказать. Это принятая рекомендация по сближению и гармонизации национального законодательства государств – членов ОДКБ в сфере обеспечения информационно-коммуникационной безопасности. Это один из пунктов программы, который в 2014 году был утверждён Президентом Российской Федерации Владимиром Владимировичем Путиным – в тот год Россия председательствовала в ОДКБ, и он в качестве председателя ОДКБ данную программу утвердил. Этот пункт выполнен,

а также подготовлены рекомендации по гармонизации законодательства государств – членов ОДКБ в сфере обеспечения безопасности критически важных объектов.

В 2018 году приняты такие важные, как мне кажется, модельные законы об информационном противоборстве терроризму и экстремизму, в этом году мы ждём их окончательного согласования. И, если будет окончательно согласован, мы будем выносить на предстоящее пленарное заседание проект рекомендаций по гармонизации законодательства государств – членов ОДКБ по обеспечению внутренней стабильности и противодействию технологиям внешнего деструктивного воздействия, направленным на дестабилизацию социально-политической обстановки.

Сложный документ, даже из названия понятно, что он многогранный.

Продолжается работа над проектами модельного закона об информационной безопасности, также разрабатывается концепция плана действий и инструментария для противодействия кибервызовам и угрозам (это инициатива наших армянских коллег), а также продолжается работа над рекомендациями по регулированию оборота виртуальных валют. Я думаю, что это тоже крайне важный момент. Несмотря на то, что достаточно актуальные модельные акты сегодня есть в программе работы Парламентской ассамблеи ОДКБ, безусловно, у нас всё ещё есть моменты, которыми необходимо дополнять данную программу.

Все эти вопросы обсуждались экспертами в 2017–2018 годах на ряде международных конференций.

Хотел бы отметить важность некоторых рекомендаций, их частично Анатолий Борисович озвучил, я бы хотел остановиться на некоторых из них.

Вот рекомендации, которые были приняты после конференции, проведённой совместно с Комитетом Государственной Думы по безопасности и противодействию коррупции, НИЦ ФСБ и Университетом прокуратуры, некоторые из них очень важны.

Первое – это процесс синхронизации и имплементации законодательства. Иногда бывает так: мы приняли модельное законодательство, рекомендации, одна страна имплементировала и ждём имплементации в других странах, что тоже иногда создаёт проблемы для продолжения работы.

Второе. Это создание общедоступных справочных информационных законодательных ресурсов в сфере безопасности и противодействия новым вызовам и угрозам, в том числе, можно, в принципе, подумать, на каком языке могли бы быть эти рекомендации. Учитывая, что русский язык – это язык работы внутри нашей организации, иногда бывают сложности с получением таких документов в других странах. Этот момент был отражён в рамках рекомендаций международной конференции.

А также есть ещё один момент. Это установление нормативных основ рассмотрения принятых в организации модельных законов и регламентных актов, как раз то, о чём говорил Анатолий Борисович. Это, конечно, внутреннее дело каждого государства, но вот, например, приведу пример Российской Федерации. Буквально год назад по инициативе Леонида Ивановича Калашникова и его комитета, в Регламент Государственной Думы была внесена поправка, предусматривающая обязательное их рассмотрение при принятии законодательных актов в сфере безопасности, сравнение их с модельными законами и рекомендациями, принятыми в рамках Парламентской ассамблеи ОДКБ.

Ну и, завершая, хочу сказать, в рамках информационной работы, конечно, нам много ещё предстоит сделать, в том числе и в рамках Парламентской ассамблеи ОДКБ.

Буквально на днях мы завершаем работу по созданию нового интернет-ресурса, нового сайта. Работаем над его созданием, понимая специфику организации, тут есть некоторые ограничения, это работа в социальных сетях. Хотел бы ради интереса привести пример информационной работы, которая ведётся нашими визави.

Если можно, следующий слайд, я его не буду комментировать. *(Демонстрируется слайд.)*

Ну, вот например, агентство НАТО по связи и информации выступает в качестве основного поставщика программ по консультированию, командованию и контролю, а также провайдера коммуникационных и информационных систем в рамках организации. Это всего лишь небольшой пример, говорящий о том, что нам совершенно не нужно стесняться этой работы, и она является сегодня абсолютно необходимой. Вот на этом бы хотел закончить.

Спасибо большое.

Выборный А. Б. Спасибо, Сергей Валерьевич.

Работы много. Я надеюсь, что если мы сейчас переформатируем работу секретариата благодаря тем научно-практическим конференциям, которые мы проводили на базе Генеральной прокуратуры Российской Федерации, а сейчас проводим в Минобороны России, то сможем придать новую динамику, которая даст нам возможность превзойти оборонительную повестку. С учётом тех вызовов и угроз, с которыми мы сталкиваемся, мы сможем, по крайней мере, создавать мощную превенцию для создания безопасного интернет-пространства, в том числе.

Слово сейчас предоставляется Димитрову Илие, президенту и основателю группы компаний «Селдон». Пожалуйста. Три минуты достаточно будет?

Димитров И. И. Я думаю, да.

Выборный А. Б. Прошу прощения, Илия, вы выходили с инициативой о создании параллельного интернет-пространства, которое не только обеспечило бы нашу национальную безопасность на интернет-платформе, но и наднациональную, в рамках ОДКБ.

Димитров И. И. Большое спасибо за предоставленное слово.

Все говорят, что мы находимся в новой реальности, то есть входим в ситуацию не просто так называемых гибридных войн, а в ситуацию, когда у нас меняется вообще парадигма мышления. К сожалению, а может быть, к счастью, большинство текущих систем безопасности, которые у нас есть, они построены в первую очередь на закрытых системах. Мы понимаем, что сеть «Интернет» – это, в первую очередь, открытая система. Если мы будем следовать тем же самым аспектам, выстраивать дальше системы защиты, связанные с закрытыми системами, то с одной стороны, это действительно правильно – защищать.

Но, может быть, нам сменить парадигму? Может быть, попытаться начать строить системы при открытом пространстве? И тогда просто системы безопасности, в том числе кибербезопасности и так далее, становятся другими. Потому что сейчас и мы, и наши американские так называемые друзья, строим свою работу так, что изначально был закрытый мир, и мы пытаемся его защищать.

По многим вещам это логично, но мы понимаем, что у нас есть отставание по ряду технологий, которое мы не можем преодолеть. Второй момент – все

языки программирования, начиная от низкого и заканчивая высоким уровнем, это не наши языки программирования. И тут мы тоже являемся заложниками, потому что подготовка специалистов, она в первую очередь ведётся на тех же самых языках. Создание нового языка, как и создание собственных операционных систем, конечно, это важно, но опять же мы бьём по хвостам.

То есть если мы не изменим парадигму, мы будем постоянно находиться в ситуации догоняющих. То, что мы видим, это, с точки зрения информационных, телекоммуникационных технологий, действительно очень хорошая программа, важная цифровая экономика. Но она не отражает все вопросы. Там отдельно есть хороший раздел по безопасности, но он использует старую парадигму. И я думаю, что, наверное, не имеет смысла обсуждать дальше эту тему, потому что это имеет смысл в каком-то научном или закрытом формате. Но необходимо построение, подчёркиваю, модели безопасности при открытом мире, имея в виду, что мы переходим в киберфизический мир, где одновременно физический мир сливается с цифровым.

И ещё важный момент. Мы понимаем, что порядок нового мира, он отражает в первую очередь даже не информацию, а он отражает управление будущим с точки зрения прогностической модели поведения того или иного субъекта, в том числе цифрового пространства. Если мы говорим про прогностическую модель поведения, это, в первую очередь, модель поведения из будущего, то есть управление объектом и, в первую очередь, рисками, а не по факту, когда уже случилось.

Такой модели, мы точно понимаем, нету ни у китайских коллег, ни у европейских, ни тем более у американских.

У нас не так много времени и не так много сил. Но мы всегда делали нестандартные шаги, и сейчас если мы посмотрим на эту задачу нестандартно, можем начать разработку иного технического уровня – есть определённый задел, и можно просто уйти в другое направление.

Спасибо большое.

Выборный А. Б. Благодарю вас.

Ну есть надежда, что мы будем отталкиваться от тех идей, которые вы озвучили, в нашей дальнейшей работе. Спасибо.

Но по крайней мере теперь я буду знать, откуда в моих социальных сетях комментарии на англоязычном языке, и наши коллеги, которые появляются из-за рубежа. Просветили, спасибо.

Слово предоставляется Евгению Юрьевичу Зайцеву, заместителю директора департамента Федеральной службы по надзору в сфере связи, информационных технологий и массовых коммуникаций.

Пожалуйста, Евгений Юрьевич.

Зайцев Е. Ю. Спасибо за возможность выступить.

Моё выступление будет касаться конкретно пресечения распространения экстремистского и террористического контента в российском сегменте сети «Интернет», потому что сеть «Интернет», она всё чаще, и мы это видим, используется для распространения различных экстремистских и террористических материалов.

Это обусловлено рядом технических возможностей сети. Во-первых, это условная анонимность тех пользователей, которые размещают контент, высокая скорость передачи информации, а также возможность её тиражирования на широкую аудиторию, масштаб охвата, потому что те же соцсети, о которых говорили уже неоднократно, они миллионы людей охватывают, и, по сути, ин-

формация может быть на десятки миллионов людей распространена буквально за несколько минут, и, безусловно, это трансграничность сети «Интернет», интерактивность распространения иных материалов.

При этом распространяемые крупными экстремистскими и террористическими организациями материалы подготовлены довольно качественно и профессионально, по крайней мере, мы это видели на примере ИГИЛ, с начала его существования. Сейчас, конечно, качество снизилось, как снизилась тенденция к широкому распространению материалов, они распространяются не так массово.

При этом целью таких материалов может быть как устрашение массового пользователя, так и вербовка новых адептов. У нас имеются два механизма пресечения распространения такой информации.

Первый механизм – это запущенный в ноябре 2012 года Единый реестр запрещённой информации, порядок которого предусматривает блокировку или удаление запрещённой информации.

Хочу сказать, что эта работа, безусловно, идёт в рамках решений суда, и что бы ни говорили наши западные коллеги, Российская Федерация очень взвешенно подходит к признанию материалов экстремистскими и террористическими, это делает суд.

Эта работа ведётся нами совместно с МВД России, ФСБ и органами прокуратуры и за всё время нами удалено из сети «Интернет» порядка 70 тысяч материалов экстремистского характера, доступ к 7 тысячам сайтам заблокирован, потому что материалы удалить отказались.

Речь идёт о цифровых копиях материалов, внесённых в федеральный список экстремистских материалов. Я напомню: в списке сейчас 4900 записей.

Внесение таких сайтов в список происходит по поступлению в Роскомнадзор либо судебного решения, либо письма от прокуратуры, ФСБ или МВД России. При этом я хочу отметить, что с аппаратом НАК нами проведена большая работа, совместно с органами прокуратуры, ФСБ и МВД по подготовке специальных методических рекомендаций по взаимодействию в рамках блокировки экстремистского и террористического контента.

Второй механизм – это система блокировки сайтов на основании требований Генпрокуратуры России. Это статья 15.3 Федерального закона «Об информации», который на текущий момент регулирует деятельность сети «Интернет».

Этот механизм предусматривает незамедлительную блокировку сайтов с призывами к экстремистской деятельности, к массовым беспорядкам, несанкционированным митингам, сайтов иностранных и международных неправительственных организаций, деятельность которых признана нежелательной на территории Российской Федерации.

Вот буквально недавно в эту статью внесены изменения в отношении блокировки «фейков» так называемых, недостоверной общественно значимой информации, которая создаёт угрозу причинения вреда жизни и здоровью граждан, уже были первые кейсы работы по этой норме.

Мы блокируем такие ресурсы и, в том числе требование Генпрокуратуры России позволяет нам самостоятельно находить «зеркала». То есть что имеется в виду под «зеркалами»? В случае, когда запрещённый контент мигрирует на другой ресурс, мы его находим и блокируем снова.

На текущий момент по данному направлению наши основные усилия сконцентрированы на выявление и пресечение пропаганды деятельности и раз-

личных материалов международных террористических организаций, таких как: ИГИЛ, «Джебхат ан-Нусра», «Хизб ут-Тахрир аль-Ислами». Нами уже выявлены и приняты меры по 146 тысячам таких материалов.

Кроме того, работа ведётся и по материалам украинских экстремистских организаций, таких как «Правый сектор», УНА-УНСО, «Тризуб имени Степана Бандеры». Они не так широко распространяются в сети, поэтому нами выявлены только 15 тысяч материалов, по которым приняты соответствующие меры.

Предыдущие докладчики говорили, скажем так, о некоем своём пути России и стран ОДКБ в решении этих вопросов, касающихся, в том числе, сети «Интернет». И практика реализации российского законодательства, которое касается пресечения распространения этого контента в сети, показывает, что большинство сайтов удаляют запрещённую информацию после получения уведомления от Роскомнадзора ещё до момента блокировки ресурса.

Конечно, стоит отметить, что в основном это законопослушные сайты, форумы, соцсети, где пользователи размещают экстремистский контент, так называемый UGC-контент. И после того, как Роскомнадзор начинает взаимодействовать с такими ресурсами, запрещённый контент удаляется. Не удаляют контент экстремистского и террористического характера порядка 10 процентов сайтов. С 2012 года Роскомнадзором налажено взаимодействие с практически всеми более-менее крупными зарубежными и российскими сайтами, поэтому, когда мы к ним обращаемся, контент террористического и экстремистского толка удаляется.

В этом как раз и есть особенность российского законодательства: в то время как за рубежом, как правило, сразу блокируют сайты, мы даём определённый срок на удаление запрещённого контента. При этом в конце прошлого года этот срок был сокращён с трёх дней до суток, и сейчас все крупные ресурсы в течение суток удаляют контент экстремистского и террористического характера.

Причём я хочу отметить очень быструю и оперативную реакцию законодателей на новые вызовы и угрозы. Государственная Дума очень быстро и качественно разрабатывает и принимает новые законы, которые позволяют нам парировать новые угрозы в сети «Интернет», за это большое спасибо Леониду Леонидовичу и его комитету. В общей сложности у нас порядка 20 тысяч контактов различных площадок иностранных и российских.

Но я хотел также, об этом уже говорили до меня, отметить важность создания позитивного и профилактического контента, потому что когда мы экстремистский контент блокируем или удаляем, возникает некий вакуум, и его необходимо замещать каким-то позитивным контентом.

В заключение я хотел бы сказать, что, безусловно, мы понимаем, что наибольшей эффективности можно достигнуть в борьбе с этой угрозой на международном уровне, поэтому взаимодействие наших стран в рамках ОДКБ нужно и полезно.

Мы очень активно взаимодействовали с белорусскими коллегами, с коллегами из Казахстана, они к нам приезжали неоднократно для обмена опытом. Я считаю, что, безусловно, такие мероприятия важны, нужно обсуждать, нужно делиться опытом, перспективными практиками. Мы всегда рады такие мероприятия поддержать.

Спасибо за внимание.

Семериков В. А. Спасибо, Евгений Юрьевич, за информацию, выступление.

Ну и, пользуясь случаем, я хочу сказать спасибо вам лично и федеральной службе за активное взаимодействие, которое мы постоянно осуществляем. Мы чувствуем вашу поддержку, помощь при проведении различных мероприятий в формате ОДКБ.

Уважаемые друзья, мы специально пригласили на «круглый стол» специалиста, который непосредственно занимается в формате ОДКБ вопросами противодействия вот этим вызовам и угрозам информационной среде. И сейчас я хочу предоставить слово Александру Владимировичу Кузнецову. Он кратко проинформирует о той работе, которая ведётся, и какие результаты уже достигнуты.

Пожалуйста, Александр Владимирович.

Кузнецов А. В. Уважаемые участники «круглого стола», рад приветствовать вас на сегодняшнем мероприятии, признателен за предоставленную возможность поделиться своим видением некоторых аспектов противодействия современным вызовам и угрозам.

Эта встреча является добрым сигналом, демонстрирующим заинтересованность государств – членов ОДКБ и международных организаций в объединении усилий в борьбе с терроризмом, наркотиками, нелегальной миграцией, негативным информационным воздействием на различные социальные слои населения, компьютерными и финансовыми преступлениями, которые планируются и осуществляются с использованием достижений научно-технического прогресса, информационных технологий и глобальных коммуникаций.

В условиях нестабильной военно-политической ситуации, используемой криминальными элементами в преступных целях, в 2008 году главами государств – членов Организации был сделан единственный объективно возможный вывод о максимальном укреплении межгосударственного сотрудничества в формате Организации.

В дополнение к проводимым в формате ОДКБ операциям по противодействию незаконному обороту наркотиков, противодействию незаконной миграции из третьих стран по предложению российской стороны, поддержаны всеми государствами – членами Организации и с 2009 года осуществляются совместные мероприятия в рамках операции по противодействию криминалу в сети «Интернет».

На протяжении прошедших лет руководством государств – членов ОДКБ предпринимаются интенсивные меры по повышению уровня цифровизации в своих странах и реализации крупных государственных проектов, демонстрируемых на слайде. *(Демонстрируется слайд.)*

Процессы глобализации и стремительное развитие web-технологий привели к популяризации информационных ресурсов в открытых телекоммуникационных системах. Национальные сегменты сети «Интернет» во многом взяли на себя информационные функции, сопоставимые со средствами массовой информации, и стали средством активного, в том числе, пропагандистского психологического воздействия на население и общество.

В этих условиях стали наиболее актуальными угрозами информационной безопасности (перечень привожу на слайде, с целью экономии времени). *(Демонстрируется слайд.)*

Исходя из специфики проводимых совместных мероприятий, участие в операции по противодействию криминалу в сети «Интернет» принимают спе-

циализированные подразделения национальных регуляторов всех государств – членов Организации.

Основные усилия при проведении операции сосредоточены на противодействии распространению в национальных сегментах сети «Интернет» информации, наносящей политический ущерб национальным и союзническим интересам, включая идеи терроризма, религиозного фундаментализма и экстремизма, используемые для разжигания религиозной и национальной розни.

Одновременно ведётся работа по профилактике характерных для современных вызовов и угроз противоправных деяний, связанных с распространением наркотиков, их производством и популяризацией, с незаконной миграцией и торговлей людьми, с электронным мошенничеством, с созданием электронных информационных ресурсов, распространяющих материалы, противоречащие национальным ценностям, общественным и моральным нормам, обычаям и традициям, преступлениям, связанным с распространением вредоносных и нелицензионных программ для электронных вычислительных машин, экономическим преступлением по легализации доходов, полученных преступным путём, иным преступлениям.

Опыт проведения в формате Организации операции «Канал нелегал» показал нарастающую тенденцию перехода в интернет-пространство противоправных сделок с наркотическими веществами, торговлей людьми, оружием, боеприпасами, взрывчатыми веществами, незаконный оборот которых в значительной степени способствует совершению преступлений террористической направленности. Кроме того, опасной становится нацеленность международных преступных организаций, террористов на осуществление диверсионной деятельности в киберпространстве.

В целом, несмотря на понесённые потери, международные террористические организации остаются мощной силой, угрожающей большинству стран мира. Терроризм стал прибыльным бизнесом, замкнувшим на себя многомиллиардные денежные потоки, а многообразие используемых механизмов финансирования даёт террористам дополнительный шанс на выживание.

Уважаемые дамы и господа, на сегодняшний день национальная правовая база государств – членов ОДКБ в этой сфере продолжает совершенствоваться, так практически во всех национальных законодательствах введена уголовная ответственность за пропаганду терроризма, а также за несообщение о подготовке и совершение преступлений террористической направленности.

Создан национальный правовой базис, позволяющий осуществлять выявление и досудебное блокирование противоправного контента, предусмотрены более суровые наказания за отдельные преступления террористической направленности.

В информационно-телекоммуникационной сфере большинством государств – членов Организации приняты пакеты антитеррористических законов, в том числе возложивших на операторов связи, организаторов распространения информации обязанность хранения и предоставления органам безопасности данных абонентов и ключей для дешифрования сообщений в сети «Интернет». Единая позиция государств – членов ОДКБ по вопросам опасности современных вызовов и угроз в мировом масштабе направлена на исключение навязывания двойных стандартов в определении киберпреступников, террористов и их пособников. Давно назрела необходимость выработки международных правил поведения в информационной сфере. Ведь сейчас размещение террористических ресурсов на иностранных серверах по сути обеспечивает их неуязвимость.

Пропаганда, вербовка, финансирование, связь, управление, лишь неполный перечень возможностей, которые террористы фактически утратят, если международное сообщество сможет прийти к консенсусу в данном вопросе и будет действовать скоординировано на основе единых правовых стандартов.

Уважаемые дамы и господа, завершая своё выступление, хочу ещё раз подчеркнуть, что рост вызовов и угроз в мире требует от нас укрепления доверительности и повышения уровня деполитизированного взаимодействия. Уверен, что в ходе «круглого стола» мы сможем сблизить позиции по наиболее острым противоречивым проблемам противодействия им.

Желаю участникам успешной и плодотворной работы.

Спасибо за внимание.

Семериков В. А. Спасибо, Александр Владимирович.

Слово для выступления предоставляется члену правления Российской ассоциации электронных коммуникаций Твердынину Марку Михайловичу.

Твердынин М. М. Добрый день, уважаемые коллеги!

Спасибо за возможность выступить. Все мы прекрасно осознаём, что современные вызовы суверенитету и безопасности государства становятся всё более цифровыми. При этом помимо кибероружия и кибершпионажа актуальным является тренд контентных угроз. То есть использование цифрового пространства для дестабилизации общества, возбуждения расовой национальной или религиозной вражды призывами к насилию, для пропаганды терроризма и вербовки в террористические сообщества, провокации массовых беспорядков.

Трансграничность сети «Интернет» даёт возможность злоумышленникам выбирать максимально удобные для них юрисдикции в плане размещения контента и регистрации доменных имён вне пределов досягаемости национальных правоохранительных органов тех стран, на население которых ориентирован этот деструктивный контент.

Определённая несбалансированность хостинговых и доменных мощностей наблюдается и на пространстве ОДКБ. В разных странах существует разный уровень развития хостинговой и доменной индустрии, включая ценовую политику, диверсификацию доменных регистраторов и хостинговых предложений, а также наличие или отсутствие иных средств в распространении информации, в частности интернациональных социальных сетей и мессенджеров. Подобная ситуация делает крайне целесообразной гармонизацию. И возможно координацию административных и технических мер по выявлению и пресечению оборота подобного контента на пространстве ОДКБ, причём речь в данном случае идёт не только о традиционных межгосударственных запросах правоохранительных органов.

Для обеспечения целостности пространства ОДКБ в условиях реальных вызовов его безопасности извне представляется необходимым принять ряд инфраструктурных и организационных шагов, в том числе обеспечить гармонизацию принципов и правил информационного оборота, возможных мер и оснований для пересечения оборота отдельных видов деструктивного контента. В настоящее время данная цель частично достигается через модельное законодательство для стран – участников СНГ. Однако принципы, содержащиеся в модельном законодательстве, не всегда находят оперативное отражение в национальных законах.

Исходя из этого необходима гармонизация регламентов выявления и пресечения контентных угроз, действий в условиях военного положения, чрезвычайного положения и контртеррористических операций. В частности,

представляется, что регламенты должны содержать меры по оперативному информационному обмену в пределах ОДКБ сведений о выявленном контенте для прекращения оборотов в случаях трансграничности.

Для управления процессами контентной безопасности целесообразно создание контентно-ситуационного центра – единого для пространства ОДКБ. Такой центр должен находиться во взаимодействии в режиме реального времени с национальными администрациями связи и иными профильными структурами ОДКБ, а также с органами технического регулирования обмена информации.

Основной задачей такого центра при наступлении чрезвычайной ситуации может стать мониторинг и реагирование контентной угрозы, при этом в силу национального или многонационального статуса центра и его взаимодействия с администрацией и связи появится гарантия реализации единого подхода к обороту конкретной единицы, представляющей информацию, предоставляющую угрозу информационной продукции.

Следует отметить, что подобный центр ни в коем случае не может и не должен выполнять функции цензуры, так как его возможности могут быть задействованы только в критической ситуации, предусмотренной документами ОДКБ, а именно в случаях военного положения, чрезвычайного положения, контртеррористической операции и аналогичных ситуаций, имеющих высокий приоритет в международном праве. Нечто подобное сейчас реализуется в сфере технической инфраструктуры сети «Интернет». Представляется, что подобные меры смогут повысить уровень информационной защищённости на пространстве ОДКБ и обеспечить должный уровень информационного обмена и гармонизированного реагирования в ситуациях, представляющих угрозу.

Спасибо.

Семериков В. А. Спасибо, Марк Михайлович.

Слово для выступления предоставляется Максимову Виталию Вячеславовичу – председателю совета директоров «ТрансПроект».

Максимов В. В. Благодарю, уважаемый председатель! Уважаемые коллеги!

Я хотел рассказать о нескольких практических аспектах, связанных с безопасностью в отношении проекта государственно-частного партнёрства, которым мы занимаемся многие годы. *(Демонстрируется слайд.)*

Пожалуйста, следующий слайд. Следует отметить, что большинство государственных программ, в том числе, и стратегия отрасли, равно как и стратегия развития информационного общества прямо предусматривает использование механизма государственно-частного партнёрства при реализации данных документов.

Также следует отметить: это не означает, что некие информационные системы будут реализованы с помощью частных денег, это говорит о том, что и в отношении государственных информационных систем прямо предусмотрено использование механизма государственно-частного партнёрства, равно как и привлечение частных инвестиций.

Пожалуйста, следующий слайд. *(Демонстрируется слайд.)*

С одной стороны, конечно, кажется, что незачем пускать частные инвестиции в развитие отношений государственных информационных систем, поскольку это в определённой степени, наверное, имеет определённый риск. Но, с другой стороны, если мы хотим обеспечить современное развитие, в том числе, и государственных информационных систем, государственных центров обработки данных, подчёркиваю, с применением современных технологий, мы

вынуждены привлекать частные инвестиции, потому что бюджетных возможностей, к сожалению, недостаточно. И это видно фактически во всех и национальных проектах, и в стратегиях развития.

Пожалуйста, следующий слайд. *(Демонстрируется слайд.)*

В этой связи в конце июня прошлого года были внесены изменения в Федеральный закон № 115-ФЗ «О концессионных соглашениях» и в Федеральный закон № 224-ФЗ «О государственно-частном и муниципально-частном партнёрстве...», открывший возможность использования и программ для ЭВМ, и баз данных, и информационных систем и сайтов в сети «Интернет» в качестве объектов, в отношении которых могут заключаться соглашения о государственно-частном, муниципально-частном партнёрстве равно как концессионные соглашения. *(Демонстрируется слайд.)*

Стоит отметить, что, конечно же, за прошедшее время таких проектов, чисто IT проектов, реализуемых на основе государственно-частного партнёрства, не так много, фактически всего шесть подано частных инициатив с предложением о заключении такого соглашения, но стоит отметить, что очевидно такая тенденция будет нарастать.

(Демонстрируется слайд.)

Конечно же, существующая деятельность и государственных органов, и частных инвесторов, которые реализуют или планируют реализовывать проекты государственно-частного партнёрства в сфере информационных технологий, сконцентрирована на том, чтобы найти, в первую очередь, оптимальный инвестиционный баланс, то есть баланс финансового участия государства и частного партнёра. И вопросам, связанным с безопасностью, и технико-технологическим аспектам, тоже базирующимся на безопасности, может быть не всегда уделяется должное внимание. По крайней мере, в упомянутых законах, в которые был внесён расширенный перечень объектов таких соглашений, такого нет. То есть фактически данная деятельность отдана в определённой степени на откуп государству и частным инвесторам, заключающим такие соглашения.

Мне представляется, что надо бы как раз больше, может быть, внимания уделить реализуемым проектам и проанализировать их. И, может быть, сделать какие-то выводы на будущее, может быть, даже связанные с изменением законодательства или с какими-то подзаконными актами.

Кроме всего прочего стоит отметить, что в сравнении с государствами ОДКБ, законодательство о государственно-частном партнёрстве в России и количество реализованных проектов государственно-частного партнёрства в разы, я бы даже сказал, на порядки превышает аналогичные проекты в странах ОДКБ. Поэтому, мне кажется, Российская Федерация должна взять такое определённое кураторство, в том числе методического характера, по совершенствованию законодательства и по распространению в странах ОДКБ практики реализации проектов государственно-частного партнёрства в Российской Федерации с тем, чтобы страны, которые всё равно пойдут по этому пути, избежали тех ошибок, с которыми столкнулись мы.

Вот что я хотел по этому поводу доложить.

Спасибо.

Шакиров О. И. Уважаемые коллеги, благодарю вас за приглашение выступить на этом «круглом столе».

В своём выступлении я хотел бы остановиться на трёх областях, где я вижу перспективы и даже необходимость развития информационно-коммуникаци-

онного сотрудничества на пространстве ОДКБ. Я буду, прежде всего, концентрироваться на деятельности самой организации и её государствах-участниках.

Первая сфера – это коммуникация в целом как способ рассказать о себе, о своей работе и миссии.

Второе направление – это взаимодействие через сеть «Интернет» с новыми аудиториями.

И третье направление – это как цифровизация в целом меняет или может менять работу организации.

Начнём с первого направления. Здесь не раз уже звучало описание ОДКБ как организации, которая вносит важный вклад в обеспечение безопасности государств-участников. И также в документах и в публичных заявлениях часто подчёркивается уникальный характер организации, отмечается, что она занимается как традиционными угрозами безопасности, так и новыми угрозами. Это всё известные положения, которые хорошо знают профессионалы, люди, которые работают в государственной сфере или эксперты.

Однако среди широкой общественности ОДКБ гораздо менее известно, и я предлагаю в целом подумать о том, чтобы ориентировать коммуникацию ОДКБ на повышение узнаваемости организации в государствах-участниках, среди широкой целевой аудитории, не только профессионалов.

Я читаю курс для студентов, и мы проводим упражнение – готовим стратегию ОДКБ для сети «Интернет», коммуникационную стратегию.

Я тут должен отметить, что когда мы первый раз провели это упражнение, ОДКБ не было в соцсетях, а когда мы проводили его последний раз, то ситуация совершенно изменилась.

Но при этом участники этой игры говорят, что ОДКБ должна быть более открыта, должна быть коммуникация на языках государств – членов Организации, хотя русский язык, безусловно, является официальным языком Организации. Они также говорят, что нужно подчёркивать роль простых военнослужащих или чиновников в работе Организации. То есть, чтобы у людей, которые следят за деятельностью ОДКБ, было понимание, что это такое вообще.

И если мы говорим про внешнюю коммуникацию, то тут важный лейтмотив – это, наверное, то, что было озвучено в недавнем совместном заявлении министров иностранных дел о предложениях к сотрудничеству, в частности, западным странам, но мы можем говорить и о других регионах. И здесь нужно ориентировать внешнюю коммуникацию ОДКБ, в том числе, через соцсети и через сеть «Интернет» именно на донесение этого месседжа.

Мы плавно переходим ко второй теме – это взаимодействие с новыми аудиториями. И это взаимодействие нужно тоже выстраивать по-новому.

В плане взаимодействия со СМИ нужно, возможно, расширять традиционные функции пресс-службы и искать новые формы партнёрств со СМИ. Например, готовить тематические материалы к мероприятиям. Я знаю, что такая работа ведётся, в том числе с каналом «Мир» или с другими каналами. Но можно ориентироваться на менее крупные интернет-порталы и так далее, и готовить, возможно, мероприятия к каким-то знаковым датам ОДКБ.

Если мы говорим о диалоге с аудиторией в соцсетях, то здесь важна именно диалоговая составляющая. Мы часто слышим вот эту идею о том, что коммуникация в сети «Интернет», она может быть двусторонней, однако на практике это не всегда реализуется. И можно понять, что не всегда хватает ресурсов, иногда не выстроены, не определены правила этого взаимодействия. Но мне кажется, нужно всерьёз подумать о том, как это можно учитывать.

Я уже сказал, что имеет смысл учитывать языки государств – участников ОДКБ и использовать их также в коммуникации. Например, если у нас есть диалог с экспертами, то нужно предусмотреть возможность перевода и выступлений не только на русском языке.

То о чём я хотел бы сказать в заключение, продолжает то, что сегодня уже заявляли другие выступающие. Это как цифровизация меняет работу организации в целом. Я бы хотел поддержать предложение Сергея Валерьевича Поспелова. Уже вот звучали замечания о том, что работа секретариата будет меняться.

Мне кажется, тут главное понимать, что какие бы задачи ни ставились перед Организацией, в любом случае речь идёт о том, что мы расширяем функционал, и это должно подразумевать усиление секретариата, создание ему адекватных возможностей. Если мы говорим про коммуникацию, то возможно речь должна идти о найме специальных сотрудников, которые будут заниматься коммуникацией, вэб-дизайном или созданием видеоконтента. Если мы говорим про информационную безопасность, то соответственно должны быть соответствующие специалисты – у команды, у секретариата в целом и у команд, которые занимаются отдельными направлениями. Я, может быть, говорю о каких-то супертехнических вещах, но мне кажется, у них должно быть адекватное обеспечение программным обеспечением, аппаратурой и необходимыми онлайн-подписками, если нужно.

Важный момент. Здесь много раз упоминалась тема противодействия террористическому контенту и блокировок сайтов. И это распространённый в мире метод борьбы с этой угрозой. Однако мы видим, что это не всегда работает. Не хочу как бы никого провоцировать, но мы видим, что после решения суда о блокировке Telegram, он продолжает действовать, и если вы уделите некоторое время, то вы легко найдёте там террористические каналы. То есть блокировки – это не панацея, тем более, они действуют как бы обычно реактивно, не проактивно. При этом мы знаем, что сами соцсети и онлайн-сайты, онлайн-сервисы имеют внутренние стимулы самостоятельно бороться с такой пропагандой. Тот же Telegram борется с этой пропагандой, ВКонтакте борются. На международном уровне наиболее известная инициатива называется «глобальный интернет-форум по противодействию терроризму», она организована крупными интернет-компаниями, которые между собой обмениваются информацией. В частности, у них есть такая база ..., то есть отпечатков террористической пропаганды. Условно говоря, если террористы залили видео на YouTube, это видео было идентифицировано, его отпечаток распространяется среди всех участков этого объединения, и террористы не могут залить то же видео, допустим, на Facebook.

Мне кажется, здесь нужно, во-первых, изучить этот опыт, и возможно наладить рабочее взаимодействие и с соцсетями, и с другими, может быть, менее крупными онлайн-сайтами, которые могут помочь здесь или подсказать дальнейшее регулирование или практическую деятельность.

Коллеги, я обозначил только некоторые направления, которые государства-участники и секретариат могли бы рассмотреть, чтобы шире использовать возможности информационно-коммуникационных технологий в деятельности Организации. Конечно, они будут более эффективны, если мы будем говорить о постепенной цифровизации, цифровой трансформации организации в целом. Этот процесс уже идёт, и я думаю, что сегодняшняя встреча – это одно из подтверждений этого. И я думаю, что если со стороны исполнительных органов

Организации и государств-участников будет готовность двигаться в этом направлении, то это встретит поддержку и у экспертов, и в целом у обществ наших стран. Спасибо за ваше внимание.

Семериков В. А. Спасибо, Олег Игоревич.

Уважаемые друзья, в соответствии с нашим регламентом работы, все желающие, которые записались выступить, выступили. Есть ещё желающие, кто-то с какой-то информацией? Если нет, то я думаю, что будем заканчивать, наверное, работу нашего «круглого стола».

Хочу поблагодарить всех участников «круглого стола» за то, что нашли время и пришли обсудить очень важную тему, которая, в общем-то, важна не только для Организации Договора о коллективной безопасности, она очень важна во всём мире, эта тема. И поверьте, что информационная безопасность в последнее время у нас выходит на первый план, так сказать, в плане всех вызовов и угроз. Поэтому большое спасибо выступающим, которые сделали очень интересные сообщения.

Ну и наши коллеги из Государственной Думы подготовили проект соответствующих рекомендаций по этому вопросу. Я думаю, что мы сейчас обобщим все эти выступления, все предложения, которые были высказаны в ходе работы, и эти рекомендации мы оформим и доведём до участников «круглого стола», ну и разошлём в заинтересованные соответствующие структуры. Наверное, так будет правильно, да?

Поэтому спасибо, ещё раз спасибо всем за работу. Всего самого доброго, всего хорошего.

До свидания.


КАРТАПОЛОВ А.В.


ЛЕВИН
ЛЕОНИД ЛЕОНИДОВ


ОСУДАРСТВЕННАЯ
ДУМА
ГОСУДАРСТВЕННАЯ ДУМА
ФЕДЕРАЛЬНОГО СОБРАНИЯ РОССИЙСКОЙ ФЕДЕРАЦИИ
«Круглый стол»
на тему:
«Развитие информационно-коммуникационного сотрудничества на пространстве ОДКБ»
20 июня 2019 года, 16.00
Охотный ряд, д.1, зал № 137

Рекомендации «круглого стола» на тему «Развитие информационно-коммуникационного сотрудничества на пространстве ОДКБ»

В соответствии с поручением Председателя Государственной Думы Федерального Собрания Российской Федерации, Председателя Парламентской ассамблеи Организации Договора о коллективной безопасности В. В. Володина № 1.1-335 от 21 января 2019 г. 20 июня 2019 года Комитетом Государственной Думы по делам Содружества Независимых Государств и связям с соотечественниками в Государственной Думе был организован и проведён «круглый стол» на тему «Развитие информационно-коммуникационного сотрудничества на пространстве ОДКБ».

В работе «круглого стола» приняли участие депутаты Государственной Думы Федерального Собрания Российской Федерации, члены Совета Федерации Федерального Собрания Российской Федерации, представители Администрации Президента Российской Федерации, Правительства Российской Федерации, министерств и ведомств Российской Федерации, авторизованных на пространстве ОДКБ социальных сетей и организаций, объединяющих интернет-сообщества, аналитики, эксперты, общественные деятели, представители средств массовой информации Российской Федерации.

ОДКБ является многофункциональной организацией коллективной безопасности нового типа, созданной для отражения как классических видов угроз, так и новых видов рисков и вызовов. При этом террористическая деятельность и информационная преступность по-прежнему представляют собой наиболее опасные угрозы устойчивому развитию государств – членов ОДКБ.

В марте 2019 года Президент Российской Федерации В. В. Путин отметил, что потенциал подготовки терактов сохраняется, и число предотвращённых террористических актов остаётся высоким – порядка 20 в год. В этой связи необходимо использовать новые формы и методы противодействия угрозам по выявлению вербовщиков и сообщников террористов, пресекать каналы поставки финансовых средств, пресекать пропагандистскую деятельность радикалов и экстремистов в сети «Интернет».

В 2018 году Россия пережила вал телефонных звонков с ложными сообщениями о готовящихся терактах – на вокзалах и в аэропортах, в торговых комплексах, кинотеатрах, учебных заведениях. В большинстве случаев подобные звонки поступали из-за рубежа.

Ответом на подобные действия стали поправки в Федеральный закон «О связи», оперативно подготовленные и принятые Государственной Думой, позволившие операторам блокировать по запросам правоохранительных органов телефонные номера, с которых делались звонки с ложными сообщениями о терактах. Ужесточена уголовная ответственность, в том числе, за заведомо ложные сообщения об актах терроризма, предусмотренная статьями 207 и 274[1] Уголовного кодекса Российской Федерации.

В законодательство внесены нормы, призванные воспрепятствовать использованию террористами информационных технологий и средств связи.

В Федеральный закон № 149-ФЗ «Об информации, информационных технологиях и защите информации» от 27 июля 2006 года внесены изменения, возлагающие на организаторов обмена сообщениями с использованием мессенджеров обязанность предоставлять ключи дешифровки сообщений и их передачу исключительно идентифицированным пользователям. После более четырёх миллиардов компьютерных атак 26 июля 2017 года был принят Федеральный закон № 187-ФЗ «О безопасности критической информационной инфраструктуры Российской Федерации».

Учитывая, что сеть «Интернет» – это сугубо трансграничное явление, которое пока стоит особняком в международном правовом поле, сегодня крайне необходимы как серьёзные международные договорённости, так и рекомендации тех органов, которые занимаются техническим регулированием. Вместе с тем, развитие информационно-коммуникационных технологий и необходимость совершенствования механизмов защиты информационного пространства ОДКБ требует консолидации усилий государств – членов ОДКБ в данной области и закрепления их на межнациональном уровне.

По итогам выступлений участников «круглого стола» сделаны следующие выводы:

1. Глобальное распространение радикальных, экстремистских идей представляет собой тревожную тенденцию в современном мире, ведёт к обострению террористических угроз, подрывает безопасность как отдельных государств, так и целых регионов, весьма негативно воздействует на международную безопасность и стабильность. Приоритетные задачи международного сотрудничества в рамках комплексных усилий по предупреждению терроризма, недопущению распространения экстремистских идей, организации эффективной контрпропаганды должны формулироваться в строгом соответствии с международным правом. Прежде всего Уставом ООН.

2. Риски и вызовы, связанные с использованием информационно-телекоммуникационных технологий (сеть «Интернет», социальные сети, блогосфера) в качестве инструмента для деструктивного воздействия на ОДКБ, включая пропаганду терроризма и экстремизма, требуют дальнейшей консолидации усилий государств-членов в формате Организации.

3. Гармонизация национального законодательства государств – членов ОДКБ в сфере противодействия угрозам информационному суверенитету должна стать темой для рассмотрения на площадке Парламентской ассамблеи ОДКБ, располагающей для этого необходимым опытом и экспертным потенциалом.

4. Цифровизация внешнеполитической деятельности, расширение присутствия государства в социальных сетях заключают в себе серьёзный потенциал позитивного воздействия на целевые аудитории, в первую очередь молодёжь.

5. Современные процессы, происходящие в информационном пространстве, обуславливают необходимость развития конструктивного сотрудничества между провайдерами и регулирующими структурами в интересах создания надёжной системы государственно-частного партнёрства в сети «Интернет».

Информационная сфера приобрела статус системообразующей, и от неё в значительной степени зависит уровень экономического, социального и политического развития общества и государства. С учётом изложенного предлагаем по итогам мероприятия в интересах развития информационно-коммуникационного сотрудничества на пространстве ОДКБ закрепить в качестве рекомендаций «круглого стола» законодательным органам, правительственным учрежде-

ниям, гражданскому обществу, академическим кругам и деловому сообществу, международным и неправительственным организациям государств – членов ОДКБ:

– выработать направления совершенствования правовых механизмов взаимодействия уполномоченных органов государств – членов ОДКБ с национальными компетентными структурами в области информационной политики и информационной безопасности в целях расширения диапазона возможностей совместной деятельности по борьбе с веб-ресурсами, пропагандирующими экстремистскую и террористическую деятельность, и совершенствования контроля информационного пространства ОДКБ;

– активизировать работу по совершенствованию правового регулирования и унификации законодательства, а также выработки единой политики в сфере противодействия деструктивному воздействию и информационной преступности на пространстве ОДКБ;

– содействовать выработке единых международных стандартов и подходов к проблематике блокирования и удаления противоправного контента в сети «Интернет». Обеспечивать как на национальном, так и на международном уровнях признание за государствами и их компетентными органами главенствующей роли по противодействию террористической пропаганде, включая определение критериев и контроль над блокировкой и удалением террористических и экстремистских материалов в сети «Интернет», при взаимодействии с частным сектором и гражданским обществом;

– противодействовать выдвижению на первый план международного контртеррористического сотрудничества элементов неконсенсусной концепции «противодействия насильственному экстремизму», допускающей вмешательство во внутренние дела суверенных государств, провоцирования протестных настроений и дестабилизации «неугодных» правительств, в том числе, под предлогом содействия в борьбе с терроризмом и экстремизмом;

– содействовать развитию практического взаимодействия между государствами – членами ОДКБ в области обеспечения международной информационной безопасности, в том числе, посредством реализации Соглашения о сотрудничестве государств – членов ОДКБ в области обеспечения информационной безопасности;

– активизировать межведомственное взаимодействие и оказывать информационную и организационную поддержку ОДКБ на уровне руководства федеральных министерств и ведомств в вопросах развития информационно-коммуникационного сотрудничества;

– проработать вопрос о создании Контентно-ситуационного центра, находящегося во взаимосвязи с органами технического регулирования, обмена информацией и осуществляющего мониторинг и реагирование на контентные угрозы в указанных ситуациях;

– предусмотреть возможность создания позитивного контента в популярных социальных сетях, направленного на укрепление межнационального и межконфессионального мира между молодыми гражданами в рамках межведомственного взаимодействия государств – членов ОДКБ;

– с целью обмена эффективными практиками по недопущению распространения деструктивного контента в сети «Интернет» рассмотреть возможность межведомственного взаимодействия в пределах государств – членов ОДКБ;

– проработать вопрос о создании объединённой рабочей группы экспертов, представителей ответственных ведомств государств – членов ОДКБ

по разработке общего алгоритма и перечня мер противодействия деструктивному информационно-психологическому влиянию;

– наладить рабочее взаимодействие по вопросам коммуникации в интернете между пресс-службой ОДКБ и ответственными отделами в министерствах обороны, иностранных дел и при необходимости в других ведомствах государств – членов ОДКБ;

– развивать информационные партнёрства с новостными агентствами и тематическими сайтами, выходящие за рамки традиционного взаимодействия пресс-службы со СМИ;

– рассмотреть возможность взаимодействия с частными интернет-компаниями по вопросам контртерроризма, в частности с российскими компаниями, а также с международными структурами, такими как Глобальный интернет-форум по противодействию терроризму (Global Internet Forum to Counter Terrorism);

– проработать вопрос создания рабочей группы по подготовке плана совместных мероприятий государств – членов ОДКБ, посвящённых 75-летию Победы в Великой Отечественной войне, с учётом развития информационно-коммуникационного сотрудничества;

– провести научно-практическую конференцию по проблеме подготовки кадров для решения задач обеспечения информационной безопасности в государствах – членах ОДКБ;

– используя опыт российской Юнармии, подготовить методические рекомендации для министерств образования государств – членов Организации Договора о коллективной безопасности по военно-патриотической работе со школьниками;

– распространить основные выводы и тезисы выступлений данного «круглого стола» в ведущих СМИ государств – членов Организации Договора о коллективной безопасности.

РОССИЙСКАЯ ФЕДЕРАЦИЯ

ФЕДЕРАЛЬНЫЙ ЗАКОН

ОБ ИНФОРМАЦИИ, ИНФОРМАЦИОННЫХ ТЕХНОЛОГИЯХ И О ЗАЩИТЕ ИНФОРМАЦИИ

Принят
Государственной Думой
8 июля 2006 года

Одобрен
Советом Федерации
14 июля 2006 года

Статья 1. Сфера действия настоящего Федерального закона

1. Настоящий Федеральный закон регулирует отношения, возникающие при:

1) осуществлении права на поиск, получение, передачу, производство и распространение информации;

2) применении информационных технологий;

3) обеспечении защиты информации.

2. Положения настоящего Федерального закона не распространяются на отношения, возникающие при правовой охране результатов интеллектуальной деятельности и приравненных к ним средств индивидуализации, за исключением случаев, предусмотренных настоящим Федеральным законом.

(в ред. Федерального закона от 02.07.2013 № 187-ФЗ)

Статья 2. Основные понятия, используемые в настоящем Федеральном законе

В настоящем Федеральном законе используются следующие основные понятия:

1) информация – сведения (сообщения, данные) независимо от формы их представления;

2) информационные технологии – процессы, методы поиска, сбора, хранения, обработки, предоставления, распространения информации и способы осуществления таких процессов и методов;

3) информационная система – совокупность содержащейся в базах данных информации и обеспечивающих ее обработку информационных технологий и технических средств;

4) информационно-телекоммуникационная сеть – технологическая система, предназначенная для передачи по линиям связи информации, доступ к которой осуществляется с использованием средств вычислительной техники;

5) обладатель информации – лицо, самостоятельно создавшее информацию либо получившее на основании закона или договора право разрешать или ограничивать доступ к информации, определяемой по каким-либо признакам;

6) доступ к информации – возможность получения информации и ее использования;

7) конфиденциальность информации – обязательное для выполнения лицом, получившим доступ к определенной информации, требование не передавать такую информацию третьим лицам без согласия ее обладателя;

8) предоставление информации – действия, направленные на получение информации определенным кругом лиц или передачу информации определенному кругу лиц;

9) распространение информации – действия, направленные на получение информации неопределенным кругом лиц или передачу информации неопределенному кругу лиц;

10) электронное сообщение – информация, переданная или полученная пользователем информационно-телекоммуникационной сети;

11) документированная информация – зафиксированная на материальном носителе путем документирования информация с реквизитами, позволяющими определить такую информацию или в установленных законодательством Российской Федерации случаях ее материальный носитель;

11.1) электронный документ – документированная информация, представленная в электронной форме, то есть в виде, пригодном для восприятия человеком с использованием электронных вычислительных машин, а также для передачи по информационно-телекоммуникационным сетям или обработки в информационных системах;

(п. 11.1 введен Федеральным законом от 27.07.2010 № 227-ФЗ)

12) оператор информационной системы – гражданин или юридическое лицо, осуществляющие деятельность по эксплуатации информационной системы, в том числе по обработке информации, содержащейся в ее базах данных;

13) сайт в сети «Интернет» – совокупность программ для электронных вычислительных машин и иной информации, содержащейся в информационной системе, доступ к которой обеспечивается посредством информационно-телекоммуникационной сети «Интернет» (далее – сеть «Интернет») по доменным именам и (или) по сетевым адресам, позволяющим идентифицировать сайты в сети «Интернет»;

(п. 13 введен Федеральным законом от 28.07.2012 № 139-ФЗ, в ред. Федерального закона от 07.06.2013 № 112-ФЗ)

14) страница сайта в сети «Интернет» (далее также – интернет-страница) – часть сайта в сети «Интернет», доступ к которой осуществляется по указателю, состоящему из доменного имени и символов, определенных владельцем сайта в сети «Интернет»;

(п. 14 введен Федеральным законом от 28.07.2012 № 139-ФЗ)

15) доменное имя – обозначение символами, предназначенное для адресации сайтов в сети «Интернет» в целях обеспечения доступа к информации, размещенной в сети «Интернет»;

(п. 15 введен Федеральным законом от 28.07.2012 № 139-ФЗ)

16) сетевой адрес – идентификатор в сети передачи данных, определяющий при оказании телематических услуг связи абонентский терминал или иные средства связи, входящие в информационную систему;

(п. 16 введен Федеральным законом от 28.07.2012 № 139-ФЗ)

17) владелец сайта в сети «Интернет» – лицо, самостоятельно и по своему усмотрению определяющее порядок использования сайта в сети «Интернет», в том числе порядок размещения информации на таком сайте;

(п. 17 введен Федеральным законом от 28.07.2012 № 139-ФЗ)

18) провайдер хостинга – лицо, оказывающее услуги по предоставлению вычислительной мощности для размещения информации в информационной системе, постоянно подключенной к сети «Интернет»;

(п. 18 введен Федеральным законом от 28.07.2012 № 139-ФЗ)

19) единая система идентификации и аутентификации – федеральная государственная информационная система, порядок использования которой устанавливается Правительством Российской Федерации и которая обеспечивает в случаях, предусмотренных законодательством Российской Федерации, санкционированный доступ к информации, содержащейся в информационных системах;

(п. 19 введен Федеральным законом от 07.06.2013 № 112-ФЗ)

20) поисковая система – информационная система, осуществляющая по запросу пользователя поиск в сети «Интернет» информации определенного содержания и предоставляющая пользователю сведения об указателе страницы сайта в сети «Интернет» для доступа к запрашиваемой информации, расположенной на сайтах в сети «Интернет», принадлежащих иным лицам, за исключением информационных систем, используемых для осуществления государственных и муниципальных функций, оказания государственных и муниципальных услуг, а также для осуществления иных публичных полномочий, установленных федеральными законами.

(п. 20 введен Федеральным законом от 13.07.2015 № 264-ФЗ)

Статья 3. Принципы правового регулирования отношений в сфере информации, информационных технологий и защиты информации

Правовое регулирование отношений, возникающих в сфере информации, информационных технологий и защиты информации, основывается на следующих принципах:

1) свобода поиска, получения, передачи, производства и распространения информации любым законным способом;

2) установление ограничений доступа к информации только федеральными законами;

3) открытость информации о деятельности государственных органов и органов местного самоуправления и свободный доступ к такой информации, кроме случаев, установленных федеральными законами;

4) равноправие языков народов Российской Федерации при создании информационных систем и их эксплуатации;

5) обеспечение безопасности Российской Федерации при создании информационных систем, их эксплуатации и защите содержащейся в них информации;

6) достоверность информации и своевременность ее предоставления;

7) неприкосновенность частной жизни, недопустимость сбора, хранения, использования и распространения информации о частной жизни лица без его согласия;

8) недопустимость установления нормативными правовыми актами каких-либо преимуществ применения одних информационных технологий перед другими, если только обязательность применения определенных информационных технологий для создания и эксплуатации государственных информационных систем не установлена федеральными законами.

Статья 4. Законодательство Российской Федерации об информации, информационных технологиях и о защите информации

1. Законодательство Российской Федерации об информации, информационных технологиях и о защите информации основывается на Конституции Российской Федерации, международных договорах Российской Федерации и состоит из настоящего Федерального закона и других регулирующих отношения по использованию информации федеральных законов.

2. Правовое регулирование отношений, связанных с организацией и деятельностью средств массовой информации, осуществляется в соответствии с законодательством Российской Федерации о средствах массовой информации.

3. Порядок хранения и использования включенной в состав архивных фондов документированной информации устанавливается законодательством об архивном деле в Российской Федерации.

Статья 5. Информация как объект правовых отношений

1. Информация может являться объектом публичных, гражданских и иных правовых отношений. Информация может свободно использоваться любым лицом и передаваться одним лицом другому лицу, если федеральными законами не установлены ограничения доступа к информации либо иные требования к порядку ее предоставления или распространения.

2. Информация в зависимости от категории доступа к ней подразделяется на общедоступную информацию, а также на информацию, доступ к которой ограничен федеральными законами (информация ограниченного доступа).

3. Информация в зависимости от порядка ее предоставления или распространения подразделяется на:

1) информацию, свободно распространяемую;

2) информацию, предоставляемую по соглашению лиц, участвующих в соответствующих отношениях;

3) информацию, которая в соответствии с федеральными законами подлежит предоставлению или распространению;

4) информацию, распространение которой в Российской Федерации ограничивается или запрещается.

4. Законодательством Российской Федерации могут быть установлены виды информации в зависимости от ее содержания или обладателя.

Статья 6. Обладатель информации

1. Обладателем информации может быть гражданин (физическое лицо), юридическое лицо, Российская Федерация, субъект Российской Федерации, муниципальное образование.

2. От имени Российской Федерации, субъекта Российской Федерации, муниципального образования правомочия обладателя информации осуществляются соответственно государственными органами и органами местного самоуправления в пределах их полномочий, установленных соответствующими нормативными правовыми актами.

3. Обладатель информации, если иное не предусмотрено федеральными законами, вправе:

1) разрешать или ограничивать доступ к информации, определять порядок и условия такого доступа;

2) использовать информацию, в том числе распространять ее, по своему усмотрению;

3) передавать информацию другим лицам по договору или на ином установленном законом основании;

4) защищать установленными законом способами свои права в случае незаконного получения информации или ее незаконного использования иными лицами;

5) осуществлять иные действия с информацией или разрешать осуществление таких действий.

4. Обладатель информации при осуществлении своих прав обязан:

1) соблюдать права и законные интересы иных лиц;

2) принимать меры по защите информации;

3) ограничивать доступ к информации, если такая обязанность установлена федеральными законами.

Статья 7. Общедоступная информация

1. К общедоступной информации относятся общеизвестные сведения и иная информация, доступ к которой не ограничен.

2. Общедоступная информация может использоваться любыми лицами по их усмотрению при соблюдении установленных федеральными законами ограничений в отношении распространения такой информации.

3. Обладатель информации, ставшей общедоступной по его решению, вправе требовать от лиц, распространяющих такую информацию, указывать себя в качестве источника такой информации.

4. Информация, размещаемая ее обладателями в сети «Интернет» в формате, допускающем автоматизированную обработку без предварительных изменений человеком в целях повторного ее использования, является общедоступной информацией, размещаемой в форме открытых данных.

(часть 4 введена Федеральным законом от 07.06.2013 № 112-ФЗ)

5. Информация в форме открытых данных размещается в сети «Интернет» с учетом требований законодательства Российской Федерации о государственной тайне. В случае, если размещение информации в форме открытых данных может привести к распространению сведений, составляющих государственную тайну, размещение указанной информации в форме открытых данных должно быть прекращено по требованию органа, наделенного полномочиями по распоряжению такими сведениями.

(часть 5 введена Федеральным законом от 07.06.2013 № 112-ФЗ)

6. В случае, если размещение информации в форме открытых данных может повлечь за собой нарушение прав обладателей информации, доступ к которой ограничен в соответствии с федеральными законами, или нарушение прав субъектов персональных данных, размещение указанной информации в форме открытых данных должно быть прекращено по решению суда. В случае, если размещение информации в форме открытых данных осуществляется с нарушением требований Федерального закона от 27 июля 2006 года № 152-ФЗ «О персональных данных», размещение информации в форме открытых данных должно быть приостановлено или прекращено по требованию уполномоченного органа по защите прав субъектов персональных данных.

(часть 6 введена Федеральным законом от 07.06.2013 № 112-ФЗ)

Статья 8. Право на доступ к информации

1. Граждане (физические лица) и организации (юридические лица) (далее – организации) вправе осуществлять поиск и получение любой информации

в любых формах и из любых источников при условии соблюдения требований, установленных настоящим Федеральным законом и другими федеральными законами.

2. Гражданин (физическое лицо) имеет право на получение от государственных органов, органов местного самоуправления, их должностных лиц в порядке, установленном законодательством Российской Федерации, информации, непосредственно затрагивающей его права и свободы.

3. Организация имеет право на получение от государственных органов, органов местного самоуправления информации, непосредственно касающейся прав и обязанностей этой организации, а также информации, необходимой в связи с взаимодействием с указанными органами при осуществлении этой организацией своей уставной деятельности.

4. Не может быть ограничен доступ к:

1) нормативным правовым актам, затрагивающим права, свободы и обязанности человека и гражданина, а также устанавливающим правовое положение организаций и полномочия государственных органов, органов местного самоуправления;

2) информации о состоянии окружающей среды;

3) информации о деятельности государственных органов и органов местного самоуправления, а также об использовании бюджетных средств (за исключением сведений, составляющих государственную или служебную тайну);

4) информации, накапливаемой в открытых фондах библиотек, музеев и архивов, а также в государственных, муниципальных и иных информационных системах, созданных или предназначенных для обеспечения граждан (физических лиц) и организаций такой информацией;

5) иной информации, недопустимость ограничения доступа к которой установлена федеральными законами.

5. Государственные органы и органы местного самоуправления обязаны обеспечивать доступ, в том числе с использованием информационно-телекоммуникационных сетей, в том числе сети «Интернет», к информации о своей деятельности на русском языке и государственном языке соответствующей республики в составе Российской Федерации в соответствии с федеральными законами, законами субъектов Российской Федерации и нормативными правовыми актами органов местного самоуправления. Лицо, желающее получить доступ к такой информации, не обязано обосновывать необходимость ее получения.

(в ред. Федерального закона от 27.07.2010 № 227-ФЗ)

6. Решения и действия (бездействие) государственных органов и органов местного самоуправления, общественных объединений, должностных лиц, нарушающие право на доступ к информации, могут быть обжалованы в вышестоящий орган или вышестоящему должностному лицу либо в суд.

7. В случае, если в результате неправомерного отказа в доступе к информации, несвоевременного ее предоставления, предоставления заведомо недостоверной или не соответствующей содержанию запроса информации были причинены убытки, такие убытки подлежат возмещению в соответствии с гражданским законодательством.

8. Предоставляется бесплатно информация:

1) о деятельности государственных органов и органов местного самоуправления, размещенная такими органами в информационно-телекоммуникационных сетях;

2) затрагивающая права и установленные законодательством Российской Федерации обязанности заинтересованного лица;

3) иная установленная законом информация.

9. Установление платы за предоставление государственным органом или органом местного самоуправления информации о своей деятельности возможно только в случаях и на условиях, которые установлены федеральными законами.

Статья 9. Ограничение доступа к информации

1. Ограничение доступа к информации устанавливается федеральными законами в целях защиты основ конституционного строя, нравственности, здоровья, прав и законных интересов других лиц, обеспечения обороны страны и безопасности государства.

2. Обязательным является соблюдение конфиденциальности информации, доступ к которой ограничен федеральными законами.

2.1. Порядок идентификации информационных ресурсов в целях принятия мер по ограничению доступа к информационным ресурсам, требования к способам (методам) ограничения такого доступа, применяемым в соответствии с настоящим Федеральным законом, а также требования к размещаемой информации об ограничении доступа к информационным ресурсам определяются федеральным органом исполнительной власти, осуществляющим функции по контролю и надзору в сфере средств массовой информации, массовых коммуникаций, информационных технологий и связи.

(часть 2.1 введена Федеральным законом от 29.07.2017 № 276-ФЗ)

3. Защита информации, составляющей государственную тайну, осуществляется в соответствии с законодательством Российской Федерации о государственной тайне.

4. Федеральными законами устанавливаются условия отнесения информации к сведениям, составляющим коммерческую тайну, служебную тайну и иную тайну, обязательность соблюдения конфиденциальности такой информации, а также ответственность за ее разглашение.

5. Информация, полученная гражданами (физическими лицами) при исполнении ими профессиональных обязанностей или организациями при осуществлении ими определенных видов деятельности (профессиональная тайна), подлежит защите в случаях, если на эти лица федеральными законами возложены обязанности по соблюдению конфиденциальности такой информации.

6. Информация, составляющая профессиональную тайну, может быть предоставлена третьим лицам в соответствии с федеральными законами и (или) по решению суда.

7. Срок исполнения обязанностей по соблюдению конфиденциальности информации, составляющей профессиональную тайну, может быть ограничен только с согласия гражданина (физического лица), предоставившего такую информацию о себе.

8. Запрещается требовать от гражданина (физического лица) предоставления информации о его частной жизни, в том числе информации, составляющей личную или семейную тайну, и получать такую информацию помимо воли гражданина (физического лица), если иное не предусмотрено федеральными законами.

9. Порядок доступа к персональным данным граждан (физических лиц) устанавливается федеральным законом о персональных данных.

Статья 10. Распространение информации или предоставление информации

1. В Российской Федерации распространение информации осуществляется свободно при соблюдении требований, установленных законодательством Российской Федерации.

2. Информация, распространяемая без использования средств массовой информации, должна включать в себя достоверные сведения о ее обладателе или об ином лице, распространяющем информацию, в форме и в объеме, которые достаточны для идентификации такого лица. Владелец сайта в сети «Интернет» обязан разместить на принадлежащем ему сайте информацию о своих наименовании, месте нахождения и адресе, адресе электронной почты для направления заявления, указанного в статье 15.7 настоящего Федерального закона, а также вправе предусмотреть возможность направления этого заявления посредством заполнения электронной формы на сайте в сети «Интернет».

(в ред. Федерального закона от 24.11.2014 № 364-ФЗ)

3. При использовании для распространения информации средств, позволяющих определять получателей информации, в том числе почтовых отправлений и электронных сообщений, лицо, распространяющее информацию, обязано обеспечить получателю информации возможность отказа от такой информации.

4. Предоставление информации осуществляется в порядке, который устанавливается соглашением лиц, участвующих в обмене информацией.

5. Случаи и условия обязательного распространения информации или предоставления информации, в том числе предоставление обязательных экземпляров документов, устанавливаются федеральными законами.

6. Запрещается распространение информации, которая направлена на пропаганду войны, разжигание национальной, расовой или религиозной ненависти и вражды, а также иной информации, за распространение которой предусмотрена уголовная или административная ответственность.

Статья 10.1. Обязанности организатора распространения информации в сети «Интернет»

(введена Федеральным законом от 05.05.2014 № 97-ФЗ)

1. Организатором распространения информации в сети «Интернет» является лицо, осуществляющее деятельность по обеспечению функционирования информационных систем и (или) программ для электронных вычислительных машин, которые предназначены и (или) используются для приема, передачи, доставки и (или) обработки электронных сообщений пользователей сети «Интернет».

2. Организатор распространения информации в сети «Интернет» обязан в установленном Правительством Российской Федерации порядке уведомить федеральный орган исполнительной власти, осуществляющий функции по контролю и надзору в сфере средств массовой информации, массовых коммуникаций, информационных технологий и связи, о начале осуществления деятельности, указанной в части 1 настоящей статьи.

3. Организатор распространения информации в сети «Интернет» обязан хранить на территории Российской Федерации:

1) информацию о фактах приема, передачи, доставки и (или) обработки голосовой информации, письменного текста, изображений, звуков, видео- или иных электронных сообщений пользователей сети «Интернет» и информацию

об этих пользователях в течение одного года с момента окончания осуществления таких действий;

2) текстовые сообщения пользователей сети «Интернет», голосовую информацию, изображения, звуки, видео-, иные электронные сообщения пользователей сети «Интернет» до шести месяцев с момента окончания их приема, передачи, доставки и (или) обработки. Порядок, сроки и объем хранения указанной в настоящем подпункте информации устанавливаются Правительством Российской Федерации.

(п. 3 в ред. Федерального закона от 06.07.2016 № 374-ФЗ)

3.1. Организатор распространения информации в сети «Интернет» обязан предоставлять указанную в части 3 настоящей статьи информацию уполномоченным государственным органам, осуществляющим оперативно-разыскную деятельность или обеспечение безопасности Российской Федерации, в случаях, установленных федеральными законами.

(п. 3.1 введен Федеральным законом от 06.07.2016 № 374-ФЗ; в ред. Федерального закона от 29.07.2017 № 241-ФЗ)

4. Организатор распространения информации в сети «Интернет» обязан обеспечивать реализацию установленных федеральным органом исполнительной власти в области связи по согласованию с уполномоченными государственными органами, осуществляющими оперативно-разыскную деятельность или обеспечение безопасности Российской Федерации, требований к оборудованию и программно-техническим средствам, используемым указанным организатором в эксплуатируемых им информационных системах, для проведения этими органами в случаях, установленных федеральными законами, мероприятий в целях реализации возложенных на них задач, а также принимать меры по недопущению раскрытия организационных и тактических приемов проведения данных мероприятий. Порядок взаимодействия организаторов распространения информации в сети «Интернет» с уполномоченными государственными органами, осуществляющими оперативно-разыскную деятельность или обеспечение безопасности Российской Федерации, устанавливается Правительством Российской Федерации.

4.1. Организатор распространения информации в сети «Интернет» обязан при использовании для приема, передачи, доставки и (или) обработки электронных сообщений пользователей сети «Интернет» дополнительного кодирования электронных сообщений и (или) при предоставлении пользователям сети «Интернет» возможности дополнительного кодирования электронных сообщений представлять в федеральный орган исполнительной власти в области обеспечения безопасности информацию, необходимую для декодирования принимаемых, передаваемых, доставляемых и (или) обрабатываемых электронных сообщений.

(п. 4.1 введен Федеральным законом от 06.07.2016 № 374-ФЗ)

4.2. Организатор распространения информации в сети «Интернет» в случае осуществления деятельности по обеспечению функционирования информационных систем и (или) программ для электронных вычислительных машин, которые предназначены и (или) используются для обмена электронными сообщениями исключительно между пользователями этих информационных систем и (или) программ для электронных вычислительных машин, при котором отправитель электронного сообщения определяет получателя или получателей электронного сообщения, не предусматриваются размещение пользователями сети «Интернет» общедоступной информации в сети «Интернет» и передача

электронных сообщений неопределенному кругу лиц (далее – организатор сервиса обмена мгновенными сообщениями), также обязан:

1) осуществлять идентификацию пользователей сети «Интернет», передачу электронных сообщений которых осуществляет организатор сервиса обмена мгновенными сообщениями (далее – пользователи сервиса обмена мгновенными сообщениями), по абонентскому номеру оператора подвижной радиотелефонной связи в порядке, установленном Правительством Российской Федерации, на основании договора об идентификации, заключенного организатором сервиса обмена мгновенными сообщениями с оператором подвижной радиотелефонной связи, за исключением случаев, предусмотренных настоящим Федеральным законом;

2) в течение суток с момента получения соответствующего требования уполномоченного федерального органа исполнительной власти ограничить возможность осуществления пользователем сервиса обмена мгновенными сообщениями, указанным в этом требовании, передачи электронных сообщений, содержащих информацию, распространение которой в Российской Федерации запрещено, а также информацию, распространяемую с нарушением требований законодательства Российской Федерации, в порядке, определенном Правительством Российской Федерации;

3) обеспечивать техническую возможность отказа пользователей сервиса обмена мгновенными сообщениями от получения электронных сообщений от других пользователей;

4) обеспечивать конфиденциальность передаваемых электронных сообщений;

5) обеспечивать возможность передачи электронных сообщений по инициативе государственных органов в соответствии с законодательством Российской Федерации;

6) не допускать передачу электронных сообщений пользователям сервиса обмена мгновенными сообщениями в случаях и в порядке, которые определены Правительством Российской Федерации.

(часть 4.2 введена Федеральным законом от 29.07.2017 № 241-ФЗ)

4.3. Организатор сервиса обмена мгновенными сообщениями, являющийся российским юридическим лицом или гражданином Российской Федерации, вправе осуществлять идентификацию пользователей сервиса обмена мгновенными сообщениями самостоятельно путем определения абонентского номера подвижной радиотелефонной связи пользователя сервиса обмена мгновенными сообщениями. Правительством Российской Федерации могут устанавливаться требования к порядку определения абонентского номера подвижной радиотелефонной связи пользователя сервиса обмена мгновенными сообщениями организатором сервиса обмена мгновенными сообщениями, являющимся российским юридическим лицом или гражданином Российской Федерации.

(часть 4.3 введена Федеральным законом от 29.07.2017 № 241-ФЗ)

4.4. Организатор сервиса обмена мгновенными сообщениями, являющийся российским юридическим лицом или гражданином Российской Федерации, обязан хранить сведения об идентификации абонентского номера подвижной радиотелефонной связи пользователя сервиса обмена мгновенными сообщениями (далее – идентификационные сведения об абонентском номере) только на территории Российской Федерации. Предоставление третьим лицам идентификационных сведений об абонентском номере может осуществляться только с согласия пользователя сервиса обмена мгновенными сооб-

щениями, за исключением случаев, предусмотренных настоящим Федеральным законом и другими федеральными законами. Обязанность предоставить доказательство получения согласия пользователя сервиса обмена мгновенными сообщениями на предоставление третьим лицам идентификационных сведений об абонентском номере данного пользователя сервиса обмена мгновенными сообщениями возлагается на организатора сервиса обмена мгновенными сообщениями.

(часть 4.4 введена Федеральным законом от 29.07.2017 № 241-ФЗ)

5. Обязанности, предусмотренные настоящей статьей, не распространяются на операторов государственных информационных систем, операторов муниципальных информационных систем, операторов связи, оказывающих услуги связи на основании соответствующей лицензии, в части лицензируемой деятельности, а также не распространяются на граждан (физических лиц), осуществляющих указанную в части 1 настоящей статьи деятельность для личных, семейных и домашних нужд. Правительством Российской Федерации в целях применения положений настоящей статьи определяется перечень личных, семейных и домашних нужд при осуществлении деятельности, указанной в части 1 настоящей статьи.

6. Состав информации, подлежащей хранению в соответствии с частью 3 настоящей статьи, место и правила ее хранения, порядок ее предоставления уполномоченным государственным органам, осуществляющим оперативно-разыскную деятельность или обеспечение безопасности Российской Федерации, а также порядок осуществления контроля за деятельностью организаторов распространения информации в сети «Интернет», связанной с хранением такой информации, и федеральный орган исполнительной власти, уполномоченный на осуществление этого контроля, определяются Правительством Российской Федерации.

Статья 10.2. Утратила силу. – Федеральный закон от 29.07.2017 № 276-ФЗ.

Статья 10.3. Обязанности оператора поисковой системы

(введена Федеральным законом от 13.07.2015 № 264-ФЗ)

1. Оператор поисковой системы, распространяющий в сети «Интернет» рекламу, которая направлена на привлечение внимания потребителей, находящихся на территории Российской Федерации, по требованию гражданина (физического лица) (далее в настоящей статье – заявитель) обязан прекратить выдачу сведений об указателе страницы сайта в сети «Интернет» (далее также – ссылка), позволяющих получить доступ к информации о заявителе, распространяемой с нарушением законодательства Российской Федерации, являющейся недостоверной, а также неактуальной, утратившей значение для заявителя в силу последующих событий или действий заявителя, за исключением информации о событиях, содержащих признаки уголовно наказуемых деяний, сроки привлечения к уголовной ответственности по которым не истекли, и информации о совершении гражданином преступления, по которому не снята или не погашена судимость.

2. Требование заявителя должно содержать:

1) фамилию, имя, отчество, паспортные данные, контактную информацию (номера телефона и (или) факса, адрес электронной почты, почтовый адрес);

2) информацию о заявителе, указанную в части 1 настоящей статьи, выдача ссылок на которую подлежит прекращению;

3) указатель страницы сайта в сети «Интернет», на которой размещена информация, указанная в части 1 настоящей статьи;

4) основание для прекращения выдачи ссылок поисковой системой;

5) согласие заявителя на обработку его персональных данных.

3. В случае обнаружения неполноты сведений, неточностей или ошибок в требовании заявителя оператор поисковой системы вправе направить заявителю в течение десяти рабочих дней с момента получения указанного требования уведомление об уточнении представленных сведений. Оператор поисковой системы также вправе направить заявителю уведомление о необходимости предоставления документа, удостоверяющего личность. Указанное уведомление может быть направлено заявителю однократно.

4. В течение десяти рабочих дней с момента получения уведомления, указанного в части 3 настоящей статьи, заявитель принимает меры, направленные на восполнение недостающих сведений, устранение неточностей и ошибок, и направляет оператору поисковой системы уточненные сведения, а также документ, удостоверяющий личность (в случае необходимости).

5. В течение десяти рабочих дней с момента получения требования заявителя или уточненных заявителем сведений (в случае направления заявителю уведомления, указанного в части 3 настоящей статьи) оператор поисковой системы обязан прекратить выдачу ссылок на информацию, указанную в требовании заявителя, при показе результатов поиска по запросам пользователей поисковой системы, содержащих имя и (или) фамилию заявителя, уведомить об этом заявителя или направить заявителю мотивированный отказ.

6. Оператор поисковой системы направляет заявителю уведомление об удовлетворении указанного в части 1 настоящей статьи требования заявителя или мотивированный отказ в его удовлетворении в той же форме, в которой было получено указанное требование.

7. Заявитель, считающий отказ оператора поисковой системы необоснованным, вправе обратиться в суд с исковым заявлением о прекращении выдачи ссылок на информацию, указанную в требовании заявителя.

8. Оператор поисковой системы обязан не раскрывать информацию о факте обращения к нему заявителя с требованием, указанным в части 1 настоящей статьи, за исключением случаев, установленных федеральными законами.

Статья 10.4. Особенности распространения информации новостным агрегатором

(введена Федеральным законом от 23.06.2016 № 208-ФЗ)

1. Владелец программы для электронных вычислительных машин, владелец сайта и (или) страницы сайта в сети «Интернет», которые используются для обработки и распространения новостной информации в сети «Интернет» на государственном языке Российской Федерации, государственных языках республик в составе Российской Федерации или иных языках народов Российской Федерации, на которых может распространяться реклама, направленная на привлечение внимания потребителей, находящихся на территории Российской Федерации, и доступ к которым в течение суток составляет более одного миллиона пользователей сети «Интернет» (далее – владелец новостного агрегатора), обязаны соблюдать требования законодательства Российской Федерации, в частности:

1) не допускать использование программы для электронных вычислительных машин, сайта и (или) страницы сайта в сети «Интернет», которые

используются для обработки и распространения новостной информации в сети «Интернет» на государственном языке Российской Федерации, государственных языках республик в составе Российской Федерации или иных языках народов Российской Федерации, на которых может распространяться реклама, направленная на привлечение внимания потребителей, находящихся на территории Российской Федерации, и доступ к которым в течение суток составляет более одного миллиона пользователей сети «Интернет» (далее – новостной агрегатор), в целях совершения уголовно наказуемых деяний, разглашения сведений, составляющих государственную или иную специально охраняемую законом тайну, распространения материалов, содержащих публичные призывы к осуществлению террористической деятельности или публично оправдывающих терроризм, других экстремистских материалов, а также материалов, пропагандирующих порнографию, культ насилия и жестокости, и материалов, содержащих нецензурную брань;

2) проверять достоверность распространяемых общественно значимых сведений до их распространения и незамедлительно прекратить их распространение на основании предписания, указанного в части 9 настоящей статьи;

3) не допускать использование новостного агрегатора в целях сокрытия или фальсификации общественно значимых сведений, распространения недостоверной общественно значимой новостной информации под видом достоверных сообщений, а также распространения информации с нарушением законодательства Российской Федерации;

4) не допускать распространение новостной информации с целью опорочить гражданина или отдельные категории граждан по признакам пола, возраста, расовой или национальной принадлежности, языка, отношения к религии, профессии, места жительства и работы, а также в связи с их политическими убеждениями;

5) не допускать распространение новостной информации о частной жизни гражданина с нарушением гражданского законодательства;

6) соблюдать запреты и ограничения, предусмотренные законодательством Российской Федерации о референдуме и законодательством Российской Федерации о выборах;

7) соблюдать требования законодательства Российской Федерации, регулирующие порядок распространения массовой информации;

8) соблюдать права и законные интересы граждан и организаций, в том числе честь, достоинство и деловую репутацию граждан, деловую репутацию организаций;

9) разместить на новостном агрегаторе адреса электронной почты для направления им юридически значимых сообщений, а также свои фамилию и инициалы (для физического лица) или наименование (для юридического лица);

10) хранить в течение шести месяцев распространенную ими новостную информацию, сведения об источнике ее получения, а также сведения о сроках ее распространения;

11) обеспечить доступ федерального органа исполнительной власти, осуществляющего функции по контролю и надзору в сфере средств массовой информации, массовых коммуникаций, информационных технологий и связи, к информации, указанной в пункте 10 настоящей части, посредством системы взаимодействия указанного федерального органа исполнительной власти с владельцем новостного агрегатора, порядок функционирования которой устанавливается указанным федеральным органом исполнительной власти;

12) установить одну из предлагаемых федеральным органом исполнительной власти, осуществляющим функции по контролю и надзору в сфере средств массовой информации, массовых коммуникаций, информационных технологий и связи, предназначенных для определения количества пользователей информационным ресурсом в сети «Интернет» программ для электронных вычислительных машин.

(п. 12 введен Федеральным законом от 01.05.2017 № 87-ФЗ)

2. Владелец новостного агрегатора не несет ответственность за распространение им новостной информации в случае, если она является дословным воспроизведением сообщений и материалов или их фрагментов, размещенных на официальном сайте государственного органа в сети «Интернет» или распространенных средством массовой информации, которое может быть установлено и привлечено к ответственности за нарушение законодательства Российской Федерации о средствах массовой информации.

(в ред. Федерального закона от 25.11.2017 № 327-ФЗ)

3. Федеральный орган исполнительной власти, осуществляющий функции по контролю и надзору в сфере средств массовой информации, массовых коммуникаций, информационных технологий и связи, ведет реестр новостных агрегаторов. В целях обеспечения формирования реестра новостных агрегаторов федеральный орган исполнительной власти, осуществляющий функции по контролю и надзору в сфере средств массовой информации, массовых коммуникаций, информационных технологий и связи:

1) организует мониторинг информационных ресурсов;

2) утверждает методику определения количества пользователей информационных ресурсов в сутки;

3) вправе запрашивать у владельца новостного агрегатора и иных лиц информацию, необходимую для ведения такого реестра. Указанные лица обязаны предоставлять запрашиваемую информацию не позднее чем в течение десяти дней со дня получения запроса федерального органа исполнительной власти, осуществляющего функции по контролю и надзору в сфере средств массовой информации, массовых коммуникаций, информационных технологий и связи.

4. В случае обнаружения в информационно-телекоммуникационных сетях, в том числе в сети «Интернет», информационного ресурса, на котором происходит обработка и распространение новостной информации в сети «Интернет» на государственном языке Российской Федерации, государственных языках республик в составе Российской Федерации или иных языках народов Российской Федерации, на котором может распространяться реклама, направленная на привлечение внимания потребителей, находящихся на территории Российской Федерации, и доступ к которому в течение суток составляет более одного миллиона пользователей сети «Интернет», включая рассмотрение соответствующих обращений органов государственной власти, органов местного самоуправления, граждан или организаций, федеральный орган исполнительной власти, осуществляющий функции по контролю и надзору в сфере средств массовой информации, массовых коммуникаций, информационных технологий и связи:

1) признает информационный ресурс новостным агрегатором и включает его в реестр новостных агрегаторов;

2) определяет провайдера хостинга или иное обеспечивающее размещение новостного агрегатора в сети «Интернет» лицо;

3) направляет провайдеру хостинга или указанному в пункте 2 настоящей части лицу уведомление в электронном виде на русском и английском языках

о необходимости предоставления данных, позволяющих идентифицировать владельца новостного агрегатора;

4) фиксирует дату и время направления указанного в пункте 3 настоящей части уведомления провайдеру хостинга или указанному в пункте 2 настоящей части лицу в соответствующей информационной системе.

5. В течение трех рабочих дней с момента получения уведомления, указанного в пункте 3 части 4 настоящей статьи, провайдер хостинга или указанное в пункте 2 части 4 настоящей статьи лицо обязаны предоставить данные, позволяющие идентифицировать владельца новостного агрегатора.

6. После получения данных, указанных в пункте 3 части 4 настоящей статьи, федеральный орган исполнительной власти, осуществляющий функции по контролю и надзору в сфере средств массовой информации, массовых коммуникаций, информационных технологий и связи, направляет владельцу новостного агрегатора уведомление о включении его информационного ресурса в реестр новостных агрегаторов с указанием требований законодательства Российской Федерации, применимых к данным информационным ресурсам.

7. В случае, если доступ к новостному агрегатору на протяжении трех месяцев составляет в течение суток менее одного миллиона пользователей сети «Интернет», данный новостной агрегатор по заявлению его владельца исключается из реестра новостных агрегаторов, о чем владельцу новостного агрегатора направляется соответствующее уведомление. Данный новостной агрегатор может быть исключен из реестра новостных агрегаторов при отсутствии заявления его владельца, если доступ к данному новостному агрегатору на протяжении шести месяцев составляет в течение суток менее одного миллиона пользователей сети «Интернет».

8. В случае обнаружения на новостном агрегаторе фактов фальсификации общественно значимых сведений, распространения недостоверной общественно значимой новостной информации под видом достоверных сообщений, а также распространения новостной информации с нарушением законодательства Российской Федерации уполномоченные государственные органы вправе обратиться в федеральный орган исполнительной власти, осуществляющий функции по контролю и надзору в сфере средств массовой информации, массовых коммуникаций, информационных технологий и связи, посредством заполнения электронной формы на официальном сайте федерального органа исполнительной власти, осуществляющего функции по контролю и надзору в сфере средств массовой информации, массовых коммуникаций, информационных технологий и связи, с приложением решения суда или решения указанного государственного органа с требованием принять меры по прекращению распространения такой информации. Форма и порядок направления данного требования и прилагаемых к нему документов определяются федеральным органом исполнительной власти, осуществляющим функции по контролю и надзору в сфере средств массовой информации, массовых коммуникаций, информационных технологий и связи.

9. В случае получения требования, указанного в части 8 настоящей статьи, и прилагаемых к нему документов федеральный орган исполнительной власти, осуществляющий функции по контролю и надзору в сфере средств массовой информации, массовых коммуникаций, информационных технологий и связи, в течение 24 часов с момента их получения рассматривает их и направляет владельцу новостного агрегатора предписание, в том числе посредством системы взаимодействия, указанной в пункте 11 части 1 настоящей статьи, о незамед-

лительном прекращении распространения информации, указанной в части 8 настоящей статьи.

10. Для целей настоящей статьи под новостной информацией понимается общедоступная информация, полученная из средств массовой информации, зарегистрированных в соответствии с Законом Российской Федерации от 27 декабря 1991 года № 2124-1 «О средствах массовой информации», а также иных источников.

11. Информационные ресурсы, которые зарегистрированы в соответствии с Законом Российской Федерации от 27 декабря 1991 года № 2124-1 «О средствах массовой информации» в качестве сетевых изданий, не являются новостными агрегаторами.

12. Владельцем новостного агрегатора может быть только российское юридическое лицо или гражданин Российской Федерации.

13. Нарушение владельцем новостного агрегатора требований настоящей статьи влечет за собой уголовную, административную или иную ответственность в соответствии с законодательством Российской Федерации.

Статья 10.5. Обязанности владельца аудиовизуального сервиса

(введена Федеральным законом от 01.05.2017 № 87-ФЗ)

1. Владелец сайта и (или) страницы сайта в сети «Интернет», и (или) информационной системы, и (или) программы для электронных вычислительных машин, которые используются для формирования и (или) организации распространения в сети «Интернет» совокупности аудиовизуальных произведений, доступ к которым предоставляется за плату и (или) при условии просмотра рекламы, направленной на привлечение внимания потребителей, находящихся на территории Российской Федерации, и доступ к которым в течение суток составляет более ста тысяч пользователей сети «Интернет», находящихся на территории Российской Федерации (далее – владелец аудиовизуального сервиса), обязан соблюдать требования законодательства Российской Федерации, в частности:

1) не допускать использование сайта и (или) страницы сайта в сети «Интернет», и (или) информационной системы, и (или) программы для электронных вычислительных машин, которые используются для формирования и (или) организации распространения в сети «Интернет» совокупности аудиовизуальных произведений, доступ к которым предоставляется за плату и (или) при условии просмотра рекламы, направленной на привлечение внимания потребителей, находящихся на территории Российской Федерации, и доступ к которым в течение суток составляет более ста тысяч пользователей сети «Интернет», находящихся на территории Российской Федерации (далее – аудиовизуальный сервис), в целях совершения уголовно наказуемых деяний, разглашения сведений, составляющих государственную или иную специально охраняемую законом тайну, распространения материалов, содержащих публичные призывы к осуществлению террористической деятельности или публично оправдывающих терроризм, других экстремистских материалов, а также материалов, пропагандирующих порнографию, культ насилия и жестокости, и материалов, содержащих нецензурную брань;

2) осуществлять в соответствии с требованиями Федерального закона от 29 декабря 2010 года № 436-ФЗ «О защите детей от информации, причиняющей вред их здоровью и развитию» классификацию аудиовизуальных произведений до начала их распространения в случае, если классификация

соответствующего аудиовизуального произведения не была осуществлена ранее его производителем или распространителем, а также обеспечивать обозначение категории данного аудиовизуального произведения соответствующим знаком информационной продукции и (или) текстовым предупреждением об ограничении распространения среди детей информационной продукции, причиняющей вред их здоровью и (или) развитию, за исключением аудиовизуальных произведений, размещаемых на таком аудиовизуальном сервисе его пользователями;

3) соблюдать запреты и ограничения, предусмотренные законодательством Российской Федерации о референдуме и законодательством Российской Федерации о выборах;

4) соблюдать требования законодательства Российской Федерации, регулирующие порядок распространения массовой информации;

5) не допускать распространения аудиовизуальным сервисом телеканалов или телепрограмм, не зарегистрированных в соответствии с Законом Российской Федерации от 27 декабря 1991 года № 2124-1 «О средствах массовой информации»;

6) разместить на аудиовизуальном сервисе адрес электронной почты для направления ему юридически значимых сообщений, а также свои фамилию и инициалы (для физического лица) или наименование (для юридического лица);

7) установить одну из предлагаемых федеральным органом исполнительной власти, осуществляющим функции по контролю и надзору в сфере средств массовой информации, массовых коммуникаций, информационных технологий и связи, предназначенных для определения количества пользователей информационным ресурсом в сети «Интернет» программ для электронных вычислительных машин.

2. Федеральный орган исполнительной власти, осуществляющий функции по контролю и надзору в сфере средств массовой информации, массовых коммуникаций, информационных технологий и связи, ведет реестр аудиовизуальных сервисов. В целях обеспечения формирования реестра аудиовизуальных сервисов федеральный орган исполнительной власти, осуществляющий функции по контролю и надзору в сфере средств массовой информации, массовых коммуникаций, информационных технологий и связи:

1) организует мониторинг информационных ресурсов;

2) утверждает методику определения количества пользователей информационных ресурсов в сутки;

3) вправе запрашивать у владельца аудиовизуального сервиса и иных лиц информацию, необходимую для ведения такого реестра. Указанные лица обязаны предоставлять запрашиваемую информацию не позднее чем в течение десяти дней со дня получения запроса федерального органа исполнительной власти, осуществляющего функции по контролю и надзору в сфере средств массовой информации, массовых коммуникаций, информационных технологий и связи.

3. В случае обнаружения в сети «Интернет» информационного ресурса, который используется для формирования и (или) организации распространения в сети «Интернет» совокупности аудиовизуальных произведений, доступ к которым предоставляется за плату и (или) при условии просмотра рекламы, направленной на привлечение внимания потребителей, находящихся на территории Российской Федерации, и доступ к которым в течение суток составляет

более ста тысяч пользователей сети «Интернет», находящихся на территории Российской Федерации, включая рассмотрение соответствующих обращений органов государственной власти, органов местного самоуправления, граждан или организаций, федеральный орган исполнительной власти, осуществляющий функции по контролю и надзору в сфере средств массовой информации, массовых коммуникаций, информационных технологий и связи:

1) признает информационный ресурс аудиовизуальным сервисом и включает его в реестр аудиовизуальных сервисов;

2) определяет провайдера хостинга или иное обеспечивающее размещение аудиовизуального сервиса в сети «Интернет» лицо;

3) направляет провайдеру хостинга или указанному в пункте 2 настоящей части лицу уведомление в электронном виде на русском и английском языках о необходимости предоставления данных, позволяющих идентифицировать владельца аудиовизуального сервиса;

4) фиксирует дату и время направления указанного в пункте 3 настоящей части уведомления провайдеру хостинга или указанному в пункте 2 настоящей части лицу в соответствующей информационной системе.

4. В течение трех рабочих дней с момента получения уведомления, указанного в пункте 3 части 3 настоящей статьи, провайдер хостинга или указанное в пункте 2 части 3 настоящей статьи лицо обязаны предоставить данные, позволяющие идентифицировать владельца аудиовизуального сервиса.

5. После получения данных, указанных в пункте 3 части 3 настоящей статьи, федеральный орган исполнительной власти, осуществляющий функции по контролю и надзору в сфере средств массовой информации, массовых коммуникаций, информационных технологий и связи, направляет владельцу аудиовизуального сервиса уведомление о включении его информационного ресурса в реестр аудиовизуальных сервисов с указанием требований законодательства Российской Федерации, применимых к данным информационным ресурсам.

6. Владелец аудиовизуального сервиса, получивший указанное в части 5 настоящей статьи уведомление, обязан в течение двух месяцев со дня его получения предоставить в федеральный орган исполнительной власти, осуществляющий функции по контролю и надзору в сфере средств массовой информации, массовых коммуникаций, информационных технологий и связи, документы, свидетельствующие о соблюдении требований части 7 настоящей статьи.

7. Владельцем аудиовизуального сервиса может выступать российское юридическое лицо или гражданин Российской Федерации, не имеющий гражданства другого государства. Если иное не предусмотрено международным договором Российской Федерации, иностранное государство, международная организация, а также находящаяся под их контролем организация, иностранное юридическое лицо, российское юридическое лицо, доля иностранного участия в уставном капитале которого составляет более двадцати процентов, иностранный гражданин, лицо без гражданства, гражданин Российской Федерации, имеющий гражданство другого государства, их аффилированные лица, в совокупности или каждый в отдельности владеющие информационным ресурсом, который используется для распространения в сети «Интернет» совокупности аудиовизуальных произведений и количество пользователей которого на территории Российской Федерации составляет менее пятидесяти процентов от общего количества пользователей

такого информационного ресурса, вправе осуществлять владение, управление либо контроль прямо или косвенно в отношении более чем двадцати процентов долей (акций) в уставном капитале владельца аудиовизуального сервиса при условии согласования указанных владения, управления либо контроля с правительственной комиссией.

8. Правительственная комиссия принимает решение о согласовании владения, управления либо контроля, указанных в части 7 настоящей статьи, при условии, что такие владение, управление либо контроль в отношении владельца аудиовизуального сервиса будут способствовать развитию рынка аудиовизуальных сервисов в Российской Федерации.

9. Положение о правительственной комиссии, ее состав и порядок принятия ею решений утверждаются Правительством Российской Федерации.

10. Положения части 7 настоящей статьи не распространяются на хозяйственные общества, имеющие стратегическое значение для обеспечения обороны страны и безопасности государства и осуществляющие деятельность, указанную в пунктах 11-14, 34, 37 статьи 6 Федерального закона от 29 апреля 2008 года № 57-ФЗ «О порядке осуществления иностранных инвестиций в хозяйственные общества, имеющие стратегическое значение для обеспечения обороны страны и безопасности государства», и (или) лиц, входящих с такими хозяйственными обществами в одну группу лиц, в части соблюдения требований об ограничении владения, управления либо контроля в отношении владельца аудиовизуального сервиса.

11. Перечень документов, свидетельствующих о соблюдении владельцем аудиовизуального сервиса требований части 7 настоящей статьи, а также форма и порядок направления в федеральный орган исполнительной власти, осуществляющий функции по контролю и надзору в сфере средств массовой информации, массовых коммуникаций, информационных технологий и связи, таких документов утверждаются Правительством Российской Федерации.

12. В случае, если доступ к аудиовизуальному сервису на протяжении трех месяцев составляет в течение суток менее ста тысяч пользователей сети «Интернет», данный аудиовизуальный сервис по заявлению его владельца исключается из реестра аудиовизуальных сервисов, о чем владельцу аудиовизуального сервиса направляется соответствующее уведомление. Данный аудиовизуальный сервис может быть исключен из реестра аудиовизуальных сервисов при отсутствии заявления его владельца, если доступ к данному аудиовизуальному сервису на протяжении шести месяцев составляет в течение суток менее ста тысяч пользователей сети «Интернет».

13. В случае обнаружения на аудиовизуальном сервисе информации, распространяемой с нарушением законодательства Российской Федерации, федеральный орган исполнительной власти, осуществляющий функции по контролю и надзору в сфере средств массовой информации, массовых коммуникаций, информационных технологий и связи, направляет владельцу аудиовизуального сервиса требование принять меры по устранению выявленных нарушений законодательства Российской Федерации.

14. Федеральный орган исполнительной власти, осуществляющий функции по контролю и надзору в сфере средств массовой информации, массовых коммуникаций, информационных технологий и связи, обращается в суд с заявлением об ограничении доступа к аудиовизуальному сервису в случае:

1) установленного вступившим в законную силу постановлением по делу об административном правонарушении повторного в течение года неисполне-

ния владельцем аудиовизуального сервиса требования принять меры по устранению выявленных нарушений законодательства Российской Федерации;

2) неисполнения владельцем аудиовизуального сервиса требований, предусмотренных частями 6 и 7 настоящей статьи.

15. На основании вступившего в законную силу решения суда до исполнения владельцем аудиовизуального сервиса требований, предусмотренных частями 6 и 7 настоящей статьи, доступ к аудиовизуальному сервису ограничивается оператором связи, оказывающим услуги по предоставлению доступа к сети «Интернет». Порядок взаимодействия федерального органа исполнительной власти, осуществляющего функции по контролю и надзору в сфере средств массовой информации, массовых коммуникаций, информационных технологий и связи, с оператором связи, владельцем аудиовизуального сервиса, а также порядок ограничения и возобновления доступа к аудиовизуальному сервису и порядок информирования о таком ограничении устанавливаются Правительством Российской Федерации.

16. Не являются аудиовизуальными сервисами:

1) информационные ресурсы, которые зарегистрированы в соответствии с Законом Российской Федерации от 27 декабря 1991 года № 2124-1 «О средствах массовой информации» в качестве сетевых изданий;

2) поисковые системы;

3) информационные ресурсы, на которых аудиовизуальные произведения размещаются преимущественно пользователями сети «Интернет». Порядок и критерии определения таких информационных ресурсов утверждаются федеральным органом исполнительной власти, осуществляющим функции по контролю и надзору в сфере средств массовой информации, массовых коммуникаций, информационных технологий и связи.

17. Нарушение владельцем аудиовизуального сервиса требований настоящей статьи влечет за собой уголовную, административную или иную ответственность в соответствии с законодательством Российской Федерации.

Статья 11. Документирование информации

1. Законодательством Российской Федерации или соглашением сторон могут быть установлены требования к документированию информации.

2. В государственных органах, органах местного самоуправления документирование информации осуществляется в соответствии с правилами делопроизводства, установленными уполномоченным федеральным органом исполнительной власти в сфере архивного дела и делопроизводства.

(часть 2 в ред. Федерального закона от 18.06.2017 № 127-ФЗ)

3. Утратил силу. – Федеральный закон от 06.04.2011 № 65-ФЗ.

4. В целях заключения гражданско-правовых договоров или оформления иных правоотношений, в которых участвуют лица, обменивающиеся электронными сообщениями, обмен электронными сообщениями, каждое из которых подписано электронной подписью или иным аналогом собственноручной подписи отправителя такого сообщения, в порядке, установленном федеральными законами, иными нормативными правовыми актами или соглашением сторон, рассматривается как обмен документами.

(в ред. Федерального закона от 06.04.2011 № 65-ФЗ)

5. Право собственности и иные вещные права на материальные носители, содержащие документированную информацию, устанавливаются гражданским законодательством.

Статья 11.1. Обмен информацией в форме электронных документов при осуществлении полномочий органов государственной власти и органов местного самоуправления

(введена Федеральным законом от 13.07.2015 № 263-ФЗ)

1. Органы государственной власти, органы местного самоуправления, а также организации, осуществляющие в соответствии с федеральными законами отдельные публичные полномочия, в пределах своих полномочий обязаны предоставлять по выбору граждан (физических лиц) и организаций информацию в форме электронных документов, подписанных усиленной квалифицированной электронной подписью, и (или) документов на бумажном носителе, за исключением случаев, если иной порядок предоставления такой информации установлен федеральными законами или иными нормативными правовыми актами Российской Федерации, регулирующими правоотношения в установленной сфере деятельности.

2. Информация, необходимая для осуществления полномочий органов государственной власти и органов местного самоуправления, организаций, осуществляющих в соответствии с федеральными законами отдельные публичные полномочия, может быть представлена гражданами (физическими лицами) и организациями в органы государственной власти, органы местного самоуправления, в организации, осуществляющие в соответствии с федеральными законами отдельные публичные полномочия, в форме электронных документов, подписанных электронной подписью, если иное не установлено федеральными законами, регулирующими правоотношения в установленной сфере деятельности.

3. Требования к осуществлению взаимодействия в электронной форме граждан (физических лиц) и организаций с органами государственной власти, органами местного самоуправления, с организациями, осуществляющими в соответствии с федеральными законами отдельные публичные полномочия, и порядок такого взаимодействия устанавливаются Правительством Российской Федерации в соответствии с Федеральным законом от 6 апреля 2011 года № 63-ФЗ «Об электронной подписи».

Статья 12. Государственное регулирование в сфере применения информационных технологий

1. Государственное регулирование в сфере применения информационных технологий предусматривает:

1) регулирование отношений, связанных с поиском, получением, передачей, производством и распространением информации с применением информационных технологий (информатизации), на основании принципов, установленных настоящим Федеральным законом;

2) развитие информационных систем различного назначения для обеспечения граждан (физических лиц), организаций, государственных органов и органов местного самоуправления информацией, а также обеспечение взаимодействия таких систем;

3) создание условий для эффективного использования в Российской Федерации информационно-телекоммуникационных сетей, в том числе сети «Интернет» и иных подобных информационно-телекоммуникационных сетей;

4) обеспечение информационной безопасности детей.

(п. 4 введен Федеральным законом от 21.07.2011 № 252-ФЗ)

2. Государственные органы, органы местного самоуправления в соответствии со своими полномочиями:

1) участвуют в разработке и реализации целевых программ применения информационных технологий;

2) создают информационные системы и обеспечивают доступ к содержащейся в них информации на русском языке и государственном языке соответствующей республики в составе Российской Федерации.

Статья 12.1. Особенности государственного регулирования в сфере использования российских программ для электронных вычислительных машин и баз данных

(введена Федеральным законом от 29.06.2015 № 188-ФЗ)

1. В целях расширения использования российских программ для электронных вычислительных машин и баз данных, подтверждения их происхождения из Российской Федерации, а также в целях оказания правообладателям программ для электронных вычислительных машин или баз данных мер государственной поддержки создается единый реестр российских программ для электронных вычислительных машин и баз данных (далее – реестр российского программного обеспечения).

2. Правила формирования и ведения реестра российского программного обеспечения, состав сведений, включаемых в реестр российского программного обеспечения, в том числе об основаниях возникновения исключительного права у правообладателя (правообладателей), условия включения таких сведений в реестр российского программного обеспечения и исключения их из реестра российского программного обеспечения, порядок предоставления сведений, включаемых в реестр российского программного обеспечения, порядок принятия решения о включении таких сведений в реестр российского программного обеспечения устанавливаются Правительством Российской Федерации.

3. Уполномоченный Правительством Российской Федерации федеральный орган исполнительной власти в порядке и в соответствии с критериями, которые определяются Правительством Российской Федерации, может привлечь к формированию и ведению реестра российского программного обеспечения оператора реестра российского программного обеспечения – организацию, зарегистрированную на территории Российской Федерации.

4. Уполномоченный Правительством Российской Федерации федеральный орган исполнительной власти утверждает классификатор программ для электронных вычислительных машин и баз данных в целях ведения реестра российского программного обеспечения.

5. В реестр российского программного обеспечения включаются сведения о программах для электронных вычислительных машин и базах данных, которые соответствуют следующим требованиям:

1) исключительное право на программу для электронных вычислительных машин или базу данных на территории всего мира и на весь срок действия исключительного права принадлежит одному либо нескольким из следующих лиц (правообладателей):

а) Российской Федерации, субъекту Российской Федерации, муниципальному образованию;

б) российской некоммерческой организации, высший орган управления которой формируется прямо и (или) косвенно Российской Федерацией, субъектами Российской Федерации, муниципальными образованиями и (или) гражданами Российской Федерации и решения которой иностранное лицо не име-

ет возможности определять в силу особенностей отношений между таким иностранным лицом и российской некоммерческой организацией;

в) российской коммерческой организации, в которой суммарная доля прямого и (или) косвенного участия Российской Федерации, субъектов Российской Федерации, муниципальных образований, российских некоммерческих организаций, указанных в подпункте «б» настоящего пункта, граждан Российской Федерации составляет более пятидесяти процентов;

г) гражданину Российской Федерации;

2) программа для электронных вычислительных машин или база данных правомерно введена в гражданский оборот на территории Российской Федерации, экземпляры программы для электронных вычислительных машин или базы данных либо права использования программы для электронных вычислительных машин или базы данных свободно реализуются на всей территории Российской Федерации;

3) общая сумма выплат по лицензионным и иным договорам, предусматривающим предоставление прав на результаты интеллектуальной деятельности и средства индивидуализации, выполнение работ, оказание услуг в связи с разработкой, адаптацией и модификацией программы для электронных вычислительных машин или базы данных и для разработки, адаптации и модификации программы для электронных вычислительных машин или базы данных, в пользу иностранных юридических лиц и (или) физических лиц, контролируемых ими российских коммерческих организаций и (или) российских некоммерческих организаций, агентов, представителей иностранных лиц и контролируемых ими российских коммерческих организаций и (или) российских некоммерческих организаций составляет менее тридцати процентов от выручки правообладателя (правообладателей) программы для электронных вычислительных машин или базы данных от реализации программы для электронных вычислительных машин или базы данных, включая предоставление прав использования, независимо от вида договора за календарный год;

4) сведения о программе для электронных вычислительных машин или базе данных не составляют государственную тайну, и программа для электронных вычислительных машин или база данных не содержит сведений, составляющих государственную тайну.

6. Правительством Российской Федерации могут быть установлены дополнительные требования к программам для электронных вычислительных машин и базам данных, сведения о которых включены в реестр российского программного обеспечения.

7. Программы для электронных вычислительных машин и базы данных, сведения о которых включены в реестр российского программного обеспечения, признаются происходящими из Российской Федерации.

8. Для целей настоящей статьи доля участия одной организации в другой организации или гражданина Российской Федерации в организации определяется в соответствии с порядком, установленным главой 14.1 Налогового кодекса Российской Федерации.

9. Для целей настоящей статьи контролируемой иностранным лицом российской коммерческой организацией или российской некоммерческой организацией признается организация, решения которой иностранное лицо имеет возможность определять в силу преобладающего прямого и (или) косвенного участия в этой организации, участия в договоре (соглашении), предметом

которого является управление этой организацией, или иных особенностей отношений между иностранным лицом и этой организацией и (или) иными лицами.

10. Решение об отказе во включении в реестр российского программного обеспечения программ для электронных вычислительных машин или баз данных может быть обжаловано правообладателем программы для электронных вычислительных машин или базы данных в суд в течение трех месяцев со дня получения такого решения.

Статья 13. Информационные системы

1. Информационные системы включают в себя:

1) государственные информационные системы – федеральные информационные системы и региональные информационные системы, созданные на основании соответственно федеральных законов, законов субъектов Российской Федерации, на основании правовых актов государственных органов;

2) муниципальные информационные системы, созданные на основании решения органа местного самоуправления;

3) иные информационные системы.

2. Если иное не установлено федеральными законами, оператором информационной системы является собственник используемых для обработки содержащейся в базах данных информации технических средств, который правомерно пользуется такими базами данных, или лицо, с которым этот собственник заключил договор об эксплуатации информационной системы. В случаях и в порядке, установленных федеральными законами, оператор информационной системы должен обеспечить возможность размещения информации в сети «Интернет» в форме открытых данных.

(в ред. Федерального закона от 07.06.2013 № 112-ФЗ)

2.1. Технические средства информационных систем, используемых государственными органами, органами местного самоуправления, государственными и муниципальными унитарными предприятиями или государственными и муниципальными учреждениями, должны размещаться на территории Российской Федерации.

(часть 2.1 введена Федеральным законом от 31.12.2014 № 531-ФЗ)

2.2. В случае создания или модернизации информационной системы на основании концессионного соглашения или соглашения о государственно-частном партнерстве функции оператора информационной системы в пределах, в объемах и в сроки, которые предусмотрены соответствующим соглашением, осуществляются концессионером или частным партнером соответственно.

(часть 2.2 введена Федеральным законом от 29.06.2018 № 173-ФЗ)

3. Права обладателя информации, содержащейся в базах данных информационной системы, подлежат охране независимо от авторских и иных прав на такие базы данных.

4. Установленные настоящим Федеральным законом требования к государственным информационным системам распространяются на муниципальные информационные системы, если иное не предусмотрено законодательством Российской Федерации о местном самоуправлении.

5. Особенности эксплуатации государственных информационных систем и муниципальных информационных систем могут устанавливаться в соответствии с техническими регламентами, нормативными правовыми актами государственных органов, нормативными правовыми актами органов местного

самоуправления, принимающих решения о создании таких информационных систем.

6. Порядок создания и эксплуатации информационных систем, не являющихся государственными информационными системами или муниципальными информационными системами, определяется операторами таких информационных систем в соответствии с требованиями, установленными настоящим Федеральным законом или другими федеральными законами.

7. Порядок осуществления контроля за соблюдением требований, предусмотренных частью 2.1 настоящей статьи и частью 6 статьи 14 настоящего Федерального закона, устанавливается Правительством Российской Федерации.

(часть 7 введена Федеральным законом от 31.12.2014 № 531-ФЗ)

Статья 14. Государственные информационные системы

1. Государственные информационные системы создаются в целях реализации полномочий государственных органов и обеспечения обмена информацией между этими органами, а также в иных установленных федеральными законами целях.

2. Государственные информационные системы создаются, модернизируются и эксплуатируются с учетом требований, предусмотренных законодательством Российской Федерации о контрактной системе в сфере закупок товаров, работ, услуг для обеспечения государственных и муниципальных нужд либо законодательством Российской Федерации о государственно-частном партнерстве, о муниципально-частном партнерстве, законодательством о концессионных соглашениях, а в случаях, если эксплуатация государственных информационных систем осуществляется без привлечения средств бюджетов бюджетной системы Российской Федерации, в соответствии с иными федеральными законами.

(в ред. Федеральных законов от 28.12.2013 № 396-ФЗ, от 29.06.2018 № 173-ФЗ, от 19.07.2018 № 211-ФЗ)

3. Государственные информационные системы создаются и эксплуатируются на основе статистической и иной документированной информации, предоставляемой гражданами (физическими лицами), организациями, государственными органами, органами местного самоуправления.

4. Перечни видов информации, предоставляемой в обязательном порядке, устанавливаются федеральными законами, условия ее предоставления – Правительством Российской Федерации или соответствующими государственными органами, если иное не предусмотрено федеральными законами. В случае, если при создании или эксплуатации государственных информационных систем предполагается осуществление или осуществляется обработка общедоступной информации, предусмотренной перечнями, утверждаемыми в соответствии со статьей 14 Федерального закона от 9 февраля 2009 года № 8-ФЗ «Об обеспечении доступа к информации о деятельности государственных органов и органов местного самоуправления», государственные информационные системы должны обеспечивать размещение такой информации в сети «Интернет» в форме открытых данных.

(в ред. Федерального закона от 07.06.2013 № 112-ФЗ)

4.1. Правительство Российской Федерации определяет случаи, при которых доступ с использованием сети «Интернет» к информации, содержащейся в государственных информационных системах, предоставляется исключительно пользователям информации, прошедшим авторизацию в единой системе

идентификации и аутентификации, а также порядок использования единой системы идентификации и аутентификации.

(часть 4.1 введена Федеральным законом от 07.06.2013 № 112-ФЗ)

5. Если иное не установлено решением о создании государственной информационной системы, функции ее оператора осуществляются заказчиком, заключившим государственный контракт на создание такой информационной системы. При этом ввод государственной информационной системы в эксплуатацию осуществляется в порядке, установленном указанным заказчиком.

5.1. В случае создания или модернизации государственной информационной системы на основании концессионного соглашения или соглашения о государственно-частном партнерстве функции оператора данной системы в пределах, в объемах и в сроки, которые предусмотрены соответствующим соглашением, осуществляются концессионером или частным партнером.

(часть 5.1 введена Федеральным законом от 29.06.2018 № 173-ФЗ)

6. Правительство Российской Федерации утверждает требования к порядку создания, развития, ввода в эксплуатацию, эксплуатации и вывода из эксплуатации государственных информационных систем, дальнейшего хранения содержащейся в их базах данных информации, включающие в себя перечень, содержание и сроки реализации этапов мероприятий по созданию, развитию, вводу в эксплуатацию, эксплуатации и выводу из эксплуатации государственных информационных систем, дальнейшему хранению содержащейся в их базах данных информации.

(часть 6 в ред. Федерального закона от 31.12.2014 № 531-ФЗ)

7. Не допускается эксплуатация государственной информационной системы без надлежащего оформления прав на использование ее компонентов, являющихся объектами интеллектуальной собственности.

8. Технические средства, предназначенные для обработки информации, содержащейся в государственных информационных системах, в том числе программно-технические средства и средства защиты информации, должны соответствовать требованиям законодательства Российской Федерации о техническом регулировании.

9. Информация, содержащаяся в государственных информационных системах, а также иные имеющиеся в распоряжении государственных органов сведения и документы являются государственными информационными ресурсами. Информация, содержащаяся в государственных информационных системах, является официальной. Государственные органы, определенные в соответствии с нормативным правовым актом, регламентирующим функционирование государственной информационной системы, обязаны обеспечить достоверность и актуальность информации, содержащейся в данной информационной системе, доступ к указанной информации в случаях и в порядке, предусмотренных законодательством, а также защиту указанной информации от неправомерных доступа, уничтожения, модифицирования, блокирования, копирования, предоставления, распространения и иных неправомерных действий.

(в ред. Федерального закона от 27.07.2010 № 227-ФЗ)

Статья 14.1. Применение информационных технологий в целях идентификации граждан Российской Федерации

(введена Федеральным законом от 31.12.2017 № 482-ФЗ)

1. Государственные органы, банки и иные организации в случаях, определенных федеральными законами, после проведения идентификации при лич-

ном присутствии гражданина Российской Федерации с его согласия на безвозмездной основе размещают в электронной форме:

1) сведения, необходимые для регистрации гражданина Российской Федерации в единой системе идентификации и аутентификации, и иные сведения, если такие сведения предусмотрены федеральными законами, – в единой системе идентификации и аутентификации;

2) биометрические персональные данные гражданина Российской Федерации – в единой информационной системе персональных данных, обеспечивающей обработку, включая сбор и хранение биометрических персональных данных, их проверку и передачу информации о степени их соответствия предоставленным биометрическим персональным данным гражданина Российской Федерации (далее – единая биометрическая система).

2. Правительство Российской Федерации по согласованию с Центральным банком Российской Федерации устанавливает требования:

1) к фиксированию действий при размещении сведений, указанных в пунктах 1 и 2 части 1 настоящей статьи;

2) к проведению государственными органами и организациями, указанными в части 1 настоящей статьи, идентификации гражданина Российской Федерации, за исключением организаций, проводящих такую идентификацию в порядке, установленном Федеральным законом от 7 августа 2001 года № 115-ФЗ «О противодействии легализации (отмыванию) доходов, полученных преступным путем, и финансированию терроризма».

3. Федеральные законы, устанавливающие обязанность государственных органов и организаций по размещению сведений, указанных в пунктах 1 и 2 части 1 настоящей статьи, должны предусматривать осуществление контроля и надзора за соответствующими действиями, а также определение органа государственной власти или организации, уполномоченных на их осуществление.

4. Сведения, указанные в пунктах 1 и 2 части 1 настоящей статьи, размещаются соответственно в единой системе идентификации и аутентификации и в единой биометрической системе уполномоченным сотрудником государственного органа или организации и подписываются усиленной квалифицированной электронной подписью такого государственного органа или организации.

5. Форма согласия на обработку персональных данных и биометрических персональных данных, указанных в пунктах 1 и 2 части 1 настоящей статьи, утверждается Правительством Российской Федерации.

6. Порядок регистрации гражданина Российской Федерации в единой системе идентификации и аутентификации, включая состав сведений, необходимых для регистрации гражданина Российской Федерации в указанной системе, порядок и сроки проверки и обновления сведений, размещаемых в единой системе идентификации и аутентификации с использованием государственных информационных систем, устанавливаются Правительством Российской Федерации. Федеральные органы исполнительной власти, в том числе федеральный орган исполнительной власти, осуществляющий функции по выработке и реализации государственной политики и нормативно-правовому регулированию в сфере внутренних дел, органы государственных внебюджетных фондов направляют в единую систему идентификации и аутентификации сведения о гражданах Российской Федерации в целях их обновления в соответствии с указанным порядком.

7. В случаях, установленных федеральными законами, государственные органы и организации вправе обновлять информацию о гражданах Российской Федерации, идентифицированных в соответствии с частью 18 настоящей статьи, с использованием сведений, полученных из единой системы идентификации и аутентификации.

8. Состав сведений, размещаемых в единой биометрической системе, включая вид биометрических персональных данных, определяется Правительством Российской Федерации.

9. Обработка биометрических персональных данных в государственных органах, банках и иных организациях, указанных в абзаце первом части 1 настоящей статьи, в том числе с использованием единой биометрической системы, осуществляется в соответствии с требованиями к защите биометрических персональных данных, установленными в соответствии со статьей 19 Федерального закона от 27 июля 2006 года № 152-ФЗ «О персональных данных».

10. Контроль и надзор за выполнением организационных и технических мер по обеспечению безопасности персональных данных, установленных в соответствии со статьей 19 Федерального закона от 27 июля 2006 года № 152-ФЗ «О персональных данных», при обработке персональных данных в единой биометрической системе, за исключением контроля и надзора за выполнением банками организационных и технических мер по обеспечению безопасности персональных данных при использовании единой биометрической системы, осуществляются федеральным органом исполнительной власти, уполномоченным в области обеспечения безопасности, и федеральным органом исполнительной власти, уполномоченным в области противодействия техническим разведкам и технической защиты информации, в пределах их полномочий, установленных законодательством Российской Федерации о персональных данных.

11. Контроль и надзор за выполнением банками организационных и технических мер по обеспечению безопасности персональных данных при использовании единой биометрической системы осуществляются Центральным банком Российской Федерации.

12. Правительство Российской Федерации определяет федеральный орган исполнительной власти, осуществляющий регулирование в сфере идентификации граждан Российской Федерации на основе биометрических персональных данных.

13. Федеральный орган исполнительной власти, осуществляющий регулирование в сфере идентификации граждан Российской Федерации на основе биометрических персональных данных:

1) определяет порядок обработки, включая сбор и хранение, параметров биометрических персональных данных в целях идентификации, порядок размещения и обновления биометрических персональных данных в единой биометрической системе, а также требования к информационным технологиям и техническим средствам, предназначенным для обработки биометрических персональных данных в целях проведения идентификации (в банковской сфере и иных сферах финансового рынка указанные требования устанавливаются по согласованию с Центральным банком Российской Федерации);

2) определяет формы подтверждения соответствия информационных технологий и технических средств, предназначенных для обработки биометрических персональных данных в целях проведения идентификации, требованиям, определенным в соответствии с пунктом 1 настоящей части, и публикует пере-

чень технологий и средств, имеющих подтверждение соответствия (в банковской сфере и иных сферах финансового рынка формы подтверждения соответствия устанавливаются по согласованию с Центральным банком Российской Федерации);

3) разрабатывает и утверждает методики проверки соответствия предоставленных биометрических персональных данных физического лица его биометрическим персональным данным, содержащимся в единой биометрической системе, а также определяет степень взаимного соответствия указанных биометрических персональных данных, достаточную для проведения идентификации, предусмотренной настоящим Федеральным законом.

14. Центральный банк Российской Федерации совместно с оператором единой биометрической системы определяет перечень угроз безопасности, актуальных при обработке, включая сбор и хранение, биометрических персональных данных, их проверке и передаче информации о степени их соответствия предоставленным биометрическим персональным данным гражданина Российской Федерации в государственных органах, банках и иных организациях, указанных в абзаце первом части 1 настоящей статьи, в единой биометрической системе с учетом оценки возможного вреда, проведенной в соответствии с законодательством Российской Федерации о персональных данных, и согласовывает указанный перечень с федеральным органом исполнительной власти, уполномоченным в области обеспечения безопасности, и федеральным органом исполнительной власти, уполномоченным в области противодействия техническим разведкам и технической защиты информации.

15. Государственные органы, банки и иные организации, указанные в абзаце первом части 1 настоящей статьи, оператор единой биометрической системы при обработке, включая сбор и хранение, биометрических персональных данных, их проверке и определении степени их соответствия предоставленным биометрическим персональным данным гражданина Российской Федерации:

1) осуществляют свои функции в соответствии с законодательством Российской Федерации о персональных данных и требованиями настоящего Федерального закона;

2) осуществляют обработку, включая сбор и хранение, биометрических персональных данных с применением информационных технологий и технических средств, имеющих подтверждение соответствия требованиям, установленным в соответствии с настоящим Федеральным законом;

3) обеспечивают проверку соответствия предоставленных биометрических персональных данных гражданина Российской Федерации его биометрическим персональным данным согласно методикам, утвержденным в соответствии с настоящим Федеральным законом.

16. Оператор единой биометрической системы:

1) осуществляет передачу информации о результатах проверки соответствия предоставленных биометрических персональных данных гражданина Российской Федерации его биометрическим персональным данным, содержащимся в единой биометрической системе, в государственные органы, банки и иные организации, указанные в абзаце первом части 1 настоящей статьи;

2) предоставляет в федеральный орган исполнительной власти, осуществляющий функции по выработке и реализации государственной политики и нормативно-правовому регулированию в сфере внутренних дел, и федеральный орган исполнительной власти в области обеспечения безопасности в целях обеспечения обороны страны, безопасности государства, охраны правопорядка и про-

тиводействия терроризму сведения, содержащиеся в единой биометрической системе, в порядке, установленном Правительством Российской Федерации.

17. Функции оператора единой биометрической системы возлагаются Правительством Российской Федерации на оператора, занимающего существенное положение в сети связи общего пользования на территориях не менее чем двух третей субъектов Российской Федерации.

18. Идентификация гражданина Российской Федерации с применением информационных технологий осуществляется без его личного присутствия в случаях, установленных федеральными законами, путем предоставления государственным органам и организациям:

1) сведений о гражданине Российской Федерации, размещенных в единой системе идентификации и аутентификации, в порядке, установленном Правительством Российской Федерации;

2) информации о степени соответствия предоставленных биометрических персональных данных гражданина Российской Федерации его биометрическим персональным данным, содержащимся в единой биометрической системе.

19. При предоставлении биометрических персональных данных физического лица по каналам связи в целях проведения его идентификации без личного присутствия посредством сети «Интернет» должны применяться шифровальные (криптографические) средства, позволяющие обеспечить безопасность передаваемых данных от угроз безопасности, актуальных при обработке биометрических персональных данных, определенных в соответствии с частью 14 настоящей статьи, и имеющие подтверждение соответствия требованиям, установленным в соответствии со статьей 19 Федерального закона от 27 июля 2006 года № 152-ФЗ «О персональных данных». Государственный орган, банк или иная организация, указанные в абзаце первом части 1 настоящей статьи, обязаны предложить использовать указанные средства физическим лицам, обратившимся к ним в целях проведения идентификации без личного присутствия, и указать страницу сайта в сети «Интернет», с которой предоставляются эти средства.

20. В случае, если физическое лицо для предоставления своих биометрических персональных данных в целях проведения идентификации без личного присутствия посредством сети «Интернет» использует мобильный телефон, смартфон или планшетный компьютер и отказывается от использования шифровальных (криптографических) средств, указанных в части 19 настоящей статьи, государственный орган, банк или иная организация, указанные в абзаце первом части 1 настоящей статьи, обязаны отказать такому лицу в проведении указанной идентификации.

21. В случае, если физическое лицо при предоставлении своих биометрических персональных данных в целях проведения идентификации без личного присутствия посредством сети «Интернет» использует иные устройства, в том числе персональный компьютер, и отказывается от применения шифровальных (криптографических) средств, указанных в части 19 настоящей статьи, государственный орган, банк или иная организация, указанные в абзаце первом части 1 настоящей статьи, уведомляет его о рисках, связанных с таким отказом. После подтверждения физическим лицом своего решения государственный орган, банк или иная организация, указанные в абзаце первом части 1 настоящей статьи, может провести соответствующую идентификацию физического лица посредством сети «Интернет» без использования им указанных шифровальных (криптографических) средств.

22. Государственные органы, банки и иные организации при проведении идентификации гражданина Российской Федерации с применением информационных технологий в соответствии с частью 18 настоящей статьи вправе подтверждать достоверность сведений, предусмотренных пунктом 1 части 18 настоящей статьи, с использованием информационных систем государственных органов, в том числе федерального органа исполнительной власти, осуществляющего функции по выработке и реализации государственной политики и нормативно-правовому регулированию в сфере внутренних дел, Пенсионного фонда Российской Федерации, Федерального фонда обязательного медицинского страхования и (или) государственной информационной системы, определенной Правительством Российской Федерации.

23. Согласие гражданина Российской Федерации на обработку персональных данных, содержащихся в единой системе идентификации и аутентификации, и биометрических персональных данных для проведения его идентификации с применением информационных технологий в соответствии с частью 18 настоящей статьи может быть подписано его простой электронной подписью, ключ которой получен в соответствии с правилами использования простой электронной подписи при обращении за получением государственных и муниципальных услуг в электронной форме, установленными Правительством Российской Федерации. Указанное согласие, подписанное простой электронной подписью, признается электронным документом, равнозначным документу на бумажном носителе, подписанному собственноручной подписью данного гражданина Российской Федерации.

24. Размер и порядок взимания оператором единой биометрической системы платы за предоставление государственным органам и организациям сведений, указанных в пункте 2 части 18 настоящей статьи, определяются федеральным органом исполнительной власти, осуществляющим функции по выработке и реализации государственной политики и нормативно-правовому регулированию в сфере информационных технологий, по согласованию с оператором единой биометрической системы и иными государственными органами и организациями в случаях, установленных федеральными законами.

Статья 15. Использование информационно-телекоммуникационных сетей

1. На территории Российской Федерации использование информационно-телекоммуникационных сетей осуществляется с соблюдением требований законодательства Российской Федерации в области связи, настоящего Федерального закона и иных нормативных правовых актов Российской Федерации.

2. Регулирование использования информационно-телекоммуникационных сетей, доступ к которым не ограничен определенным кругом лиц, осуществляется в Российской Федерации с учетом общепринятой международной практики деятельности саморегулируемых организаций в этой области. Порядок использования иных информационно-телекоммуникационных сетей определяется владельцами таких сетей с учетом требований, установленных настоящим Федеральным законом.

3. Использование на территории Российской Федерации информационно-телекоммуникационных сетей в хозяйственной или иной деятельности не может служить основанием для установления дополнительных требований или ограничений, касающихся регулирования указанной деятельности, осуществляемой без использования таких сетей, а также для несоблюдения требований, установленных федеральными законами.

4. Федеральными законами может быть предусмотрена обязательная идентификация личности, организаций, использующих информационно-телекоммуникационную сеть при осуществлении предпринимательской деятельности. При этом получатель электронного сообщения, находящийся на территории Российской Федерации, вправе провести проверку, позволяющую установить отправителя электронного сообщения, а в установленных федеральными законами или соглашением сторон случаях обязан провести такую проверку.

5. Передача информации посредством использования информационно-телекоммуникационных сетей осуществляется без ограничений при условии соблюдения установленных федеральными законами требований к распространению информации и охране объектов интеллектуальной собственности. Передача информации может быть ограничена только в порядке и на условиях, которые установлены федеральными законами.

6. Особенности подключения государственных информационных систем к информационно-телекоммуникационным сетям могут быть установлены нормативным правовым актом Президента Российской Федерации или нормативным правовым актом Правительства Российской Федерации.

Статья 15.1. Единый реестр доменных имен, указателей страниц сайтов в сети «Интернет» и сетевых адресов, позволяющих идентифицировать сайты в сети «Интернет», содержащие информацию, распространение которой в Российской Федерации запрещено

(введена Федеральным законом от 28.07.2012 № 139-ФЗ)

1. В целях ограничения доступа к сайтам в сети «Интернет», содержащим информацию, распространение которой в Российской Федерации запрещено, создается единая автоматизированная информационная система «Единый реестр доменных имен, указателей страниц сайтов в сети «Интернет» и сетевых адресов, позволяющих идентифицировать сайты в сети «Интернет», содержащие информацию, распространение которой в Российской Федерации запрещено» (далее – реестр).

2. В реестр включаются:

1) доменные имена и (или) указатели страниц сайтов в сети «Интернет», содержащих информацию, распространение которой в Российской Федерации запрещено;

2) сетевые адреса, позволяющие идентифицировать сайты в сети «Интернет», содержащие информацию, распространение которой в Российской Федерации запрещено.

3. Создание, формирование и ведение реестра осуществляются федеральным органом исполнительной власти, осуществляющим функции по контролю и надзору в сфере средств массовой информации, массовых коммуникаций, информационных технологий и связи, в порядке, установленном Правительством Российской Федерации.

4. Федеральный орган исполнительной власти, осуществляющий функции по контролю и надзору в сфере средств массовой информации, массовых коммуникаций, информационных технологий и связи, в порядке и в соответствии с критериями, которые определяются Правительством Российской Федерации, может привлечь к формированию и ведению реестра оператора реестра – организацию, зарегистрированную на территории Российской Федерации.

5. Основаниями для включения в реестр сведений, указанных в части 2 настоящей статьи, являются:

1) решения уполномоченных Правительством Российской Федерации федеральных органов исполнительной власти, принятые в соответствии с их компетенцией в порядке, установленном Правительством Российской Федерации, в отношении распространяемых посредством сети «Интернет»:

а) материалов с порнографическими изображениями несовершеннолетних и (или) объявлений о привлечении несовершеннолетних в качестве исполнителей для участия в зрелищных мероприятиях порнографического характера;

б) информации о способах, методах разработки, изготовления и использования наркотических средств, психотропных веществ и их прекурсоров, новых потенциально опасных психоактивных веществ, местах их приобретения, способах и местах культивирования наркосодержащих растений;

(пп. «б» в ред. Федерального закона от 19.12.2016 № 442-ФЗ)

в) информации о способах совершения самоубийства, а также призывов к совершению самоубийства;

г) информации о несовершеннолетнем, пострадавшем в результате противоправных действий (бездействия), распространение которой запрещено федеральными законами;

(пп. «г» введен Федеральным законом от 05.04.2013 № 50-ФЗ)

д) информации, нарушающей требования Федерального закона от 29 декабря 2006 года № 244-ФЗ «О государственном регулировании деятельности по организации и проведению азартных игр и о внесении изменений в некоторые законодательные акты Российской Федерации» и Федерального закона от 11 ноября 2003 года № 138-ФЗ «О лотереях» о запрете деятельности по организации и проведению азартных игр и лотерей с использованием сети «Интернет» и иных средств связи;

(пп. «д» введен Федеральным законом от 21.07.2014 № 222-ФЗ)

е) информации, содержащей предложения о розничной продаже дистанционным способом алкогольной продукции, и (или) спиртосодержащей пищевой продукции, и (или) этилового спирта, и (или) спиртосодержащей непищевой продукции, розничная продажа которой ограничена или запрещена законодательством о государственном регулировании производства и оборота этилового спирта, алкогольной и спиртосодержащей продукции и об ограничении потребления (распития) алкогольной продукции;

(пп. «е» введен Федеральным законом от 29.07.2017 № 278-ФЗ)

ж) информации, направленной на склонение или иное вовлечение несовершеннолетних в совершение противоправных действий, представляющих угрозу для их жизни и (или) здоровья либо для жизни и (или) здоровья иных лиц;

(пп. «ж» введен Федеральным законом от 18.12.2018 № 472-ФЗ)

2) вступившее в законную силу решение суда о признании информации, распространяемой посредством сети «Интернет», информацией, распространение которой в Российской Федерации запрещено;

3) постановление судебного пристава-исполнителя об ограничении доступа к информации, распространяемой в сети «Интернет», порочащей честь, достоинство или деловую репутацию гражданина либо деловую репутацию юридического лица.

(п. 3 введен Федеральным законом от 23.04.2018 № 102-ФЗ)

6. Решение о включении в реестр доменных имен, указателей страниц сайтов в сети «Интернет» и сетевых адресов, позволяющих идентифицировать сайты в сети «Интернет», содержащие информацию, распространение

которой в Российской Федерации запрещено, может быть обжаловано владельцем сайта в сети «Интернет», провайдером хостинга, оператором связи, оказывающим услуги по предоставлению доступа к информационно-телекоммуникационной сети «Интернет», в суд в течение трех месяцев со дня принятия такого решения.

7. Незамедлительно с момента получения от оператора реестра уведомления о включении доменного имени и (или) указателя страницы сайта в сети «Интернет» в реестр провайдер хостинга обязан проинформировать об этом обслуживаемого им владельца сайта в сети «Интернет» и уведомить его о необходимости удаления интернет-страницы, содержащей информацию, распространение которой в Российской Федерации запрещено.

(в ред. Федерального закона от 18.12.2018 № 472-ФЗ)

8. Незамедлительно с момента получения от провайдера хостинга уведомления о включении доменного имени и (или) указателя страницы сайта в сети «Интернет» в реестр владелец сайта в сети «Интернет» обязан удалить интернет-страницу, содержащую информацию, распространение которой в Российской Федерации запрещено. В случае отказа или бездействия владельца сайта в сети «Интернет» провайдер хостинга обязан ограничить доступ к такому сайту в сети «Интернет» незамедлительно.

(в ред. Федерального закона от 18.12.2018 № 472-ФЗ)

9. В случае непринятия провайдером хостинга и (или) владельцем сайта в сети «Интернет» мер, указанных в частях 7 и 8 настоящей статьи, сетевой адрес, позволяющий идентифицировать сайт в сети «Интернет», содержащий информацию, распространение которой в Российской Федерации запрещено, включается в реестр.

10. В течение суток с момента включения в реестр сетевого адреса, позволяющего идентифицировать сайт в сети «Интернет», содержащий информацию, распространение которой в Российской Федерации запрещено, оператор связи, оказывающий услуги по предоставлению доступа к информационно-телекоммуникационной сети «Интернет», обязан ограничить доступ к такому сайту в сети «Интернет».

11. Федеральный орган исполнительной власти, осуществляющий функции по контролю и надзору в сфере средств массовой информации, массовых коммуникаций, информационных технологий и связи, или привлеченный им в соответствии с частью 4 настоящей статьи оператор реестра исключает из реестра доменное имя, указатель страницы сайта в сети «Интернет» или сетевой адрес, позволяющий идентифицировать сайт в сети «Интернет», на основании обращения владельца сайта в сети «Интернет», провайдера хостинга или оператора связи, оказывающего услуги по предоставлению доступа к информационно-телекоммуникационной сети «Интернет», не позднее чем в течение трех дней со дня такого обращения после принятия мер по удалению информации, распространение которой в Российской Федерации запрещено, либо на основании вступившего в законную силу решения суда об отмене решения федерального органа исполнительной власти, осуществляющего функции по контролю и надзору в сфере средств массовой информации, массовых коммуникаций, информационных технологий и связи, о включении в реестр доменного имени, указателя страницы сайта в сети «Интернет» или сетевого адреса, позволяющего идентифицировать сайт в сети «Интернет».

12. Порядок взаимодействия оператора реестра с провайдером хостинга и порядок получения доступа к содержащейся в реестре информации опера-

тором связи, оказывающим услуги по предоставлению доступа к информационно-телекоммуникационной сети «Интернет», устанавливаются уполномоченным Правительством Российской Федерации федеральным органом исполнительной власти.

13. Порядок ограничения доступа к сайтам в сети «Интернет», предусмотренный настоящей статьей, не применяется к информации, порядок ограничения доступа к которой предусмотрен статьей 15.3 настоящего Федерального закона.

(часть 13 введена Федеральным законом от 28.12.2013 № 398-ФЗ)

14. Федеральный орган исполнительной власти, осуществляющий функции по контролю и надзору в сфере средств массовой информации, массовых коммуникаций, информационных технологий и связи, или привлеченный им в соответствии с частью 4 настоящей статьи оператор реестра в течение суток с момента получения решений, указанных в подпунктах «а», «в» и «ж» пункта 1 части 5 настоящей статьи, уведомляет по системе взаимодействия об этом федеральный орган исполнительной власти в сфере внутренних дел.

(часть 14 введена Федеральным законом от 07.06.2017 № 109-ФЗ; в ред. Федерального закона от 18.12.2018 № 472-ФЗ)

Статья 15.1-1. Порядок ограничения доступа к информации, выражающей в неприличной форме, которая оскорбляет человеческое достоинство и общественную нравственность, явное неуважение к обществу, государству, официальным государственным символам Российской Федерации, Конституции Российской Федерации или органам, осуществляющим государственную власть в Российской Федерации

(введена Федеральным законом от 18.03.2019 № 30-ФЗ)

1. В случае обнаружения в информационно-телекоммуникационных сетях, в том числе в сети «Интернет», информации, выражающей в неприличной форме, которая оскорбляет человеческое достоинство и общественную нравственность, явное неуважение к обществу, государству, официальным государственным символам Российской Федерации, Конституции Российской Федерации или органам, осуществляющим государственную власть в Российской Федерации, Генеральный прокурор Российской Федерации или его заместители обращаются в федеральный орган исполнительной власти, осуществляющий функции по контролю и надзору в сфере средств массовой информации, массовых коммуникаций, информационных технологий и связи, с требованием о принятии мер по удалению указанной информации и по ограничению доступа к информационным ресурсам, распространяющим указанную информацию, в случае ее неудаления.

2. Федеральный орган исполнительной власти, осуществляющий функции по контролю и надзору в сфере средств массовой информации, массовых коммуникаций, информационных технологий и связи, на основании обращения, указанного в части 1 настоящей статьи, незамедлительно:

1) определяет провайдера хостинга или иное лицо, обеспечивающее размещение в информационно-телекоммуникационной сети, в том числе в сети «Интернет», указанного информационного ресурса, обслуживающего владельца сайта в сети «Интернет», на котором размещена информация, указанная в части 1 настоящей статьи;

2) направляет провайдеру хостинга или иному указанному в пункте 1 настоящей части лицу уведомление в электронном виде на русском и английском

языках о нарушении порядка распространения информации с указанием доменного имени и сетевого адреса, позволяющих идентифицировать сайт в сети «Интернет», на котором размещена информация, указанная в части 1 настоящей статьи, а также указателей страниц сайта в сети «Интернет», позволяющих идентифицировать такую информацию, и с требованием принять меры по удалению такой информации;

3) фиксирует дату и время направления уведомления провайдеру хостинга или иному указанному в пункте 1 настоящей части лицу в соответствующей информационной системе.

3. Незамедлительно с момента получения уведомления, указанного в пункте 2 части 2 настоящей статьи, провайдер хостинга или иное указанное в пункте 1 части 2 настоящей статьи лицо обязаны проинформировать об этом обслуживаемого ими владельца информационного ресурса и уведомить его о необходимости незамедлительно удалить информацию, указанную в части 1 настоящей статьи.

4. В течение суток с момента получения от провайдера хостинга или иного указанного в пункте 1 части 2 настоящей статьи лица уведомления о необходимости удалить информацию, указанную в части 1 настоящей статьи, владелец информационного ресурса обязан удалить такую информацию. В случае отказа или бездействия владельца информационного ресурса провайдер хостинга или иное указанное в пункте 1 части 2 настоящей статьи лицо обязаны ограничить доступ к соответствующему информационному ресурсу незамедлительно по истечении суток с момента получения уведомления, указанного в пункте 2 части 2 настоящей статьи.

5. В случае непринятия провайдером хостинга или иным указанным в пункте 1 части 2 настоящей статьи лицом и (или) владельцем информационного ресурса мер, указанных в частях 3 и 4 настоящей статьи, доменное имя сайта в сети «Интернет», его сетевой адрес, указатели страниц сайта в сети «Интернет», позволяющие идентифицировать информацию, указанную в части 1 настоящей статьи, направляются по системе взаимодействия операторам связи для принятия мер по ограничению доступа к данному информационному ресурсу, в том числе к сайту в сети «Интернет».

6. После получения по системе взаимодействия сведений, указанных в части 5 настоящей статьи, оператор связи, оказывающий услуги по предоставлению доступа к информационно-телекоммуникационной сети «Интернет», обязан незамедлительно ограничить доступ к информационному ресурсу, в том числе к сайту в сети «Интернет», на котором размещена информация, указанная в части 1 настоящей статьи.

7. В случае, если владелец информационного ресурса удалил информацию, указанную в части 1 настоящей статьи, он направляет уведомление об этом в федеральный орган исполнительной власти, осуществляющий функции по контролю и надзору в сфере средств массовой информации, массовых коммуникаций, информационных технологий и связи. Такое уведомление может быть направлено также в электронном виде.

8. После получения уведомления, указанного в части 7 настоящей статьи, и проверки его достоверности федеральный орган исполнительной власти, осуществляющий функции по контролю и надзору в сфере средств массовой информации, массовых коммуникаций, информационных технологий и связи, обязан незамедлительно уведомить по системе взаимодействия оператора связи, оказывающего услуги по предоставлению доступа к информационно-

телекоммуникационной сети «Интернет», о возобновлении доступа к информационному ресурсу, в том числе к сайту в сети «Интернет».

9. После получения уведомления, указанного в части 8 настоящей статьи, оператор связи незамедлительно возобновляет доступ к информационному ресурсу, в том числе к сайту в сети «Интернет».

Статья 15.2. Порядок ограничения доступа к информации, распространяемой с нарушением авторских и (или) смежных прав

(в ред. Федерального закона от 24.11.2014 № 364-ФЗ)

(введена Федеральным законом от 02.07.2013 № 187-ФЗ)

1. Правообладатель в случае обнаружения в информационно-телекоммуникационных сетях, в том числе в сети «Интернет», объектов авторских и (или) смежных прав (кроме фотографических произведений и произведений, полученных способами, аналогичными фотографии), распространяемых в таких сетях, или информации, необходимой для их получения с использованием информационно-телекоммуникационных сетей, которые распространяются без его разрешения или иного законного основания, вправе обратиться в федеральный орган исполнительной власти, осуществляющий функции по контролю и надзору в сфере средств массовой информации, массовых коммуникаций, информационных технологий и связи, с заявлением о принятии мер по ограничению доступа к информационным ресурсам, распространяющим такие объекты или информацию, на основании вступившего в силу судебного акта. Форма указанного заявления утверждается федеральным органом исполнительной власти, осуществляющим функции по контролю и надзору в сфере средств массовой информации, массовых коммуникаций, информационных технологий и связи.

(в ред. Федерального закона от 24.11.2014 № 364-ФЗ)

2. Федеральный орган исполнительной власти, осуществляющий функции по контролю и надзору в сфере средств массовой информации, массовых коммуникаций, информационных технологий и связи, на основании вступившего в силу судебного акта в течение трех рабочих дней:

1) определяет провайдера хостинга или иное лицо, обеспечивающее размещение в информационно-телекоммуникационной сети, в том числе в сети «Интернет», указанного информационного ресурса, обслуживающего владельца сайта в сети «Интернет», на котором размещена информация, содержащая объекты авторских и (или) смежных прав (кроме фотографических произведений и произведений, полученных способами, аналогичными фотографии), или информация, необходимая для их получения с использованием информационно-телекоммуникационных сетей, без разрешения правообладателя или иного законного основания;

(в ред. Федерального закона от 24.11.2014 № 364-ФЗ)

2) направляет провайдеру хостинга или иному указанному в пункте 1 настоящей части лицу в электронном виде уведомление на русском и английском языках о нарушении исключительных прав на объекты авторских и (или) смежных прав (кроме фотографических произведений и произведений, полученных способами, аналогичными фотографии), распространяемые в информационно-телекоммуникационных сетях, в том числе в сети «Интернет», с указанием наименования произведения, его автора, правообладателя, доменного имени и сетевого адреса, позволяющих идентифицировать сайт в сети «Интернет», на котором размещена информация, содержащая объекты авторских и (или) смежных прав (кроме фотографических произведений и произведений, полу-

ченных способами, аналогичными фотографии), или информация, необходимая для их получения с использованием информационно-телекоммуникационных сетей, без разрешения правообладателя или иного законного основания, а также указателей страниц сайта в сети «Интернет», позволяющих идентифицировать такую информацию, и с требованием принять меры по ограничению доступа к такой информации;

(в ред. Федерального закона от 24.11.2014 № 364-ФЗ)

3) фиксирует дату и время направления уведомления провайдеру хостинга или иному указанному в пункте 1 настоящей части лицу в соответствующей информационной системе.

3. В течение одного рабочего дня с момента получения уведомления, указанного в пункте 2 части 2 настоящей статьи, провайдер хостинга или иное указанное в пункте 1 части 2 настоящей статьи лицо обязаны проинформировать об этом обслуживаемого ими владельца информационного ресурса и уведомить его о необходимости незамедлительно ограничить доступ к незаконно размещенной информации.

(в ред. Федерального закона от 24.11.2014 № 364-ФЗ)

4. В течение одного рабочего дня с момента получения от провайдера хостинга или иного указанного в пункте 1 части 2 настоящей статьи лица уведомления о необходимости ограничить доступ к незаконно размещенной информации владелец информационного ресурса обязан удалить незаконно размещенную информацию или принять меры по ограничению доступа к ней. В случае отказа или бездействия владельца информационного ресурса провайдер хостинга или иное указанное в пункте 1 части 2 настоящей статьи лицо обязаны ограничить доступ к соответствующему информационному ресурсу не позднее истечения трех рабочих дней с момента получения уведомления, указанного в пункте 2 части 2 настоящей статьи.

(часть 4 в ред. Федерального закона от 24.11.2014 № 364-ФЗ)

5. В случае непринятия провайдером хостинга или иным указанным в пункте 1 части 2 настоящей статьи лицом и (или) владельцем информационного ресурса мер, указанных в частях 3 и 4 настоящей статьи, доменное имя сайта в сети «Интернет», его сетевой адрес, указатели страниц сайта в сети «Интернет», позволяющие идентифицировать информацию, содержащую объекты авторских и (или) смежных прав (кроме фотографических произведений и произведений, полученных способами, аналогичными фотографии), или информацию, необходимую для их получения с использованием информационно-телекоммуникационных сетей, и размещенную без разрешения правообладателя или иного законного основания, а также иные сведения об этом сайте и информация направляются по системе взаимодействия операторам связи для принятия мер по ограничению доступа к данному информационному ресурсу, в том числе к сайту в сети «Интернет», или к размещенной на нем информации.

(в ред. Федерального закона от 24.11.2014 № 364-ФЗ)

6. Федеральный орган исполнительной власти, осуществляющий функции по контролю и надзору в сфере средств массовой информации, массовых коммуникаций, информационных технологий и связи, на основании вступившего в силу судебного акта в течение трех рабочих дней со дня получения судебного акта об отмене ограничения доступа к информационному ресурсу, содержащему объекты авторских и (или) смежных прав (кроме фотографических произведений и произведений, полученных способами, аналогичными фотографии), распространяемые в информационно-телекоммуникационных

сетях, в том числе в сети «Интернет», или информацию, необходимую для их получения с использованием информационно-телекоммуникационных сетей, которые распространяются без разрешения правообладателя или иного законного основания, уведомляет провайдера хостинга или иное указанное в пункте 1 части 2 настоящей статьи лицо и операторов связи об отмене мер по ограничению доступа к данному информационному ресурсу. В течение одного рабочего дня со дня получения от указанного федерального органа исполнительной власти уведомления об отмене мер по ограничению доступа к информационному ресурсу провайдер хостинга обязан проинформировать об этом владельца информационного ресурса и уведомить о возможности снятия ограничения доступа.

(в ред. Федерального закона от 24.11.2014 № 364-ФЗ)

7. В течение суток с момента получения по системе взаимодействия сведений об информационном ресурсе, содержащем объекты авторских и (или) смежных прав (кроме фотографических произведений и произведений, полученных способами, аналогичными фотографии), распространяемые в информационно-телекоммуникационных сетях, в том числе в сети «Интернет», или информацию, необходимую для их получения с использованием информационно-телекоммуникационных сетей, которые используются без разрешения правообладателя или иного законного основания, оператор связи, оказывающий услуги по предоставлению доступа к информационно-телекоммуникационной сети «Интернет», обязан ограничить доступ к незаконно размещенной информации в соответствии с вступившим в законную силу судебным актом. В случае отсутствия у оператора связи технической возможности ограничить доступ к незаконно размещенной информации оператор связи обязан ограничить доступ к такому информационному ресурсу.

(часть 7 в ред. Федерального закона от 24.11.2014 № 364-ФЗ)

8. Порядок функционирования информационной системы взаимодействия устанавливается федеральным органом исполнительной власти, осуществляющим функции по контролю и надзору в сфере средств массовой информации, массовых коммуникаций, информационных технологий и связи.

9. Предусмотренный настоящей статьей порядок не применяется к информации, подлежащей включению в реестр в соответствии со статьей 15.1 настоящего Федерального закона.

Статья 15.3. Порядок ограничения доступа к информации, распространяемой с нарушением закона

(введена Федеральным законом от 28.12.2013 № 398-ФЗ)

1. В случае обнаружения в информационно-телекоммуникационных сетях, в том числе в сети «Интернет», информации, содержащей призывы к массовым беспорядкам, осуществлению экстремистской деятельности, участию в массовых (публичных) мероприятиях, проводимых с нарушением установленного порядка, недостоверной общественно значимой информации, распространяемой под видом достоверных сообщений, которая создает угрозу причинения вреда жизни и (или) здоровью граждан, имуществу, угрозу массового нарушения общественного порядка и (или) общественной безопасности либо угрозу создания помех функционированию или прекращения функционирования объектов жизнеобеспечения, транспортной или социальной инфраструктуры, кредитных организаций, объектов энергетики, промышленности или связи, информационных материалов иностранной или международной

неправительственной организации, деятельность которой признана нежелательной на территории Российской Федерации в соответствии с Федеральным законом от 28 декабря 2012 года № 272-ФЗ «О мерах воздействия на лиц, причастных к нарушениям основополагающих прав и свобод человека, прав и свобод граждан Российской Федерации», сведений, позволяющих получить доступ к указанным информации или материалам (далее – распространяемая с нарушением закона информация), включая случай поступления уведомления о распространяемой с нарушением закона информации от федеральных органов государственной власти, органов государственной власти субъектов Российской Федерации, органов местного самоуправления, организаций или граждан, Генеральный прокурор Российской Федерации или его заместители обращаются в федеральный орган исполнительной власти, осуществляющий функции по контролю и надзору в сфере средств массовой информации, массовых коммуникаций, информационных технологий и связи, с требованием о принятии мер по ограничению доступа к информационным ресурсам, распространяющим такую информацию.

(в ред. Федеральных законов от 25.11.2017 № 327-ФЗ, от 18.03.2019 № 31-ФЗ)

1.1. Федеральный орган исполнительной власти, осуществляющий функции по контролю и надзору в сфере средств массовой информации, массовых коммуникаций, информационных технологий и связи, на основании обращения, указанного в части 1 настоящей статьи и поступившего в отношении недостоверной общественно значимой информации, распространяемой под видом достоверных сообщений, которая создает угрозу причинения вреда жизни и (или) здоровью граждан, имуществу, угрозу массового нарушения общественного порядка и (или) общественной безопасности либо угрозу создания помех функционированию или прекращения функционирования объектов жизнеобеспечения, транспортной или социальной инфраструктуры, кредитных организаций, объектов энергетики, промышленности или связи, которая размещена на информационном ресурсе, зарегистрированном в соответствии с Законом Российской Федерации от 27 декабря 1991 года № 2124-1 «О средствах массовой информации» в качестве сетевого издания (далее – сетевое издание), незамедлительно уведомляет редакцию сетевого издания о необходимости удаления указанной информации и фиксирует дату и время направления такого уведомления редакции сетевого издания в соответствующей информационной системе.

(часть 1.1 введена Федеральным законом от 18.03.2019 № 31-ФЗ)

1.2. Незамедлительно с момента получения от федерального органа исполнительной власти, осуществляющего функции по контролю и надзору в сфере средств массовой информации, массовых коммуникаций, информационных технологий и связи, уведомления, указанного в части 1.1 настоящей статьи, редакция сетевого издания обязана удалить информацию, указанную в части 1.1 настоящей статьи.

(часть 1.2 введена Федеральным законом от 18.03.2019 № 31-ФЗ)

1.3. В случае, если редакция сетевого издания незамедлительно не удалила информацию, указанную в части 1.1 настоящей статьи, федеральный орган исполнительной власти, осуществляющий функции по контролю и надзору в сфере средств массовой информации, массовых коммуникаций, информационных технологий и связи, направляет по системе взаимодействия операторам связи требование о принятии мер по ограничению доступа к сетевому изданию, в котором размещена информация, указанная в части 1.1 настоящей статьи.

Данное требование должно содержать доменное имя сайта в сети «Интернет», сетевой адрес, указатели страниц сайта в сети «Интернет», позволяющие идентифицировать такую информацию.

(часть 1.3 введена Федеральным законом от 18.03.2019 № 31-ФЗ)

1.4. После получения по системе взаимодействия требования, указанного в части 1.3 настоящей статьи, оператор связи, оказывающий услуги по предоставлению доступа к информационно-телекоммуникационной сети «Интернет», незамедлительно обязан ограничить доступ к сетевому изданию, в котором размещена информация, указанная в части 1.1 настоящей статьи.

(часть 1.4 введена Федеральным законом от 18.03.2019 № 31-ФЗ)

1.5. В случае ограничения доступа к сетевому изданию в порядке, предусмотренном частями 1.1–1.4 настоящей статьи, возобновление доступа к сетевому изданию производится в соответствии с порядком, предусмотренным частями 5–7 настоящей статьи.

(часть 1.5 введена Федеральным законом от 18.03.2019 № 31-ФЗ)

2. Федеральный орган исполнительной власти, осуществляющий функции по контролю и надзору в сфере средств массовой информации, массовых коммуникаций, информационных технологий и связи, на основании обращения, указанного в части 1 настоящей статьи, за исключением случаев, предусмотренных частями 1.1-1.4 настоящей статьи, незамедлительно:

(в ред. Федерального закона от 18.03.2019 № 31-ФЗ)

1) направляет по системе взаимодействия операторам связи требование о принятии мер по ограничению доступа к информационному ресурсу, в том числе к сайту в сети «Интернет», на котором размещена распространяемая с нарушением закона информация. Данное требование должно содержать доменное имя сайта в сети «Интернет», сетевой адрес, указатели страниц сайта в сети «Интернет», позволяющие идентифицировать такую информацию;

(в ред. Федерального закона от 25.11.2017 № 327-ФЗ)

2) определяет провайдера хостинга или иное лицо, обеспечивающее размещение в информационно-телекоммуникационной сети, в том числе в сети «Интернет», указанного информационного ресурса, обслуживающего владельца сайта в сети «Интернет», на котором размещена распространяемая с нарушением закона информация;

(в ред. Федерального закона от 25.11.2017 № 327-ФЗ)

3) направляет провайдеру хостинга или иному указанному в пункте 2 настоящей части лицу уведомление в электронном виде на русском и английском языках о нарушении порядка распространения информации с указанием доменного имени и сетевого адреса, позволяющих идентифицировать сайт в сети «Интернет», на котором размещена распространяемая с нарушением закона информация, а также указателей страниц сайта в сети «Интернет», позволяющих идентифицировать такую информацию, и с требованием принять меры по удалению такой информации;

(в ред. Федерального закона от 25.11.2017 № 327-ФЗ)

4) фиксирует дату и время направления уведомления провайдеру хостинга или иному указанному в пункте 2 настоящей части лицу в соответствующей информационной системе.

3. После получения по системе взаимодействия требования федерального органа исполнительной власти, осуществляющего функции по контролю и надзору в сфере средств массовой информации, массовых коммуникаций, информационных технологий и связи, о принятии мер по ограничению досту-

па оператор связи, оказывающий услуги по предоставлению доступа к информационно-телекоммуникационной сети «Интернет», обязан незамедлительно ограничить доступ к информационному ресурсу, в том числе к сайту в сети «Интернет», на котором размещена распространяемая с нарушением закона информация.

(в ред. Федерального закона от 25.11.2017 № 327-ФЗ)

4. В течение суток с момента получения уведомления, указанного в пункте 3 части 2 настоящей статьи, провайдер хостинга или иное указанное в пункте 2 части 2 настоящей статьи лицо обязаны проинформировать об этом обслуживаемого ими владельца информационного ресурса и уведомить его о необходимости незамедлительно удалить распространяемую с нарушением закона информацию.

(в ред. Федерального закона от 25.11.2017 № 327-ФЗ)

5. В случае, если владелец информационного ресурса удалил распространяемую с нарушением закона информацию, он направляет уведомление об этом в федеральный орган исполнительной власти, осуществляющий функции по контролю и надзору в сфере средств массовой информации, массовых коммуникаций, информационных технологий и связи. Такое уведомление может быть направлено также в электронном виде.

(в ред. Федерального закона от 25.11.2017 № 327-ФЗ)

6. После получения уведомления, указанного в части 5 настоящей статьи, и проверки его достоверности федеральный орган исполнительной власти, осуществляющий функции по контролю и надзору в сфере средств массовой информации, массовых коммуникаций, информационных технологий и связи, обязан незамедлительно уведомить по системе взаимодействия оператора связи, оказывающего услуги по предоставлению доступа к информационно-телекоммуникационной сети «Интернет», о возобновлении доступа к информационному ресурсу, в том числе к сайту в сети «Интернет».

7. После получения уведомления, указанного в части 6 настоящей статьи, оператор связи незамедлительно возобновляет доступ к информационному ресурсу, в том числе к сайту в сети «Интернет».

8. Предусмотренный настоящей статьей порядок не применяется в случае обнаружения недостоверной общественно значимой информации, распространяемой под видом достоверных сообщений, которая создает угрозу причинения вреда жизни и (или) здоровью граждан, имуществу, угрозу массового нарушения общественного порядка и (или) общественной безопасности либо угрозу создания помех функционированию или прекращения функционирования объектов жизнеобеспечения, транспортной или социальной инфраструктуры, кредитных организаций, объектов энергетики, промышленности или связи, на информационном ресурсе, указанном в статье 10.4 настоящего Федерального закона.

(часть 8 введена Федеральным законом от 18.03.2019 № 31-ФЗ)

Статья 15.4. Порядок ограничения доступа к информационному ресурсу организатора распространения информации в сети «Интернет»

(введена Федеральным законом от 05.05.2014 № 97-ФЗ)

1. В случае установления факта неисполнения организатором распространения информации в сети «Интернет» обязанностей, предусмотренных статьей 10.1 настоящего Федерального закона, в его адрес (адрес его филиала или представительства) уполномоченным федеральным органом исполнительной

власти направляется уведомление, в котором указывается срок исполнения таких обязанностей, составляющий не менее чем пятнадцать дней.

(в ред. Федерального закона от 29.07.2017 № 241-ФЗ)

2. В случае неисполнения организатором распространения информации в сети «Интернет» в указанный в уведомлении срок обязанностей, предусмотренных статьей 10.1 настоящего Федерального закона, доступ к информационным системам и (или) программам для электронных вычислительных машин, которые предназначены и (или) используются для приема, передачи, доставки и (или) обработки электронных сообщений пользователей сети «Интернет» и функционирование которых обеспечивается данным организатором, до исполнения таких обязанностей ограничивается оператором связи, оказывающим услуги по предоставлению доступа к сети «Интернет», на основании вступившего в законную силу решения суда.

(в ред. Федерального закона от 29.07.2017 № 241-ФЗ)

3. Порядок взаимодействия уполномоченного федерального органа исполнительной власти с организатором распространения информации в сети «Интернет», порядок направления указанного в части 1 настоящей статьи уведомления, порядок ограничения и возобновления доступа к указанным в части 2 настоящей статьи информационным системам и (или) программам и порядок информирования граждан (физических лиц) о таком ограничении устанавливаются Правительством Российской Федерации.

Статья 15.5. Порядок ограничения доступа к информации, обрабатываемой с нарушением законодательства Российской Федерации в области персональных данных

(введена Федеральным законом от 21.07.2014 № 242-ФЗ)

1. В целях ограничения доступа к информации в сети «Интернет», обрабатываемой с нарушением законодательства Российской Федерации в области персональных данных, создается автоматизированная информационная система «Реестр нарушителей прав субъектов персональных данных» (далее – реестр нарушителей).

2. В реестр нарушителей включаются:

1) доменные имена и (или) указатели страниц сайтов в сети «Интернет», содержащих информацию, обрабатываемую с нарушением законодательства Российской Федерации в области персональных данных;

2) сетевые адреса, позволяющие идентифицировать сайты в сети «Интернет», содержащие информацию, обрабатываемую с нарушением законодательства Российской Федерации в области персональных данных;

3) указание на вступивший в законную силу судебный акт;

4) информация об устранении нарушения законодательства Российской Федерации в области персональных данных;

5) дата направления операторам связи данных об информационном ресурсе для ограничения доступа к этому ресурсу.

3. Создание, формирование и ведение реестра нарушителей осуществляются федеральным органом исполнительной власти, осуществляющим функции по контролю и надзору в сфере средств массовой информации, массовых коммуникаций, информационных технологий и связи, в порядке, установленном Правительством Российской Федерации.

4. Федеральный орган исполнительной власти, осуществляющий функции по контролю и надзору в сфере средств массовой информации, массовых

коммуникаций, информационных технологий и связи, в соответствии с критериями, определенными Правительством Российской Федерации, может привлечь к формированию и ведению реестра нарушителей оператора такого реестра – организацию, зарегистрированную на территории Российской Федерации.

5. Основанием для включения в реестр нарушителей информации, указанной в части 2 настоящей статьи, является вступивший в законную силу судебный акт.

6. Субъект персональных данных вправе обратиться в федеральный орган исполнительной власти, осуществляющий функции по контролю и надзору в сфере средств массовой информации, массовых коммуникаций, информационных технологий и связи, с заявлением о принятии мер по ограничению доступа к информации, обрабатываемой с нарушением законодательства Российской Федерации в области персональных данных, на основании вступившего в законную силу судебного акта. Форма указанного заявления утверждается федеральным органом исполнительной власти, осуществляющим функции по контролю и надзору в сфере средств массовой информации, массовых коммуникаций, информационных технологий и связи.

7. В течение трех рабочих дней со дня получения вступившего в законную силу судебного акта федеральный орган исполнительной власти, осуществляющий функции по контролю и надзору в сфере средств массовой информации, массовых коммуникаций, информационных технологий и связи, на основании указанного решения суда:

1) определяет провайдера хостинга или иное лицо, обеспечивающее обработку информации в информационно-телекоммуникационной сети, в том числе в сети «Интернет», с нарушением законодательства Российской Федерации в области персональных данных;

2) направляет провайдеру хостинга или иному указанному в пункте 1 настоящей части лицу в электронном виде уведомление на русском и английском языках о нарушении законодательства Российской Федерации в области персональных данных с информацией о вступившем в законную силу судебном акте, доменном имени и сетевом адресе, позволяющих идентифицировать сайт в сети «Интернет», на котором осуществляется обработка информации с нарушением законодательства Российской Федерации в области персональных данных, а также об указателях страниц сайта в сети «Интернет», позволяющих идентифицировать такую информацию, и с требованием принять меры по устранению нарушения законодательства Российской Федерации в области персональных данных, указанные в решении суда;

3) фиксирует дату и время направления уведомления провайдеру хостинга или иному указанному в пункте 1 настоящей части лицу в реестре нарушителей.

8. В течение одного рабочего дня с момента получения уведомления, указанного в пункте 2 части 7 настоящей статьи, провайдер хостинга или иное указанное в пункте 1 части 7 настоящей статьи лицо обязаны проинформировать об этом обслуживаемого ими владельца информационного ресурса и уведомить его о необходимости незамедлительно принять меры по устранению нарушения законодательства Российской Федерации в области персональных данных, указанного в уведомлении, или принять меры по ограничению доступа к информации, обрабатываемой с нарушением законодательства Российской Федерации в области персональных данных.

9. В течение одного рабочего дня с момента получения от провайдера хостинга или иного указанного в пункте 1 части 7 настоящей статьи лица уведомления о необходимости устранения нарушения законодательства Российской Федерации в области персональных данных владелец информационного ресурса обязан принять меры по устранению указанного в уведомлении нарушения. В случае отказа или бездействия владельца информационного ресурса провайдер хостинга или иное указанное в пункте 1 части 7 настоящей статьи лицо обязаны ограничить доступ к соответствующему информационному ресурсу не позднее истечения трех рабочих дней с момента получения уведомления, указанного в пункте 2 части 7 настоящей статьи.

10. В случае непринятия провайдером хостинга или иным указанным в пункте 1 части 7 настоящей статьи лицом и (или) владельцем информационного ресурса мер, указанных в частях 8 и 9 настоящей статьи, доменное имя сайта в сети «Интернет», его сетевой адрес, указатели страниц сайта в сети «Интернет», позволяющие идентифицировать информацию, обрабатываемую с нарушением законодательства Российской Федерации в области персональных данных, а также иные сведения об этом сайте и информация направляются по автоматизированной информационной системе операторам связи для принятия мер по ограничению доступа к данному информационному ресурсу, в том числе к сетевому адресу, доменному имени, указателю страниц сайта в сети «Интернет».

11. Федеральный орган исполнительной власти, осуществляющий функции по контролю и надзору в сфере средств массовой информации, массовых коммуникаций, информационных технологий и связи, или привлеченный им в соответствии с частью 4 настоящей статьи оператор реестра нарушителей исключает из такого реестра доменное имя, указатель страницы сайта в сети «Интернет» или сетевой адрес, позволяющие идентифицировать сайт в сети «Интернет», на основании обращения владельца сайта в сети «Интернет», провайдера хостинга или оператора связи не позднее чем в течение трех дней со дня такого обращения после принятия мер по устранению нарушения законодательства Российской Федерации в области персональных данных или на основании вступившего в законную силу решения суда об отмене ранее принятого судебного акта.

12. Порядок взаимодействия оператора реестра нарушителей с провайдером хостинга и порядок получения доступа к содержащейся в таком реестре информации оператором связи устанавливаются уполномоченным Правительством Российской Федерации федеральным органом исполнительной власти.

Статья 15.6. Порядок ограничения доступа к сайтам в сети «Интернет», на которых неоднократно и неправомерно размещалась информация, содержащая объекты авторских и (или) смежных прав, или информация, необходимая для их получения с использованием информационно-телекоммуникационных сетей, в том числе сети «Интернет»

(введена Федеральным законом от 24.11.2014 № 364-ФЗ)

1. В течение суток с момента поступления по системе взаимодействия в адрес федерального органа исполнительной власти, осуществляющего функции по контролю и надзору в сфере средств массовой информации, массовых коммуникаций, информационных технологий и связи, вступившего в законную силу соответствующего решения Московского городского суда указанный орган:

1) направляет операторам связи по системе взаимодействия требование о принятии мер по постоянному ограничению доступа к сайту в сети «Интернет», на котором неоднократно и неправомерно размещалась информация, содержащая объекты авторских и (или) смежных прав, или информация, необходимая для их получения с использованием информационно-телекоммуникационных сетей, в том числе сети «Интернет»;

2) направляет в порядке, установленном федеральным органом исполнительной власти, осуществляющим функции по контролю и надзору в сфере средств массовой информации, массовых коммуникаций, информационных технологий и связи, операторам поисковых систем, распространяющим в сети «Интернет» рекламу, которая направлена на привлечение внимания потребителей, находящихся на территории Российской Федерации, в электронном виде требование о прекращении выдачи сведений о доменном имени и об указателях страниц сайтов в сети «Интернет», на которых неоднократно и неправомерно размещалась информация, содержащая объекты авторских и (или) смежных прав, или информация, необходимая для их получения с использованием информационно-телекоммуникационных сетей, в том числе сети «Интернет».

(часть 1 в ред. Федерального закона от 01.07.2017 № 156-ФЗ)

2. В течение суток с момента получения указанного в пункте 1 части 1 настоящей статьи требования оператор связи, оказывающий услуги по предоставлению доступа к информационно-телекоммуникационной сети «Интернет», обязан ограничить доступ к соответствующему сайту в сети «Интернет». Снятие ограничения доступа к такому сайту в сети «Интернет» не допускается.

(в ред. Федерального закона от 01.07.2017 № 156-ФЗ)

2.1. В течение суток с момента получения указанного в пункте 2 части 1 настоящей статьи требования оператор поисковой системы, распространяющий в сети «Интернет» рекламу, которая направлена на привлечение внимания потребителей, находящихся на территории Российской Федерации, обязан прекратить выдачу сведений о доменном имени и об указателях страниц сайтов в сети «Интернет», доступ к которым ограничен на основании соответствующего решения Московского городского суда.

(часть 2.1 введена Федеральным законом от 01.07.2017 № 156-ФЗ)

3. Сведения о сайтах в сети «Интернет», доступ к которым ограничен на основании решения Московского городского суда, размещаются на официальном сайте федерального органа исполнительной власти, осуществляющего функции по контролю и надзору в сфере средств массовой информации, массовых коммуникаций, информационных технологий и связи, в информационно-телекоммуникационной сети «Интернет».

Статья 15.6-1. Порядок ограничения доступа к копиям заблокированных сайтов

(введена Федеральным законом от 01.07.2017 № 156-ФЗ)

1. Размещение в информационно-телекоммуникационных сетях, в том числе в сети «Интернет», сайта, сходного до степени смешения с сайтом в сети «Интернет», доступ к которому ограничен по решению Московского городского суда в связи с неоднократным и неправомерным размещением информации, содержащей объекты авторских и (или) смежных прав, или информации, необходимой для их получения с использованием информационно-телекоммуникационных сетей, в том числе сети «Интернет» (далее – копия заблокированного сайта), не допускается.

2. В случае поступления от федеральных органов исполнительной власти или правообладателей информации об обнаружении в информационно-телекоммуникационных сетях, в том числе в сети «Интернет», указанного в части 1 настоящей статьи сайта федеральный орган исполнительной власти, осуществляющий функции по выработке и реализации государственной политики и нормативно-правовому регулированию в сфере массовых коммуникаций и средств массовой информации, в течение суток:

1) в порядке, установленном Правительством Российской Федерации, принимает мотивированное решение о признании сайта в сети «Интернет» копией заблокированного сайта;

2) направляет в порядке, установленном федеральным органом исполнительной власти, осуществляющим функции по выработке и реализации государственной политики и нормативно-правовому регулированию в сфере массовых коммуникаций и средств массовой информации, владельцу копии заблокированного сайта в электронном виде на русском и английском языках мотивированное решение о признании сайта в сети «Интернет» копией заблокированного сайта;

3) направляет по системе взаимодействия в федеральный орган исполнительной власти, осуществляющий функции по контролю и надзору в сфере средств массовой информации, массовых коммуникаций, информационных технологий и связи, мотивированное решение о признании сайта в сети «Интернет» копией заблокированного сайта.

3. В течение суток с момента поступления по системе взаимодействия мотивированного решения федерального органа исполнительной власти, осуществляющего функции по выработке и реализации государственной политики и нормативно-правовому регулированию в сфере массовых коммуникаций и средств массовой информации, о признании сайта в сети «Интернет» копией заблокированного сайта, федеральный орган исполнительной власти, осуществляющий функции по контролю и надзору в сфере средств массовой информации, массовых коммуникаций, информационных технологий и связи:

1) определяет провайдера хостинга или иное обеспечивающее размещение копии заблокированного сайта в сети «Интернет» лицо;

2) направляет провайдеру хостинга или указанному в пункте 1 настоящей части лицу уведомление в электронном виде на русском и английском языках о принятом федеральным органом исполнительной власти, осуществляющим функции по выработке и реализации государственной политики и нормативно-правовому регулированию в сфере массовых коммуникаций и средств массовой информации, мотивированном решении о признании сайта в сети «Интернет» копией заблокированного сайта;

3) фиксирует дату и время направления предусмотренного пунктом 2 настоящей части уведомления провайдеру хостинга или указанному в пункте 1 настоящей части лицу в соответствующей информационной системе;

4) направляет по системе взаимодействия операторам связи требование о принятии мер по ограничению доступа к копии заблокированного сайта;

5) направляет в порядке, установленном федеральным органом исполнительной власти, осуществляющим функции по контролю и надзору в сфере средств массовой информации, массовых коммуникаций, информационных технологий и связи, операторам поисковых систем, распространяющим в сети «Интернет» рекламу, которая направлена на привлечение внимания потребителей, находящихся на территории Российской Федерации, в электронном виде

требование о прекращении выдачи сведений о доменном имени и об указателях страниц копии заблокированного сайта.

4. В течение суток с момента получения указанного в пункте 4 части 3 настоящей статьи требования оператор связи, оказывающий услуги по предоставлению доступа к информационно-телекоммуникационной сети, в том числе сети «Интернет», обязан ограничить доступ к копии заблокированного сайта.

5. В течение суток с момента получения указанного в пункте 5 части 3 настоящей статьи требования оператор поисковой системы, распространяющий в сети «Интернет» рекламу, которая направлена на привлечение внимания потребителей, находящихся на территории Российской Федерации, обязан прекратить выдачу сведений о доменном имени и об указателях страниц копии заблокированного сайта.

6. Сведения о копиях заблокированных сайтов размещаются на официальном сайте федерального органа исполнительной власти, осуществляющего функции по контролю и надзору в сфере средств массовой информации, массовых коммуникаций, информационных технологий и связи, в сети «Интернет».

Статья 15.7. Внесудебные меры по прекращению нарушения авторских и (или) смежных прав в информационно-телекоммуникационных сетях, в том числе в сети «Интернет», принимаемые по заявлению правообладателя

(введена Федеральным законом от 24.11.2014 № 364-ФЗ)

1. Правообладатель в случае обнаружения в информационно-телекоммуникационных сетях, в том числе в сети «Интернет», сайта в сети «Интернет», на котором без его разрешения или иного законного основания размещена информация, содержащая объекты авторских и (или) смежных прав, или информация, необходимая для их получения с использованием информационно-телекоммуникационных сетей, в том числе сети «Интернет», вправе направить владельцу сайта в сети «Интернет» в письменной или электронной форме заявление о нарушении авторских и (или) смежных прав (далее – заявление). Заявление может быть направлено лицом, уполномоченным правообладателем в соответствии с законодательством Российской Федерации.

2. Заявление должно содержать:

1) сведения о правообладателе или лице, уполномоченном правообладателем (если заявление направляется таким лицом) (далее – заявитель):

а) для физического лица – фамилию, имя, отчество, паспортные данные (серия и номер, кем выдан, дата выдачи), контактную информацию (номера телефона и (или) факса, адрес электронной почты);

б) для юридического лица – наименование, место нахождения и адрес, контактную информацию (номера телефона и (или) факса, адрес электронной почты);

2) информацию об объекте авторских и (или) смежных прав, размещенном на сайте в сети «Интернет» без разрешения правообладателя или иного законного основания;

3) указание на доменное имя и (или) сетевой адрес сайта в сети «Интернет», на котором без разрешения правообладателя или иного законного основания размещена информация, содержащая объект авторских и (или) смежных прав, или информация, необходимая для его получения с использованием информационно-телекоммуникационных сетей, в том числе сети «Интернет»;

4) указание на наличие у правообладателя прав на объект авторских и (или) смежных прав, размещенный на сайте в сети «Интернет» без разрешения правообладателя или иного законного основания;

5) указание на отсутствие разрешения правообладателя на размещение на сайте в сети «Интернет» информации, содержащей объект авторских и (или) смежных прав, или информации, необходимой для его получения с использованием информационно-телекоммуникационных сетей, в том числе сети «Интернет»;

6) согласие заявителя на обработку его персональных данных (для заявителя – физического лица).

3. В случае, если заявление подается уполномоченным лицом, к заявлению прикладывается копия документа (в письменной или электронной форме), подтверждающего его полномочия.

4. В случае обнаружения неполноты сведений, неточностей или ошибок в заявлении владелец сайта в сети «Интернет» вправе направить заявителю в течение двадцати четырех часов с момента получения заявления уведомление об уточнении представленных сведений. Указанное уведомление может быть направлено заявителю однократно.

5. В течение двадцати четырех часов с момента получения уведомления, указанного в части 4 настоящей статьи, заявитель принимает меры, направленные на восполнение недостающих сведений, устранение неточностей и ошибок, и направляет владельцу сайта в сети «Интернет» уточненные сведения.

6. В течение двадцати четырех часов с момента получения заявления или уточненных заявителем сведений (в случае направления заявителю уведомления, указанного в части 4 настоящей статьи) владелец сайта в сети «Интернет» удаляет указанную в части 1 настоящей статьи информацию.

7. При наличии у владельца сайта в сети «Интернет» доказательств, подтверждающих правомерность размещения на принадлежащем ему сайте в сети «Интернет» информации, содержащей объект авторских и (или) смежных прав, или информации, необходимой для его получения с использованием информационно-телекоммуникационных сетей, в том числе сети «Интернет», владелец сайта в сети «Интернет» вправе не принимать предусмотренные частью 6 настоящей статьи меры и обязан направить заявителю соответствующее уведомление с приложением указанных доказательств.

8. Правила настоящей статьи в равной степени распространяются на правообладателя и на лицензиата, получившего исключительную лицензию на объект авторских и (или) смежных прав.

Статья 15.8. Меры, направленные на противодействие использованию на территории Российской Федерации информационно-телекоммуникационных сетей и информационных ресурсов, посредством которых обеспечивается доступ к информационным ресурсам и информационно-телекоммуникационным сетям, доступ к которым ограничен на территории Российской Федерации

(введена Федеральным законом от 29.07.2017 № 276-ФЗ)

1. Владельцам информационно-телекоммуникационных сетей, информационных ресурсов (сайт в сети «Интернет» и (или) страница сайта в сети «Интернет», информационная система, программа для электронных вычислительных машин), посредством которых обеспечивается доступ к информационным ресурсам, информационно-телекоммуникационным сетям, доступ к которым огра-

ничен на территории Российской Федерации в соответствии с настоящим Федеральным законом (далее также – владелец программно-аппаратных средств доступа к информационным ресурсам, информационно-телекоммуникационным сетям, доступ к которым ограничен), запрещается предоставлять возможность использования на территории Российской Федерации принадлежащих им информационно-телекоммуникационных сетей и информационных ресурсов для получения доступа к информационным ресурсам, информационно-телекоммуникационным сетям, доступ к которым ограничен на территории Российской Федерации в соответствии с настоящим Федеральным законом.

2. В целях противодействия использованию на территории Российской Федерации информационно-телекоммуникационных сетей, информационных ресурсов, посредством которых обеспечивается доступ к информационным ресурсам, информационно-телекоммуникационным сетям, доступ к которым ограничен на территории Российской Федерации в соответствии с настоящим Федеральным законом (далее также – программно-аппаратные средства доступа к информационным ресурсам, информационно-телекоммуникационным сетям, доступ к которым ограничен), для получения доступа к информационным ресурсам, информационно-телекоммуникационным сетям, доступ к которым ограничен на территории Российской Федерации в соответствии с настоящим Федеральным законом, федеральный орган исполнительной власти, осуществляющий функции по контролю и надзору в сфере средств массовой информации, массовых коммуникаций, информационных технологий и связи:

1) осуществляет создание и эксплуатацию федеральной государственной информационной системы, содержащей перечень информационных ресурсов, информационно-телекоммуникационных сетей, доступ к которым ограничен на территории Российской Федерации в соответствии с настоящим Федеральным законом (далее – федеральная государственная информационная система информационных ресурсов информационно-телекоммуникационных сетей, доступ к которым ограничен);

2) в порядке, установленном Правительством Российской Федерации, взаимодействует с федеральными органами исполнительной власти, осуществляющими оперативно-разыскную деятельность или обеспечение безопасности Российской Федерации, в целях получения информации о программно-аппаратных средствах доступа к информационным ресурсам, информационно-телекоммуникационным сетям, доступ к которым ограничен;

3) на основании обращения федерального органа исполнительной власти, осуществляющего оперативно-разыскную деятельность или обеспечение безопасности Российской Федерации, определяет провайдера хостинга или иное лицо, обеспечивающее размещение в сети «Интернет» программно-аппаратных средств доступа к информационным ресурсам, информационно-телекоммуникационным сетям, доступ к которым ограничен;

4) направляет провайдеру хостинга или иному указанному в пункте 3 настоящей части лицу уведомление в электронном виде на русском и английском языках о необходимости предоставления данных, позволяющих идентифицировать владельца программно-аппаратных средств доступа к информационным ресурсам, информационно-телекоммуникационным сетям, доступ к которым ограничен, или о необходимости уведомления владельца программно-аппаратных средств доступа к информационным ресурсам, информационно-телекоммуникационным сетям, доступ к которым ограничен, о необходимости размещения указанных данных на сайте в сети «Интернет» такого владельца;

5) фиксирует дату и время направления указанного в пункте 4 настоящей части уведомления в федеральной государственной информационной системе информационных ресурсов, информационно-телекоммуникационных сетей, доступ к которым ограничен.

3. В течение трех рабочих дней со дня получения уведомления, указанного в пункте 4 части 2 настоящей статьи, провайдер хостинга или иное указанное в пункте 3 части 2 настоящей статьи лицо обязаны предоставить информацию о совершении действий, предусмотренных таким уведомлением.

4. В течение трех рабочих дней со дня получения данных, позволяющих идентифицировать владельца программно-аппаратных средств доступа к информационным ресурсам, информационно-телекоммуникационным сетям, доступ к которым ограничен, или самостоятельного выявления таких данных федеральным органом исполнительной власти, осуществляющим функции по контролю и надзору в сфере средств массовой информации, массовых коммуникаций, информационных технологий и связи, указанный федеральный орган исполнительной власти направляет этому владельцу на русском и английском языках требование о необходимости подключения такого владельца к федеральной государственной информационной системе информационных ресурсов, информационно-телекоммуникационных сетей, доступ к которым ограничен.

5. В течение тридцати рабочих дней со дня направления требования, указанного в части 4 настоящей статьи, владелец программно-аппаратных средств доступа к информационным ресурсам, информационно-телекоммуникационным сетям, доступ к которым ограничен, обязан подключиться к федеральной государственной информационной системе информационных ресурсов, информационно-телекоммуникационных сетей, доступ к которым ограничен, в порядке, установленном федеральным органом исполнительной власти, осуществляющим функции по контролю и надзору в сфере средств массовой информации, массовых коммуникаций, информационных технологий и связи.

6. По требованию федерального органа исполнительной власти, осуществляющего функции по контролю и надзору в сфере средств массовой информации, массовых коммуникаций, информационных технологий и связи, к федеральной государственной информационной системе информационных ресурсов, информационно-телекоммуникационных сетей, доступ к которым ограничен, также обязан подключиться оператор поисковой системы, распространяющий в сети «Интернет» рекламу, которая направлена на привлечение внимания потребителей, находящихся на территории Российской Федерации, в течение тридцати рабочих дней со дня получения указанного требования.

7. Владелец программно-аппаратных средств доступа к информационным ресурсам, информационно-телекоммуникационным сетям, доступ к которым ограничен, обязан:

1) в течение трех рабочих дней после предоставления ему доступа к федеральной государственной информационной системе информационных ресурсов, информационно-телекоммуникационных сетей, доступ к которым ограничен, обеспечить соблюдение запрета предоставлять возможность использования на территории Российской Федерации программно-аппаратных средств доступа к информационным ресурсам, информационно-телекоммуникационным сетям, доступ к которым ограничен, для получения доступа к информационным ресурсам, информационно-телекоммуникационным сетям, доступ к которым ограничен на территории Российской Федерации в соответствии с настоящим Федеральным законом;

2) соблюдать установленный федеральным органом исполнительной власти, осуществляющим функции по контролю и надзору в сфере средств массовой информации, массовых коммуникаций, информационных технологий и связи, режим обработки и использования информации, размещенной в федеральной государственной информационной системе информационных ресурсов, информационно-телекоммуникационных сетей, доступ к которым ограничен.

8. В течение трех рабочих дней со дня получения доступа к федеральной государственной информационной системе информационных ресурсов, информационно-телекоммуникационных сетей, доступ к которым ограничен, оператор поисковой системы, распространяющий в сети «Интернет» рекламу, которая направлена на привлечение внимания потребителей, находящихся на территории Российской Федерации, обязан прекратить на территории Российской Федерации выдачу по запросам пользователей указанной поисковой системы сведений об информационных ресурсах, информационно-телекоммуникационных сетях, доступ к которым ограничен на территории Российской Федерации в соответствии с настоящим Федеральным законом.

9. Порядок взаимодействия федерального органа исполнительной власти, осуществляющего функции по контролю и надзору в сфере средств массовой информации, массовых коммуникаций, информационных технологий и связи, с лицами, указанными в частях 5 и 6 настоящей статьи, при предоставлении доступа к федеральной государственной информационной системе информационных ресурсов, информационно-телекоммуникационных сетей, доступ к которым ограничен, порядок доступа к указанной системе и к информации, размещенной в ней, режим обработки и использования такой информации, требования к технологическим, программным, лингвистическим, правовым и организационным средствам обеспечения пользования указанной системой устанавливаются федеральным органом исполнительной власти, осуществляющим функции по контролю и надзору в сфере средств массовой информации, массовых коммуникаций, информационных технологий и связи.

10. В случае неисполнения владельцем программно-аппаратных средств доступа к информационным ресурсам, информационно-телекоммуникационным сетям, доступ к которым ограничен, обязанностей, предусмотренных частями 5 и 7 настоящей статьи, федеральный орган исполнительной власти, осуществляющий функции по контролю и надзору в сфере средств массовой информации, массовых коммуникаций, информационных технологий и связи, принимает решение об ограничении доступа к принадлежащим такому владельцу программно-аппаратным средствам доступа к информационным ресурсам, информационно-телекоммуникационным сетям, доступ к которым ограничен.

11. В течение суток с момента принятия указанного в части 10 настоящей статьи решения федеральный орган исполнительной власти, осуществляющий функции по контролю и надзору в сфере средств массовой информации, массовых коммуникаций, информационных технологий и связи, направляет по системе взаимодействия операторам связи, оказывающим услуги по предоставлению доступа к сети «Интернет», информацию, необходимую для ограничения доступа к соответствующим программно-аппаратным средствам доступа к информационным ресурсам, информационно-телекоммуникационным сетям, доступ к которым ограничен.

12. Операторы связи, оказывающие услуги по предоставлению доступа к сети «Интернет», в течение суток с момента получения по системе взаимо-

действия информации, указанной в части 11 настоящей статьи, обязаны в соответствии с полученной информацией ограничить на территории Российской Федерации доступ к соответствующим программно-аппаратным средствам доступа к информационным ресурсам, информационно-телекоммуникационным сетям, доступ к которым ограничен.

13. В случае, если владелец программно-аппаратных средств доступа к информационным ресурсам, информационно-телекоммуникационным сетям, доступ к которым ограничен, обеспечил исполнение обязанностей, предусмотренных частями 5 и 7 настоящей статьи, он направляет уведомление об этом в федеральный орган исполнительной власти, осуществляющий функции по контролю и надзору в сфере средств массовой информации, массовых коммуникаций, информационных технологий и связи. Такое уведомление может быть направлено также в электронном виде.

14. После получения уведомления, указанного в части 13 настоящей статьи, и проверки его достоверности федеральный орган исполнительной власти, осуществляющий функции по контролю и надзору в сфере средств массовой информации, массовых коммуникаций, информационных технологий и связи, обязан в течение суток уведомить по системе взаимодействия операторов связи, оказывающих услуги по предоставлению доступа к сети «Интернет», о необходимости возобновления доступа к информационно-телекоммуникационным сетям, информационным ресурсам, доступ к которым был ограничен на основании решения указанного федерального органа исполнительной власти в соответствии с частью 10 настоящей статьи.

15. Операторы связи, оказывающие услуги по предоставлению доступа к сети «Интернет», в течение суток с момента получения по системе взаимодействия уведомления, указанного в части 14 настоящей статьи, обязаны прекратить ограничение доступа к информационно-телекоммуникационным сетям, информационным ресурсам, доступ к которым был ограничен на основании решения федерального органа исполнительной власти, осуществляющего функции по контролю и надзору в сфере средств массовой информации, массовых коммуникаций, информационных технологий и связи, в соответствии с частью 10 настоящей статьи.

16. Порядок контроля за обеспечением ограничения доступа к программно-аппаратным средствам доступа к информационным ресурсам, информационно-телекоммуникационным сетям, доступ к которым ограничен, и порядок контроля за прекращением на территории Российской Федерации выдачи операторами поисковых систем, распространяющими в сети «Интернет» рекламу, которая направлена на привлечение внимания потребителей, находящихся на территории Российской Федерации, сведений об информационных ресурсах, информационно-телекоммуникационных сетях, доступ к которым ограничен на территории Российской Федерации в соответствии с настоящим Федеральным законом, утверждаются федеральным органом исполнительной власти, осуществляющим функции по контролю и надзору в сфере средств массовой информации, массовых коммуникаций, информационных технологий и связи.

17. Положения настоящей статьи не распространяются на операторов государственных информационных систем, государственные органы и органы местного самоуправления, а также на случаи использования программно-аппаратных средств доступа к информационным ресурсам, информационно-телекоммуникационным сетям, доступ к которым ограничен, при условии,

что круг пользователей таких программно-аппаратных средств их владельцами заранее определен и использование таких программно-аппаратных средств осуществляется в технологических целях обеспечения деятельности лица, осуществляющего их использование.

Статья 16. Защита информации

1. Защита информации представляет собой принятие правовых, организационных и технических мер, направленных на:

1) обеспечение защиты информации от неправомерного доступа, уничтожения, модифицирования, блокирования, копирования, предоставления, распространения, а также от иных неправомерных действий в отношении такой информации;

2) соблюдение конфиденциальности информации ограниченного доступа;

3) реализацию права на доступ к информации.

2. Государственное регулирование отношений в сфере защиты информации осуществляется путем установления требований о защите информации, а также ответственности за нарушение законодательства Российской Федерации об информации, информационных технологиях и о защите информации.

3. Требования о защите общедоступной информации могут устанавливаться только для достижения целей, указанных в пунктах 1 и 3 части 1 настоящей статьи.

4. Обладатель информации, оператор информационной системы в случаях, установленных законодательством Российской Федерации, обязаны обеспечить:

1) предотвращение несанкционированного доступа к информации и (или) передачи ее лицам, не имеющим права на доступ к информации;

2) своевременное обнаружение фактов несанкционированного доступа к информации;

3) предупреждение возможности неблагоприятных последствий нарушения порядка доступа к информации;

4) недопущение воздействия на технические средства обработки информации, в результате которого нарушается их функционирование;

5) возможность незамедлительного восстановления информации, модифицированной или уничтоженной вследствие несанкционированного доступа к ней;

6) постоянный контроль за обеспечением уровня защищенности информации;

7) нахождение на территории Российской Федерации баз данных информации, с использованием которых осуществляются сбор, запись, систематизация, накопление, хранение, уточнение (обновление, изменение), извлечение персональных данных граждан Российской Федерации.

(п. 7 введен Федеральным законом от 21.07.2014 № 242-ФЗ)

5. Требования о защите информации, содержащейся в государственных информационных системах, устанавливаются федеральным органом исполнительной власти в области обеспечения безопасности и федеральным органом исполнительной власти, уполномоченным в области противодействия техническим разведкам и технической защиты информации, в пределах их полномочий. При создании и эксплуатации государственных информационных систем используемые в целях защиты информации методы и способы ее защиты должны соответствовать указанным требованиям.

6. Федеральными законами могут быть установлены ограничения использования определенных средств защиты информации и осуществления отдельных видов деятельности в области защиты информации.

Статья 17. Ответственность за правонарушения в сфере информации, информационных технологий и защиты информации

1. Нарушение требований настоящего Федерального закона влечет за собой дисциплинарную, гражданско-правовую, административную или уголовную ответственность в соответствии с законодательством Российской Федерации.

1.1. Лица, виновные в нарушении требований статьи 14.1 настоящего Федерального закона в части обработки, включая сбор и хранение, биометрических персональных данных, несут административную, гражданскую и уголовную ответственность в соответствии с законодательством Российской Федерации.

(часть 1.1 введена Федеральным законом от 31.12.2017 № 482-ФЗ)

2. Лица, права и законные интересы которых были нарушены в связи с разглашением информации ограниченного доступа или иным неправомерным использованием такой информации, вправе обратиться в установленном порядке за судебной защитой своих прав, в том числе с исками о возмещении убытков, компенсации морального вреда, защите чести, достоинства и деловой репутации. Требование о возмещении убытков не может быть удовлетворено в случае предъявления его лицом, не принимавшим мер по соблюдению конфиденциальности информации или нарушившим установленные законодательством Российской Федерации требования о защите информации, если принятие этих мер и соблюдение таких требований являлись обязанностями данного лица.

3. В случае, если распространение определенной информации ограничивается или запрещается федеральными законами, гражданско-правовую ответственность за распространение такой информации не несет лицо, оказывающее услуги:

1) либо по передаче информации, предоставленной другим лицом, при условии ее передачи без изменений и исправлений;

2) либо по хранению информации и обеспечению доступа к ней при условии, что это лицо не могло знать о незаконности распространения информации.

4. Провайдер хостинга, оператор связи и владелец сайта в сети «Интернет» не несут ответственность перед правообладателем и перед пользователем за ограничение доступа к информации и (или) ограничение ее распространения в соответствии с требованиями настоящего Федерального закона.

(часть 4 введена Федеральным законом от 02.07.2013 № 187-ФЗ; в ред. Федерального закона от 24.11.2014 № 364-ФЗ)

Статья 18. О признании утратившими силу отдельных законодательных актов (положений законодательных актов) Российской Федерации

Со дня вступления в силу настоящего Федерального закона признать утратившими силу:

1) Федеральный закон от 20 февраля 1995 года № 24-ФЗ «Об информации, информатизации и защите информации» (Собрание законодательства Российской Федерации, 1995, № 8, ст. 609);

2) Федеральный закон от 4 июля 1996 года № 85-ФЗ «Об участии в международном информационном обмене» (Собрание законодательства Российской Федерации, 1996, № 28, ст. 3347);

3) статью 16 Федерального закона от 10 января 2003 года № 15-ФЗ «О внесении изменений и дополнений в некоторые законодательные акты Российской Федерации в связи с принятием Федерального закона «О лицензировании отдельных видов деятельности» (Собрание законодательства Российской Федерации, 2003, № 2, ст. 167);

4) статью 21 Федерального закона от 30 июня 2003 года № 86-ФЗ «О внесении изменений и дополнений в некоторые законодательные акты Российской Федерации, признании утратившими силу отдельных законодательных актов Российской Федерации, предоставлении отдельных гарантий сотрудникам органов внутренних дел, органов по контролю за оборотом наркотических средств и психотропных веществ и упраздняемых федеральных органов налоговой полиции в связи с осуществлением мер по совершенствованию государственного управления» (Собрание законодательства Российской Федерации, 2003, № 27, ст. 2700);

5) статью 39 Федерального закона от 29 июня 2004 года № 58-ФЗ «О внесении изменений в некоторые законодательные акты Российской Федерации и признании утратившими силу некоторых законодательных актов Российской Федерации в связи с осуществлением мер по совершенствованию государственного управления» (Собрание законодательства Российской Федерации, 2004, № 27, ст. 2711).

РОССИЙСКАЯ ФЕДЕРАЦИЯ

ФЕДЕРАЛЬНЫЙ ЗАКОН

О БЕЗОПАСНОСТИ КРИТИЧЕСКОЙ ИНФОРМАЦИОННОЙ ИНФРАСТРУКТУРЫ РОССИЙСКОЙ ФЕДЕРАЦИИ

Принят
Государственной Думой
12 июля 2017 года

Одобрен
Советом Федерации
19 июля 2017 года

Статья 1. Сфера действия настоящего Федерального закона

Настоящий Федеральный закон регулирует отношения в области обеспечения безопасности критической информационной инфраструктуры Российской Федерации (далее также – критическая информационная инфраструктура) в целях ее устойчивого функционирования при проведении в отношении ее компьютерных атак.

Статья 2. Основные понятия, используемые в настоящем Федеральном законе

Для целей настоящего Федерального закона используются следующие основные понятия:

1) автоматизированная система управления – комплекс программных и программно-аппаратных средств, предназначенных для контроля за технологическим и (или) производственным оборудованием (исполнительными устройствами) и производимыми ими процессами, а также для управления такими оборудованием и процессами;

2) безопасность критической информационной инфраструктуры – состояние защищенности критической информационной инфраструктуры, обеспечивающее ее устойчивое функционирование при проведении в отношении ее компьютерных атак;

3) значимый объект критической информационной инфраструктуры – объект критической информационной инфраструктуры, которому присвоена одна из категорий значимости и который включен в реестр значимых объектов критической информационной инфраструктуры;

4) компьютерная атака – целенаправленное воздействие программных и (или) программно-аппаратных средств на объекты критической информационной инфраструктуры, сети электросвязи, используемые для организации взаимодействия таких объектов, в целях нарушения и (или) прекращения их функционирования и (или) создания угрозы безопасности обрабатываемой такими объектами информации;

5) компьютерный инцидент – факт нарушения и (или) прекращения функционирования объекта критической информационной инфраструктуры, сети электросвязи, используемой для организации взаимодействия таких объектов, и (или) нарушения безопасности обрабатываемой таким объектом информации, в том числе произошедший в результате компьютерной атаки;

6) критическая информационная инфраструктура – объекты критической информационной инфраструктуры, а также сети электросвязи, используемые для организации взаимодействия таких объектов;

7) объекты критической информационной инфраструктуры – информационные системы, информационно-телекоммуникационные сети, автоматизированные системы управления субъектов критической информационной инфраструктуры;

8) субъекты критической информационной инфраструктуры – государственные органы, государственные учреждения, российские юридические лица и (или) индивидуальные предприниматели, которым на праве собственности, аренды или на ином законном основании принадлежат информационные системы, информационно-телекоммуникационные сети, автоматизированные системы управления, функционирующие в сфере здравоохранения, науки, транспорта, связи, энергетики, банковской сфере и иных сферах финансового рынка, топливно-энергетического комплекса, в области атомной энергии, оборонной, ракетно-космической, горнодобывающей, металлургической и химической промышленности, российские юридические лица и (или) индивидуальные предприниматели, которые обеспечивают взаимодействие указанных систем или сетей.

Статья 3. Правовое регулирование отношений в области обеспечения безопасности критической информационной инфраструктуры

1. Отношения в области обеспечения безопасности критической информационной инфраструктуры регулируются в соответствии с Конституцией Российской Федерации, общепризнанными принципами и нормами международного права, настоящим Федеральным законом, другими федеральными законами и принимаемыми в соответствии с ними иными нормативными правовыми актами.

2. Особенности применения настоящего Федерального закона к сетям связи общего пользования определяются Федеральным законом от 7 июля 2003 года № 126-ФЗ «О связи» и принимаемыми в соответствии с ним нормативными правовыми актами Российской Федерации.

Статья 4. Принципы обеспечения безопасности критической информационной инфраструктуры

Принципами обеспечения безопасности критической информационной инфраструктуры являются:

1) законность;

2) непрерывность и комплексность обеспечения безопасности критической информационной инфраструктуры, достигаемые в том числе за счет взаимодействия уполномоченных федеральных органов исполнительной власти и субъектов критической информационной инфраструктуры;

3) приоритет предотвращения компьютерных атак.

Статья 5. Государственная система обнаружения, предупреждения и ликвидации последствий компьютерных атак на информационные ресурсы Российской Федерации

1. Государственная система обнаружения, предупреждения и ликвидации последствий компьютерных атак на информационные ресурсы Российской Федерации представляет собой единый территориально распределенный комплекс, включающий силы и средства, предназначенные для обнаружения, предупреждения и ликвидации последствий компьютерных атак и реагирования на компьютерные инциденты. В целях настоящей статьи под информационными ресурсами Российской Федерации понимаются информационные системы, информационно-телекоммуникационные сети и автоматизированные системы управления, находящиеся на территории Российской Федерации, в дипломатических представительствах и (или) консульских учреждениях Российской Федерации.

2. К силам, предназначенным для обнаружения, предупреждения и ликвидации последствий компьютерных атак и реагирования на компьютерные инциденты, относятся:

1) подразделения и должностные лица федерального органа исполнительной власти, уполномоченного в области обеспечения функционирования государственной системы обнаружения, предупреждения и ликвидации последствий компьютерных атак на информационные ресурсы Российской Федерации;

2) организация, создаваемая федеральным органом исполнительной власти, уполномоченным в области обеспечения функционирования государственной системы обнаружения, предупреждения и ликвидации последствий компьютерных атак на информационные ресурсы Российской Федерации, для обеспечения координации деятельности субъектов критической информационной инфраструктуры по вопросам обнаружения, предупреждения и ликвидации последствий компьютерных атак и реагирования на компьютерные инциденты (далее – национальный координационный центр по компьютерным инцидентам);

3) подразделения и должностные лица субъектов критической информационной инфраструктуры, которые принимают участие в обнаружении, предупреждении и ликвидации последствий компьютерных атак и в реагировании на компьютерные инциденты.

3. Средствами, предназначенными для обнаружения, предупреждения и ликвидации последствий компьютерных атак и реагирования на компьютерные инциденты, являются технические, программные, программно-аппаратные и иные средства для обнаружения (в том числе для поиска признаков компьютерных атак в сетях электросвязи, используемых для организации взаимодействия объектов критической информационной инфраструктуры), предупреждения, ликвидации последствий компьютерных атак и (или) обмена информацией, необходимой субъектам критической информационной инфраструктуры при обнаружении, предупреждении и (или) ликвидации последствий компьютерных атак, а также криптографические средства защиты такой информации.

4. Национальный координационный центр по компьютерным инцидентам осуществляет свою деятельность в соответствии с положением, утверждаемым федеральным органом исполнительной власти, уполномоченным в области обеспечения функционирования государственной системы обнаружения, пред-

упреждения и ликвидации последствий компьютерных атак на информационные ресурсы Российской Федерации.

5. В государственной системе обнаружения, предупреждения и ликвидации последствий компьютерных атак на информационные ресурсы Российской Федерации осуществляются сбор, накопление, систематизация и анализ информации, которая поступает в данную систему через средства, предназначенные для обнаружения, предупреждения и ликвидации последствий компьютерных атак, информации, которая представляется субъектами критической информационной инфраструктуры и федеральным органом исполнительной власти, уполномоченным в области обеспечения безопасности критической информационной инфраструктуры Российской Федерации, в соответствии с перечнем информации и в порядке, определяемыми федеральным органом исполнительной власти, уполномоченным в области обеспечения функционирования государственной системы обнаружения, предупреждения и ликвидации последствий компьютерных атак на информационные ресурсы Российской Федерации, а также информации, которая может представляться иными не являющимися субъектами критической информационной инфраструктуры органами и организациями, в том числе иностранными и международными.

6. Федеральный орган исполнительной власти, уполномоченный в области обеспечения функционирования государственной системы обнаружения, предупреждения и ликвидации последствий компьютерных атак на информационные ресурсы Российской Федерации, организует в установленном им порядке обмен информацией о компьютерных инцидентах между субъектами критической информационной инфраструктуры, а также между субъектами критической информационной инфраструктуры и уполномоченными органами иностранных государств, международными, международными неправительственными организациями и иностранными организациями, осуществляющими деятельность в области реагирования на компьютерные инциденты.

7. Предоставление из государственной системы обнаружения, предупреждения и ликвидации последствий компьютерных атак на информационные ресурсы Российской Федерации сведений, составляющих государственную либо иную охраняемую законом тайну, осуществляется в соответствии с законодательством Российской Федерации.

Статья 6. Полномочия Президента Российской Федерации и органов государственной власти Российской Федерации в области обеспечения безопасности критической информационной инфраструктуры

1. Президент Российской Федерации определяет:

1) основные направления государственной политики в области обеспечения безопасности критической информационной инфраструктуры;

2) федеральный орган исполнительной власти, уполномоченный в области обеспечения безопасности критической информационной инфраструктуры Российской Федерации;

3) федеральный орган исполнительной власти, уполномоченный в области обеспечения функционирования государственной системы обнаружения, предупреждения и ликвидации последствий компьютерных атак на информационные ресурсы Российской Федерации;

4) порядок создания и задачи государственной системы обнаружения, предупреждения и ликвидации последствий компьютерных атак на информационные ресурсы Российской Федерации.

2. Правительство Российской Федерации устанавливает:

1) показатели критериев значимости объектов критической информационной инфраструктуры и их значения, а также порядок и сроки осуществления их категорирования;

2) порядок осуществления государственного контроля в области обеспечения безопасности значимых объектов критической информационной инфраструктуры;

3) порядок подготовки и использования ресурсов единой сети электросвязи Российской Федерации для обеспечения функционирования значимых объектов критической информационной инфраструктуры.

3. Федеральный орган исполнительной власти, уполномоченный в области обеспечения безопасности критической информационной инфраструктуры Российской Федерации:

1) вносит предложения о совершенствовании нормативно-правового регулирования в области обеспечения безопасности критической информационной инфраструктуры Президенту Российской Федерации и (или) в Правительство Российской Федерации;

2) утверждает порядок ведения реестра значимых объектов критической информационной инфраструктуры и ведет данный реестр;

3) утверждает форму направления сведений о результатах присвоения объекту критической информационной инфраструктуры одной из категорий значимости либо об отсутствии необходимости присвоения ему одной из таких категорий;

4) устанавливает требования по обеспечению безопасности значимых объектов критической информационной инфраструктуры (требования по обеспечению безопасности информационно-телекоммуникационных сетей, которым присвоена одна из категорий значимости и которые включены в реестр значимых объектов критической информационной инфраструктуры, устанавливаются по согласованию с федеральным органом исполнительной власти, осуществляющим функции по выработке и реализации государственной политики и нормативно-правовому регулированию в области связи), а также требования к созданию систем безопасности таких объектов и обеспечению их функционирования (в банковской сфере и в иных сферах финансового рынка устанавливает указанные требования по согласованию с Центральным банком Российской Федерации);

5) осуществляет государственный контроль в области обеспечения безопасности значимых объектов критической информационной инфраструктуры, а также утверждает форму акта проверки, составляемого по итогам проведения указанного контроля.

4. Федеральный орган исполнительной власти, уполномоченный в области обеспечения функционирования государственной системы обнаружения, предупреждения и ликвидации последствий компьютерных атак на информационные ресурсы Российской Федерации:

1) вносит предложения о совершенствовании нормативно-правового регулирования в области обеспечения безопасности критической информационной инфраструктуры Президенту Российской Федерации и (или) в Правительство Российской Федерации;

2) создает национальный координационный центр по компьютерным инцидентам и утверждает положение о нем;

3) координирует деятельность субъектов критической информационной инфраструктуры по вопросам обнаружения, предупреждения и ликвидации последствий компьютерных атак и реагирования на компьютерные инциденты;

4) организует и проводит оценку безопасности критической информационной инфраструктуры;

5) определяет перечень информации, представляемой в государственную систему обнаружения, предупреждения и ликвидации последствий компьютерных атак на информационные ресурсы Российской Федерации, и порядок ее представления;

6) утверждает порядок информирования федерального органа исполнительной власти, уполномоченного в области обеспечения функционирования государственной системы обнаружения, предупреждения и ликвидации последствий компьютерных атак на информационные ресурсы Российской Федерации, о компьютерных инцидентах, реагирования на них, принятия мер по ликвидации последствий компьютерных атак, проведенных в отношении значимых объектов критической информационной инфраструктуры (в банковской сфере и в иных сферах финансового рынка утверждает указанный порядок по согласованию с Центральным банком Российской Федерации);

7) утверждает порядок обмена информацией о компьютерных инцидентах между субъектами критической информационной инфраструктуры, между субъектами критической информационной инфраструктуры и уполномоченными органами иностранных государств, международными, международными неправительственными организациями и иностранными организациями, осуществляющими деятельность в области реагирования на компьютерные инциденты, а также порядок получения субъектами критической информационной инфраструктуры информации о средствах и способах проведения компьютерных атак и о методах их предупреждения и обнаружения;

8) организует установку на значимых объектах критической информационной инфраструктуры и в сетях электросвязи, используемых для организации взаимодействия объектов критической информационной инфраструктуры, средств, предназначенных для обнаружения, предупреждения и ликвидации последствий компьютерных атак и реагирования на компьютерные инциденты;

9) устанавливает требования к средствам, предназначенным для обнаружения, предупреждения и ликвидации последствий компьютерных атак и реагирования на компьютерные инциденты;

10) утверждает порядок, технические условия установки и эксплуатации средств, предназначенных для обнаружения, предупреждения и ликвидации последствий компьютерных атак и реагирования на компьютерные инциденты, за исключением средств, предназначенных для поиска признаков компьютерных атак в сетях электросвязи, используемых для организации взаимодействия объектов критической информационной инфраструктуры (в банковской сфере и в иных сферах финансового рынка утверждает указанные порядок и технические условия по согласованию с Центральным банком Российской Федерации).

5. Федеральный орган исполнительной власти, осуществляющий функции по выработке и реализации государственной политики и нормативно-правовому регулированию в области связи, утверждает по согласованию с федеральным

органом исполнительной власти, уполномоченным в области обеспечения функционирования государственной системы обнаружения, предупреждения и ликвидации последствий компьютерных атак на информационные ресурсы Российской Федерации, порядок, технические условия установки и эксплуатации средств, предназначенных для поиска признаков компьютерных атак в сетях электросвязи, используемых для организации взаимодействия объектов критической информационной инфраструктуры.

Статья 7. Категорирование объектов критической информационной инфраструктуры

1. Категорирование объекта критической информационной инфраструктуры представляет собой установление соответствия объекта критической информационной инфраструктуры критериям значимости и показателям их значений, присвоение ему одной из категорий значимости, проверку сведений о результатах ее присвоения.

2. Категорирование осуществляется исходя из:

1) социальной значимости, выражающейся в оценке возможного ущерба, причиняемого жизни или здоровью людей, возможности прекращения или нарушения функционирования объектов обеспечения жизнедеятельности населения, транспортной инфраструктуры, сетей связи, а также максимальном времени отсутствия доступа к государственной услуге для получателей такой услуги;

2) политической значимости, выражающейся в оценке возможного причинения ущерба интересам Российской Федерации в вопросах внутренней и внешней политики;

3) экономической значимости, выражающейся в оценке возможного причинения прямого и косвенного ущерба субъектам критической информационной инфраструктуры и (или) бюджетам Российской Федерации;

4) экологической значимости, выражающейся в оценке уровня воздействия на окружающую среду;

5) значимости объекта критической информационной инфраструктуры для обеспечения обороны страны, безопасности государства и правопорядка.

3. Устанавливаются три категории значимости объектов критической информационной инфраструктуры – первая, вторая и третья.

4. Субъекты критической информационной инфраструктуры в соответствии с критериями значимости и показателями их значений, а также порядком осуществления категорирования присваивают одну из категорий значимости принадлежащим им на праве собственности, аренды или ином законном основании объектам критической информационной инфраструктуры. Если объект критической информационной инфраструктуры не соответствует критериям значимости, показателям этих критериев и их значениям, ему не присваивается ни одна из таких категорий.

5. Сведения о результатах присвоения объекту критической информационной инфраструктуры одной из категорий значимости либо об отсутствии необходимости присвоения ему одной из таких категорий субъекты критической информационной инфраструктуры в письменном виде в десятидневный срок со дня принятия ими соответствующего решения направляют в федеральный орган исполнительной власти, уполномоченный в области обеспечения безопасности критической информационной инфраструктуры Российской Федерации, по утвержденной им форме.

6. Федеральный орган исполнительной власти, уполномоченный в области обеспечения безопасности критической информационной инфраструктуры Российской Федерации, в тридцатидневный срок со дня получения сведений, указанных в части 5 настоящей статьи, проверяет соблюдение порядка осуществления категорирования и правильность присвоения объекту критической информационной инфраструктуры одной из категорий значимости либо неприсвоения ему ни одной из таких категорий.

7. В случае, если субъектом критической информационной инфраструктуры соблюден порядок осуществления категорирования и принадлежащему ему на праве собственности, аренды или ином законном основании объекту критической информационной инфраструктуры правильно присвоена одна из категорий значимости, федеральный орган исполнительной власти, уполномоченный в области обеспечения безопасности критической информационной инфраструктуры Российской Федерации, вносит сведения о таком объекте критической информационной инфраструктуры в реестр значимых объектов критической информационной инфраструктуры, о чем в десятидневный срок уведомляется субъект критической информационной инфраструктуры.

8. В случае, если федеральным органом исполнительной власти, уполномоченным в области обеспечения безопасности критической информационной инфраструктуры Российской Федерации, выявлены нарушения порядка осуществления категорирования и (или) объекту критической информационной инфраструктуры, принадлежащему на праве собственности, аренды или ином законном основании субъекту критической информационной инфраструктуры, неправильно присвоена одна из категорий значимости и (или) необоснованно не присвоена ни одна из таких категорий и (или) субъектом критической информационной инфраструктуры представлены неполные и (или) недостоверные сведения о результатах присвоения такому объекту критической информационной инфраструктуры одной из категорий значимости либо об отсутствии необходимости присвоения ему одной из таких категорий, федеральный орган исполнительной власти, уполномоченный в области обеспечения безопасности критической информационной инфраструктуры Российской Федерации, в десятидневный срок со дня поступления представленных сведений возвращает их в письменном виде субъекту критической информационной инфраструктуры с мотивированным обоснованием причин возврата.

9. Субъект критической информационной инфраструктуры после получения мотивированного обоснования причин возврата сведений, указанных в части 5 настоящей статьи, не более чем в десятидневный срок устраняет отмеченные недостатки и повторно направляет такие сведения в федеральный орган исполнительной власти, уполномоченный в области обеспечения безопасности критической информационной инфраструктуры Российской Федерации.

10. Сведения об отсутствии необходимости присвоения объекту критической информационной инфраструктуры одной из категорий значимости после их проверки направляются федеральным органом исполнительной власти, уполномоченным в области обеспечения безопасности критической информационной инфраструктуры Российской Федерации, в государственную систему обнаружения, предупреждения и ликвидации последствий компьютерных атак на информационные ресурсы Российской Федерации,

о чем в десятидневный срок уведомляется субъект критической информационной инфраструктуры.

11. В случае непредставления субъектом критической информационной инфраструктуры сведений, указанных в части 5 настоящей статьи, федеральный орган исполнительной власти, уполномоченный в области обеспечения безопасности критической информационной инфраструктуры Российской Федерации, направляет в адрес указанного субъекта требование о необходимости соблюдения положений настоящей статьи.

12. Категория значимости, к которой отнесен значимый объект критической информационной инфраструктуры, может быть изменена в порядке, предусмотренном для категорирования, в следующих случаях:

1) по мотивированному решению федерального органа исполнительной власти, уполномоченного в области обеспечения безопасности критической информационной инфраструктуры Российской Федерации, принятому по результатам проверки, проведенной в рамках осуществления государственного контроля в области обеспечения безопасности значимых объектов критической информационной инфраструктуры;

2) в случае изменения значимого объекта критической информационной инфраструктуры, в результате которого такой объект перестал соответствовать критериям значимости и показателям их значений, на основании которых ему была присвоена определенная категория значимости;

3) в связи с ликвидацией, реорганизацией субъекта критической информационной инфраструктуры и (или) изменением его организационно-правовой формы, в результате которых были изменены либо утрачены признаки субъекта критической информационной инфраструктуры.

Статья 8. Реестр значимых объектов критической информационной инфраструктуры

1. В целях учета значимых объектов критической информационной инфраструктуры федеральный орган исполнительной власти, уполномоченный в области обеспечения безопасности критической информационной инфраструктуры Российской Федерации, ведет реестр значимых объектов критической информационной инфраструктуры в установленном им порядке. В данный реестр вносятся следующие сведения:

1) наименование значимого объекта критической информационной инфраструктуры;

2) наименование субъекта критической информационной инфраструктуры;

3) сведения о взаимодействии значимого объекта критической информационной инфраструктуры и сетей электросвязи;

4) сведения о лице, эксплуатирующем значимый объект критической информационной инфраструктуры;

5) категория значимости, которая присвоена значимому объекту критической информационной инфраструктуры;

6) сведения о программных и программно-аппаратных средствах, используемых на значимом объекте критической информационной инфраструктуры;

7) меры, применяемые для обеспечения безопасности значимого объекта критической информационной инфраструктуры.

2. Сведения из реестра значимых объектов критической информационной инфраструктуры направляются в государственную систему обнаружения,

предупреждения и ликвидации последствий компьютерных атак на информационные ресурсы Российской Федерации.

3. В случае утраты значимым объектом критической информационной инфраструктуры категории значимости он исключается федеральным органом исполнительной власти, уполномоченным в области обеспечения безопасности критической информационной инфраструктуры Российской Федерации, из реестра значимых объектов критической информационной инфраструктуры.

Статья 9. Права и обязанности субъектов критической информационной инфраструктуры

1. Субъекты критической информационной инфраструктуры имеют право:

1) получать от федерального органа исполнительной власти, уполномоченного в области обеспечения безопасности критической информационной инфраструктуры Российской Федерации, информацию, необходимую для обеспечения безопасности значимых объектов критической информационной инфраструктуры, принадлежащих им на праве собственности, аренды или ином законном основании, в том числе об угрозах безопасности обрабатываемой такими объектами информации и уязвимости программного обеспечения, оборудования и технологий, используемых на таких объектах;

2) в порядке, установленном федеральным органом исполнительной власти, уполномоченным в области обеспечения функционирования государственной системы обнаружения, предупреждения и ликвидации последствий компьютерных атак на информационные ресурсы Российской Федерации, получать от указанного органа информацию о средствах и способах проведения компьютерных атак, а также о методах их предупреждения и обнаружения;

3) при наличии согласия федерального органа исполнительной власти, уполномоченным в области обеспечения функционирования государственной системы обнаружения, предупреждения и ликвидации последствий компьютерных атак на информационные ресурсы Российской Федерации, за свой счет приобретать, арендовать, устанавливать и обслуживать средства, предназначенные для обнаружения, предупреждения и ликвидации последствий компьютерных атак и реагирования на компьютерные инциденты;

4) разрабатывать и осуществлять мероприятия по обеспечению безопасности значимого объекта критической информационной инфраструктуры.

2. Субъекты критической информационной инфраструктуры обязаны:

1) незамедлительно информировать о компьютерных инцидентах федеральный орган исполнительной власти, уполномоченный в области обеспечения функционирования государственной системы обнаружения, предупреждения и ликвидации последствий компьютерных атак на информационные ресурсы Российской Федерации, а также Центральный банк Российской Федерации (в случае, если субъект критической информационной инфраструктуры осуществляет деятельность в банковской сфере и в иных сферах финансового рынка) в установленном указанным федеральным органом исполнительной власти порядке (в банковской сфере и в иных сферах финансового рынка указанный порядок устанавливается по согласованию с Центральным банком Российской Федерации);

2) оказывать содействие должностным лицам федерального органа исполнительной власти, уполномоченного в области обеспечения функционирования государственной системы обнаружения, предупреждения и ликвидации последствий компьютерных атак на информационные ресурсы Российской

Федерации, в обнаружении, предупреждении и ликвидации последствий компьютерных атак, установлении причин и условий возникновения компьютерных инцидентов;

3) в случае установки на объектах критической информационной инфраструктуры средств, предназначенных для обнаружения, предупреждения и ликвидации последствий компьютерных атак и реагирования на компьютерные инциденты, обеспечивать выполнение порядка, технических условий установки и эксплуатации таких средств, их сохранность.

3. Субъекты критической информационной инфраструктуры, которым на праве собственности, аренды или ином законном основании принадлежат значимые объекты критической информационной инфраструктуры, наряду с выполнением обязанностей, предусмотренных частью 2 настоящей статьи, также обязаны:

1) соблюдать требования по обеспечению безопасности значимых объектов критической информационной инфраструктуры, установленные федеральным органом исполнительной власти, уполномоченным в области обеспечения безопасности критической информационной инфраструктуры Российской Федерации;

2) выполнять предписания должностных лиц федерального органа исполнительной власти, уполномоченного в области обеспечения безопасности критической информационной инфраструктуры Российской Федерации, об устранении нарушений в части соблюдения требований по обеспечению безопасности значимого объекта критической информационной инфраструктуры, выданные этими лицами в соответствии со своей компетенцией;

3) реагировать на компьютерные инциденты в порядке, утвержденном федеральным органом исполнительной власти, уполномоченным в области обеспечения функционирования государственной системы обнаружения, предупреждения и ликвидации последствий компьютерных атак на информационные ресурсы Российской Федерации, принимать меры по ликвидации последствий компьютерных атак, проведенных в отношении значимых объектов критической информационной инфраструктуры;

4) обеспечивать беспрепятственный доступ должностным лицам федерального органа исполнительной власти, уполномоченного в области обеспечения безопасности критической информационной инфраструктуры Российской Федерации, к значимым объектам критической информационной инфраструктуры при реализации этими лицами полномочий, предусмотренных статьей 13 настоящего Федерального закона.

Статья 10. Система безопасности значимого объекта критической информационной инфраструктуры

1. В целях обеспечения безопасности значимого объекта критической информационной инфраструктуры субъект критической информационной инфраструктуры в соответствии с требованиями к созданию систем безопасности таких объектов и обеспечению их функционирования, утвержденными федеральным органом исполнительной власти, уполномоченным в области обеспечения безопасности критической информационной инфраструктуры Российской Федерации, создает систему безопасности такого объекта и обеспечивает ее функционирование.

2. Основными задачами системы безопасности значимого объекта критической информационной инфраструктуры являются:

1) предотвращение неправомерного доступа к информации, обрабатываемой значимым объектом критической информационной инфраструктуры, уничтожения такой информации, ее модифицирования, блокирования, копирования, предоставления и распространения, а также иных неправомерных действий в отношении такой информации;

2) недопущение воздействия на технические средства обработки информации, в результате которого может быть нарушено и (или) прекращено функционирование значимого объекта критической информационной инфраструктуры;

3) восстановление функционирования значимого объекта критической информационной инфраструктуры, обеспечиваемого в том числе за счет создания и хранения резервных копий необходимой для этого информации;

4) непрерывное взаимодействие с государственной системой обнаружения, предупреждения и ликвидации последствий компьютерных атак на информационные ресурсы Российской Федерации.

Статья 11. Требования по обеспечению безопасности значимых объектов критической информационной инфраструктуры

1. Требования по обеспечению безопасности значимых объектов критической информационной инфраструктуры, устанавливаемые федеральным органом исполнительной власти, уполномоченным в области обеспечения безопасности критической информационной инфраструктуры Российской Федерации, дифференцируются в зависимости от категории значимости объектов критической информационной инфраструктуры и этими требованиями предусматриваются:

1) планирование, разработка, совершенствование и осуществление внедрения мероприятий по обеспечению безопасности значимых объектов критической информационной инфраструктуры;

2) принятие организационных и технических мер для обеспечения безопасности значимых объектов критической информационной инфраструктуры;

3) установление параметров и характеристик программных и программно-аппаратных средств, применяемых для обеспечения безопасности значимых объектов критической информационной инфраструктуры.

2. Государственные органы и российские юридические лица, выполняющие функции по разработке, проведению или реализации государственной политики и (или) нормативно-правовому регулированию в установленной сфере деятельности, по согласованию с федеральным органом исполнительной власти, уполномоченным в области обеспечения безопасности критической информационной инфраструктуры Российской Федерации, могут устанавливать дополнительные требования по обеспечению безопасности значимых объектов критической информационной инфраструктуры, содержащие особенности функционирования таких объектов в установленной сфере деятельности.

Статья 12. Оценка безопасности критической информационной инфраструктуры

1. Оценка безопасности критической информационной инфраструктуры осуществляется федеральным органом исполнительной власти, уполномоченным в области обеспечения функционирования государственной системы обнаружения, предупреждения и ликвидации последствий компьютерных атак на информационные ресурсы Российской Федерации, в целях прогнозирова-

ния возникновения возможных угроз безопасности критической информационной инфраструктуры и выработки мер по повышению устойчивости ее функционирования при проведении в отношении ее компьютерных атак.

2. При осуществлении оценки безопасности критической информационной инфраструктуры проводится анализ:

1) данных, получаемых при использовании средств, предназначенных для обнаружения, предупреждения и ликвидации последствий компьютерных атак и реагирования на компьютерные инциденты, в том числе информации о наличии в сетях электросвязи, используемых для организации взаимодействия объектов критической информационной инфраструктуры, признаков компьютерных атак;

2) информации, представляемой субъектами критической информационной инфраструктуры и федеральным органом исполнительной власти, уполномоченным в области обеспечения безопасности критической информационной инфраструктуры Российской Федерации, в соответствии с перечнем информации и в порядке, определяемыми федеральным органом исполнительной власти, уполномоченным в области обеспечения функционирования государственной системы обнаружения, предупреждения и ликвидации последствий компьютерных атак на информационные ресурсы Российской Федерации, а также иными не являющимися субъектами критической информационной инфраструктуры органами и организациями, в том числе иностранными и международными;

3) сведений, представляемых в государственную систему обнаружения, предупреждения и ликвидации последствий компьютерных атак на информационные ресурсы Российской Федерации по итогам проведения государственного контроля в области обеспечения безопасности значимых объектов критической информационной инфраструктуры, о нарушении требований по обеспечению безопасности значимых объектов критической информационной инфраструктуры, в результате которого создаются предпосылки возникновения компьютерных инцидентов;

4) иной информации, получаемой федеральным органом исполнительной власти, уполномоченным в области обеспечения функционирования государственной системы обнаружения, предупреждения и ликвидации последствий компьютерных атак на информационные ресурсы Российской Федерации, в соответствии с законодательством Российской Федерации.

3. Для реализации положений, предусмотренных частями 1 и 2 настоящей статьи, федеральный орган исполнительной власти, уполномоченный в области обеспечения функционирования государственной системы обнаружения, предупреждения и ликвидации последствий компьютерных атак на информационные ресурсы Российской Федерации, организует установку в сетях электросвязи, используемых для организации взаимодействия объектов критической информационной инфраструктуры, средств, предназначенных для поиска признаков компьютерных атак в таких сетях электросвязи.

4. В целях разработки мер по совершенствованию безопасности критической информационной инфраструктуры федеральный орган исполнительной власти, уполномоченный в области обеспечения функционирования государственной системы обнаружения, предупреждения и ликвидации последствий компьютерных атак на информационные ресурсы Российской Федерации, направляет в федеральный орган исполнительной власти, уполномоченный в области обеспечения безопасности критической информационной инфраструк-

туры Российской Федерации, результаты осуществления оценки безопасности критической информационной инфраструктуры.

Статья 13. Государственный контроль в области обеспечения безопасности значимых объектов критической информационной инфраструктуры

1. Государственный контроль в области обеспечения безопасности значимых объектов критической информационной инфраструктуры проводится в целях проверки соблюдения субъектами критической информационной инфраструктуры, которым на праве собственности, аренды или ином законном основании принадлежат значимые объекты критической информационной инфраструктуры, требований, установленных настоящим Федеральным законом и принятыми в соответствии с ним нормативными правовыми актами. Указанный государственный контроль проводится путем осуществления федеральным органом исполнительной власти, уполномоченным в области обеспечения безопасности критической информационной инфраструктуры Российской Федерации, плановых или внеплановых проверок.

2. Основанием для осуществления плановой проверки является истечение трех лет со дня:

1) внесения сведений об объекте критической информационной инфраструктуры в реестр значимых объектов критической информационной инфраструктуры;

2) окончания осуществления последней плановой проверки в отношении значимого объекта критической информационной инфраструктуры.

3. Основанием для осуществления внеплановой проверки является:

1) истечение срока выполнения субъектом критической информационной инфраструктуры выданного федеральным органом исполнительной власти, уполномоченным в области обеспечения безопасности критической информационной инфраструктуры Российской Федерации, предписания об устранении выявленного нарушения требований по обеспечению безопасности значимых объектов критической информационной инфраструктуры;

2) возникновение компьютерного инцидента, повлекшего негативные последствия, на значимом объекте критической информационной инфраструктуры;

3) приказ (распоряжение) руководителя федерального органа исполнительной власти, уполномоченного в области обеспечения безопасности критической информационной инфраструктуры Российской Федерации, изданный в соответствии с поручением Президента Российской Федерации или Правительства Российской Федерации либо на основании требования прокурора об осуществлении внеплановой проверки в рамках проведения надзора за исполнением законов по поступившим в органы прокуратуры материалам и обращениям.

4. По итогам плановой или внеплановой проверки федеральным органом исполнительной власти, уполномоченным в области обеспечения безопасности критической информационной инфраструктуры Российской Федерации, составляется акт проверки по утвержденной указанным органом форме.

5. На основании акта проверки в случае выявления нарушения требований настоящего Федерального закона и принятых в соответствии с ним нормативных правовых актов по обеспечению безопасности значимых объектов критической информационной инфраструктуры федеральный орган исполнительной власти, уполномоченный в области обеспечения безопас-

ности критической информационной инфраструктуры Российской Федерации, выдает субъекту критической информационной инфраструктуры предписание об устранении выявленного нарушения с указанием сроков его устранения.

Статья 14. Ответственность за нарушение требований настоящего Федерального закона и принятых в соответствии с ним иных нормативных правовых актов

Нарушение требований настоящего Федерального закона и принятых в соответствии с ним иных нормативных правовых актов влечет за собой ответственность в соответствии с законодательством Российской Федерации.

Статья 15. Вступление в силу настоящего Федерального закона

Настоящий Федеральный закон вступает в силу с 1 января 2018 года.

Развитие информационно-
коммуникационного сотрудничества
на пространстве ОДКБ

Редактор В. В. Нарбут
Корректор Т. Д. Романосова
Технический редактор Л. А. Дерр

Оригинал-макет подготовлен
ООО «Новосибирский издательский дом»
630048, г. Новосибирск, ул. Немировича-Данченко, 104

Подписано в печать 09.09.2019
Формат 70x100/16. Печ. л. 7,0. Печать офсетная. Тираж 300 экз. Заказ № 799

Отпечатано с оригинал-макета: ИП Мочалов С. В.
162626, Вологодская область, г. Череповец, ул. Сергея Перца, 3