П О С Т А Н О В Л Е Н И Е

Парламентской Ассамблеи
Организации Договора о коллективной безопасности

О Рекомендациях для государств – членов ОДКБ по выработке общих принципов государственного регулирования сети Интернет в целях обеспечения национальной безопасности

Парламентская Ассамблея Организации Договора о коллективной безопасности п о с т а н о в л я е т:

1. Принять Рекомендации для государств – членов ОДКБ по выработке общих принципов государственного регулирования сети Интернет в целях обеспечения национальной безопасности (далее – Рекомендации) (прилагаются).

2. Направить Рекомендации в парламенты государств – членов ОДКБ для использования в работе по совершенствованию законодательства государств – членов Организации в соответствующей сфере.

3. Опубликовать текст Рекомендаций на официальном сайте и в материалах Парламентской Ассамблеи ОДКБ.

Председатель
Парламентской Ассамблеи ОДКБ **В.В.ВОЛОДИН**

Москва
9 декабря 2024 года
№ 17-7.2

Приложение
к постановлению ПА ОДКБ
от 9 декабря 2024 года № 17-7.2

Рекомендации
для государств – членов ОДКБ по выработке общих принципов государственного регулирования сети Интернет в целях обеспечения национальной безопасности

Национальная безопасность государства предполагает поддержание необходимого уровня безопасности в соответствующих сегментах общественных отношений (экономика, наука, образование, информационная сфера и др.).

С учетом зависимости современного общества от информационных технологий следует отметить, что информация, распространяемая в сети Интернет, существенным образом влияет на общественное и индивидуальное сознание граждан государств, в том числе государств – членов ОДКБ, на стабильность социально-политической системы государств. Соответственно, государства – члены ОДКБ не могут оставить без внимания столь важную для обеспечения национальной безопасности область общественных отношений. В связи с обеспечением коллективной безопасности представляется целесообразным выработать общие подходы к вопросам государственного регулирования сети Интернет, которые позволят укрепить сотрудничество государств – членов ОДКБ в противодействии угрозам национальной безопасности, создаваемым различными субъектами (злоумышленниками) с использованием сети Интернет.

Обращает на себя внимание комплексность и масштабность отношений, связанных с государственным регулированием сети Интернет. К ключевым отношениям в целях обеспечения национальной безопасности следует отнести: 1) противодействие терроризму; 2) противодействие экстремизму; 3) противодействие угрозам в военной сфере. Критерием выделения названных групп отношений является характер угроз коллективной и национальной безопасности государств – членов ОДКБ в сети Интернет.

В качестве примера можно привести перечень угроз информационной безопасности, закрепленный в пункте 8 «Основ государственной политики Российской Федерации в области международной информационной безопасности», утвержденных Указом Президента Российской Федерации от 12 апреля 2021 года № 213:

использование информационно-коммуникационных технологий в военно-политической и иных сферах в целях подрыва (ущемления) суверенитета, нарушения территориальной целостности государств, осуществления в глобальном информационном пространстве иных действий, препятствующих поддержанию международного мира, безопасности и стабильности;

использование информационно-коммуникационных технологий в террористических целях, в том числе для пропаганды терроризма и привлечения к террористической деятельности новых сторонников;

использование информационно-коммуникационных технологий в экстремистских целях, а также для вмешательства во внутренние дела суверенных государств;

использование информационно-коммуникационных технологий в преступных целях, в том числе для совершения преступлений в сфере компьютерной информации, а также для совершения различных видов мошенничества;

использование информационно-коммуникационных технологий для проведения компьютерных атак на информационные ресурсы государств, в том числе на критическую информационную инфраструктуру;

использование отдельными государствами технологического доминирования в глобальном информационном пространстве для монополизации рынка информационно-коммуникационных технологий, ограничения доступа других государств к передовым информационно-коммуникационным технологиям, а также для усиления их технологической зависимости от доминирующих в сфере информатизации государств и информационного неравенства.

Целью настоящих Рекомендаций является сближение и гармонизация законодательства государств – членов ОДКБ в сфере государственного регулирования сети Интернет для обеспечения национальной безопасности.

Нормативное регулирование сети Интернет в целях обеспечения национальной безопасности государств – членов ОДКБ

В ОДКБ по вопросам обеспечения информационной безопасности были приняты: Соглашение о сотрудничестве государств – членов Организации Договора о коллективной безопасности в области обеспечения информационной безопасности (30 ноября 2017 года), Концепция сближения и гармонизации законодательства государств – членов Организации Договора о коллективной безопасности в сфере коллективной безопасности (3 декабря 2009 года), модельный закон ОДКБ «Об информационной безопасности» (29 ноября 2021 года).

Оценивая степень разработанности правового регулирования государств – членов ОДКБ в сфере Интернета, имеет смысл выделять общее регулирование, предмет которого составляют отношения, складывающиеся в сфере Интернета государств – членов ОДКБ, и специальное регулирование, предметная область которого представляет собой отношения в области обеспечения национальной безопасности, противодействия терроризму и экстремизму, введения режима военного положения и противодействия разглашению государственной тайны (государственных секретов).

Республика Армения. Основными законами Республики Армения, регулирующими складывающиеся отношения в сети Интернет, являются Закон Республики Армения от 13 августа 2005 года № ЗР-176 «Об электронной связи» и Закон Республики Армения от 4 мая 2007 года № ЗР-172 «О публичном и персональном уведомлении через Интернет». Анализ указанных законов свидетельствует о том, что вопросы, связанные с противодействием терроризму, экстремизму и разглашению сведений, составляющих государственную тайну (государственные секреты) в сети Интернет, не нашли своего отражения в их тексте.

Вопросы противодействия терроризму и экстремизму в Республике Армения, введения режима военного положения, а также защиты государственной тайны рассматриваются в Законе Республики Армения от 19 апреля 2005 года № ЗР-79 «О борьбе с терроризмом», Законе Республики Армения от 21 июня 2008 года № ЗР-80 «О борьбе с отмыванием денег и финансированием терроризма», Законе Республики Армения от 29 декабря 2006 года № ЗР-258 «О правовом режиме военного положения», Законе Республики Армения от 30 декабря 1996 года № ЗР-94 «О государственной и служебной тайне», Законе Республики Армения от 24 марта 2023 года № ЗР-49 «О государственной тайне».

Законом Республики Армения от 13 августа 2005 года № ЗР-176 «Об электронной связи» предусматриваются функции компетентного государственного органа по эксплуатации всех сетей или служб электронной связи в случае объявления военного положения.

В остальном обозначенное выше профильное законодательство не устанавливает особенности использования сети Интернет в контексте рассматриваемых отношений по обеспечению национальной безопасности Республики Армения.

Республика Беларусь. Отношения, складывающиеся в сети Интернет, в Республике Беларусь урегулированы Законом Республики Беларусь от 10 ноября 2008 года № 455-З «Об информации, информатизации и защите информации». По большей части в указанном законе Интернет рассматривается в качестве своеобразной электронной площадки, которую государственные органы Республики Беларусь используют для размещения общедоступной информации.

В Республике Беларусь регулирование отношений в сети Интернет преимущественно носит подзаконный характер. В числе ключевых подзаконных актов следует выделить такие, как Указ Президента Республики Беларусь от 1 февраля 2010 года № 60 «О мерах по совершенствованию использования национального сегмента сети Интернет», Указ Президента Республики Беларусь от 18 сентября 2019 года № 350 «Об особенностях использования национального сегмента сети Интернет».

Общие принципы государственного регулирования сети Интернет в целях обеспечения национальной безопасности изложены в постановлении

Совета Безопасности Республики Беларусь от 18 марта 2019 года № 1 «О Концепции информационной безопасности Республики Беларусь».

Статьями 38, 51, 51[1] Закона Республики Беларусь от 17 июля 2008 года № 427-З «О средствах массовой информации» закреплен перечень информации, распространение которой в средствах массовой информации, на интернет-ресурсах, в новостных агрегаторах запрещено, а также регламентированы порядок ограничения доступа к интернет-ресурсу, сетевому изданию, новостному агрегатору и порядок прекращения выпуска средства массовой информации.

Отношения, связанные с противодействием терроризму и экстремизму, введением режима военного положения, а также с защитой государственных секретов, регулируются в Республике Беларусь следующими законами и подзаконными нормативными правовыми актами: Законом Республики Беларусь от 3 января 2002 года № 77-З «О борьбе с терроризмом», Законом Республики Беларусь от 4 января 2007 года № 203-З «О противодействии экстремизму», Постановлением Совета Министров Республики Беларусь от 12 октября 2021 года № 575 «О мерах противодействия экстремизму и реабилитации нацизма», Законом Республики Беларусь от 13 января 2003 года № 185-З «О военном положении», Постановлением Совета Министров Республики Беларусь от 4 августа 2006 года № 1010 «Об утверждении Положения о порядке приоритетного использования, приостановки или ограничения использования сетей и средств электросвязи при возникновении чрезвычайных ситуаций, введении чрезвычайного или военного положения», Законом Республики Беларусь от 19 июля 2010 года № 170-З «О государственных секретах».

В Постановлении Совета Министров Республики Беларусь от 12 октября 2021 года № 575 «О мерах противодействия экстремизму и реабилитации нацизма» определяется, что субъекты противодействия реабилитации нацизма осуществляют мониторинг соблюдения законодательства в части недопущения реабилитации нацизма владельцами интернет-ресурсов. В соответствии с указанным постановлением в Республике Беларусь осуществляется оценка символики и атрибутики, информационной продукции (в том числе материалов сети Интернет) на предмет наличия (отсутствия) в них признаков проявления экстремизма, что также является составной частью механизма обеспечения безопасности в сети Интернет.

В Законе Республики Беларусь от 13 января 2003 года № 185-З «О военном положении» устанавливается, что сети электросвязи являются объектом военной цензуры.

Также имеет смысл привести ряд реализованных законодательных инициатив, свидетельствующих о качестве и полноте законодательного регулирования информационных отношений в сети Интернет, направленных на поддержание надлежащего уровня национальной безопасности: Закон Республики Беларусь от 14 мая 2021 года № 103-З «О недопущении реабилитации нацизма», Закон Республики Беларусь от 30 июня 2014 года №

165-З «О мерах по предотвращению легализации доходов, полученных преступным путем, финансирования террористической деятельности и финансирования распространения оружия массового поражения», Указ Президента Республики Беларусь от 22 марта 2022 года № 116 «О новостных агрегаторах в глобальной компьютерной сети Интернет», Указ Президента Республики Беларусь от 29 августа 2023 года № 269 «О мерах по противодействию несанкционированным платежным операциям», Постановление Совета Министров Республики Беларусь от 23 апреля 2007 года № 513 «О ведении и опубликовании республиканского списка экстремистских материалов» и др.

Республика Казахстан. Отношения, складывающиеся в сети Интернет, в Республике Казахстан урегулированы Законом Республики Казахстан от 16 ноября 2015 года № 401-V ЗРК «О доступе к информации», Законом Республики Казахстан от 24 ноября 2015 года № 418-V ЗРК «Об информатизации», приказом Министра информации и общественного развития Республики Казахстан от 6 сентября 2022 года № 366 «Об утверждении Правил возобновления доступа к интернет-ресурсу».

Закон Республики Казахстан от 16 ноября 2015 года № 401-V ЗРК «О доступе к информации» предусматривает обязанность обладателя информации соблюдать законодательство Республики Казахстан о государственных секретах и иные охраняемые законом тайны.

Закон Республики Казахстан от 24 ноября 2015 года № 418-V ЗРК «Об информатизации» к числу основных задач государственного управления в сфере информатизации относит предупреждение и оперативное реагирование на инциденты информационной безопасности, в том числе в условиях введения военного положения. Этим же законом закрепляется правовой режим создания, приобретения, накапливания, формирования, регистрации, хранения, обработки, уничтожения, использования, передачи, защиты электронных информационных ресурсов, содержащих сведения, составляющие государственные секреты.

Таким образом, ряд отношений, непосредственно связанных с обеспечением национальной безопасности Республики Казахстан, находят свое отражение в законодательстве, регулирующем общие отношения, складывающиеся в сети Интернет, что отличает подход Республики Казахстан от подхода, который имеет место в Республике Армения.

Отношения, связанные с вопросами противодействия терроризму и экстремизму в Республике Казахстан, введения режима военного положения, а также с защитой государственной тайны (государственных секретов) в сети Интернет, урегулированы Законом Республики Казахстан от 13 июля 1999 года № 416-I «О противодействии терроризму», Законом Республики Казахстан от 28 августа 2009 года № 191-IV ЗРК «О противодействии легализации (отмыванию) доходов, полученных преступным путем, и финансированию терроризма», Законом Республики Казахстан от 18 февраля 2005 года № 31-III ЗРК «О противодействии экстремизму», Законом

Республики Казахстан от 5 марта 2003 года № 391-II «О военном положении», Законом Республики Казахстан от 15 марта 1999 года № 349-I «О государственных секретах».

Перечисленные законы не содержат в себе положений, посвященных регулированию сети Интернет, помимо законов о противодействии терроризму и экстремизму, согласно которым информация о лицах, причастных к осуществлению террористической и экстремистской деятельности, публикуется соответствующими государственными органами республики в сети Интернет (на их официальных сайтах).

Кыргызская Республика. Отношения, складывающиеся в сети Интернет, в Кыргызской Республике регулируются Законом Кыргызской Республики от 23 августа 2021 года № 101 «О защите от недостоверной (ложной) информации», Постановлением Кабинета Министров Кыргызской Республики от 8 апреля 2022 года № 204 «Об утверждении Порядка обжалования действий владельца сайта или страницы сайта, удаления недостоверной (ложной) информации и приостановления работы сайта или страницы сайта в связи с распространением недостоверной (ложной) информации в сети Интернет».

Законом Кыргызской Республики от 23 августа 2021 года № 101 «О защите от недостоверной (ложной) информации» устанавливается, что распространение недостоверной (ложной) информации в интернет-пространстве Кыргызской Республики не допускается.

Вопросы противодействия терроризму и экстремизму, введения режима военного положения, а также защиты государственной тайны (государственных секретов) урегулированы в Кыргызской Республике Законом Кыргызской Республики от 6 августа 2018 года № 87 «О противодействии финансированию террористической деятельности и легализации (отмыванию) преступных доходов», Законом Кыргызской Республики от 4 июля 2022 года № 55 «О противодействии терроризму», Постановлением Кабинета Министров Кыргызской Республики от 15 марта 2023 года № 141 «Об утверждении Программы Кабинета Министров Кыргызской Республики по противодействию экстремизму и терроризму на 2023–2027 годы», Законом Кыргызской Республики от 24 февраля 2023 года № 40 «О противодействии экстремистской деятельности», Конституционным Законом Кыргызской Республики от 30 апреля 2009 года № 149 «О военном положении», Законом Кыргызской Республики от 15 декабря 2017 года № 210 «О защите государственных секретов Кыргызской Республики».

В частности, Законом Кыргызской Республики от 4 июля 2022 года № 55 «О противодействии терроризму» предусматривается, что публичные призывы к осуществлению террористической деятельности или публичное оправдание терроризма, в том числе с использованием средств массовой информации или сети Интернет, относятся к террористической деятельности.

Постановлением Кабинета Министров Кыргызской Республики от 15 марта 2023 года № 141 «Об утверждении Программы Кабинета Министров

Кыргызской Республики по противодействию экстремизму и терроризму на 2023–2027 годы» определено, что в целях повышения эффективности работа уполномоченных государственных органов по противодействию экстремистской и террористической деятельности должна быть направлена на формирование эффективной системы предупреждения и пресечения распространения идей экстремизма и терроризма через информационно-коммуникационную сеть Интернет.

Законом Кыргызской Республики от 24 февраля 2023 года № 40 «О противодействии экстремистской деятельности» закреплена обязанность государственных органов исполнительной власти осуществлять мониторинг пространства сети Интернет с целью недопущения распространения в данной сети экстремистских материалов.

Российская Федерация. Отношения, возникающие и развивающиеся в сети Интернет, в Российской Федерации регулируются Федеральным законом Российской Федерации от 27 июля 2006 года № 149-ФЗ «Об информации, информационных технологиях и о защите информации», Постановлением Правительства Российской Федерации от 26 октября 2012 года № 1101 «О единой автоматизированной информационной системе “Единый реестр доменных имен, указателей страниц сайтов в информационно-телекоммуникационной сети “Интернет” и сетевых адресов, позволяющих идентифицировать сайты в информационно-телекоммуникационной сети “Интернет”, содержащие информацию, распространение которой в Российской Федерации запрещено”», Федеральным законом Российской Федерации от 1 мая 2019 года № 90-ФЗ «О внесении изменений в Федеральный закон “О связи” и Федеральный закон “Об информации, информационных технологиях и о защите информации”».

Федеральным законом Российской Федерации от 27 июля 2006 года № 149-ФЗ «Об информации, информационных технологиях и о защите информации» установлен запрет на разглашение новостными агрегаторами, владельцами аудиовизуальных сервисов, пользователями социальных сетей, владельцами сервисов размещения объявлений сведений, составляющих государственную тайну, а также на распространение этими субъектами в сети Интернет призывов к осуществлению террористической деятельности или публично оправдывающих терроризм экстремистских материалов.

Этим же законом устанавливается порядок ограничения доступа к информации, распространяемой с нарушением закона (призывы к терроризму, экстремизму и другая противозаконная активность).

Правовое регулирование вопросов противодействия терроризму и экстремизму, введения режима военного положения, защиты государственной тайны представлено в Российской Федерации Федеральным законом Российской Федерации от 6 марта 2006 года № 35-ФЗ «О противодействии терроризму», Федеральным законом Российской Федерации от 25 июля 2002 года № 114-ФЗ «О противодействии экстремистской деятельности», Федеральным конституционным законом Российской Федерации от 30 января

2002 года № 1-ФКЗ «О военном положении», Законом Российской Федерации от 21 июля 1993 года № 5485-1 «О государственной тайне».

Согласно Федеральному закону Российской Федерации от 6 марта 2006 года № 35-ФЗ «О противодействии терроризму» на территории (объектах), в пределах которой (на которых) введен правовой режим контртеррористической операции, в порядке, предусмотренном законодательством Российской Федерации, на период проведения контртеррористической операции допускается приостановление оказания услуг связи юридическим и физическим лицам или ограничение использования сетей связи и средств связи.

В соответствии с Федеральным законом Российской Федерации от 25 июля 2002 года № 114-ФЗ «О противодействии экстремистской деятельности» перечень общественных и религиозных объединений, деятельность которых приостановлена в связи с осуществлением ими экстремистской деятельности, подлежит размещению в информационно-телекоммуникационной сети «Интернет» на сайте федерального органа государственной регистрации.

В рамках обозначенных выше вопросов представляет интерес механизм взаимодействия с зарубежными интернет-компаниями, направленный на соблюдение ими положений российского законодательства, закрепленный в Федеральном законе от 1 июля 2021 № 236-ФЗ «О деятельности иностранных лиц в информационно-телекоммуникационной сети “Интернет” на территории Российской Федерации».

Республика Таджикистан. Отношения, формирующиеся и развивающиеся в сети Интернет, в Республике Таджикистан урегулированы подзаконным нормативным правовым актом – Правилами предоставления услуг Интернет на территории Республики Таджикистан (утверждены Постановлением Правительства Республики Таджикистан от 8 августа 2001 года № 389). Указанными Правилами устанавливается обязанность абонента не использовать сеть передачи данных для передачи сведений, составляющих государственную и иную охраняемую законом тайну.

Вопросы противодействия терроризму и экстремизму, введения режима военного положения, а также защиты государственной тайны нашли свое отражение в Законе Республики Таджикистан от 23 декабря 2021 года № 1808 «О противодействии терроризму», Законе Республики Таджикистан от 2 января 2020 года № 1655 «О противодействии экстремизму», Законе Республики Таджикистан от 20 июня 2019 года № 1608 «О военном положении», Законе Республики Таджикистан от 26 июля 2014 года № 1095 «О государственных секретах».

На основании Закона Республики Таджикистан от 23 декабря 2021 года № 1808 «О противодействии терроризму» при обнаружении в информационно-телекоммуникационных сетях, в том числе в сети Интернет, информации, содержащей призывы к массовым беспорядкам, осуществлению экстремистской и террористической деятельности, участию в массовых мероприятиях, проводимых с нарушением установленного законодательством

порядка, а также пропагандирующих экстремизм и терроризм, доступ к таким материалам ограничивается.

В соответствии с Законом Республики Таджикистан от 2 января 2020 года № 1655 «О противодействии экстремизму» служба связи при Правительстве Республики Таджикистан в сфере противодействия экстремизму проводит мониторинг всех услуг связи Интернета, в том числе социальных сетей, и при необходимости предотвращения экстремистской деятельности ограничивает или приостанавливает деятельность данных сетей (интернет-провайдеров), а также обязует физических лиц и юридические лица, которые осуществляют деятельность по предоставлению услуг связи, в том числе интернет-провайдеров, обеспечить до шести месяцев хранение информации экстремистского характера на своих серверах.

Таким образом, законодательство государств – членов ОДКБ в части правового регулирования сети Интернет для целей обеспечения национальной безопасности представляется недостаточно целостным и системным. Ни в одном из государств – членов ОДКБ не сформирована такая система нормативных правовых актов, которая с необходимой степенью детальности регулировала бы все возможные группы информационных отношений в сети Интернет, касающихся поддержания надлежащего уровня национальной безопасности.

Существующее нормативное регулирование также демонстрирует различные подходы государств – членов ОДКБ к пределам государственного вмешательства в сетевые отношения.

Анализ государственного регулирования сети Интернет в государствах – членах ОДКБ в целях обеспечения национальной безопасности по направлению «противодействие терроризму и экстремизму»

В Республике Армения был принят Закон Республики Армения от 19 апреля 2005 года № ЗР-79 «О борьбе с терроризмом», однако каких-либо положений о том, каким образом должна быть урегулирована сеть Интернет для целей противодействия терроризму (пропаганде и оправданию террористической активности) на территории республики, он не содержит.

Закон, направленный на противодействие экстремизму, в Республике Армения принят не был.

В Республике Беларусь был принят Закон Республики Беларусь от 3 января 2002 года № 77-З «О борьбе с терроризмом». Он не содержит норм о регулировании сети Интернет в части противодействия террористическим угрозам, направленным против республики.

Вместе с тем было принято Постановление Совета Министров Республики Беларусь от 25 июля 2013 года № 658 «Об утверждении Концепции борьбы с терроризмом в Республике Беларусь».

В пункте 4 главы 1 указанной Концепции зафиксировано, что усиление влияния средств массовой информации и глобальных коммуникационных механизмов на экономическую, политическую и социальную обстановку в мире создает благоприятные условия для использования террористами информационных технологий как в целях причинения ущерба критически важным объектам, так и для пропаганды идеологии терроризма.

В пункте 6 главы 2 Концепции указано, что к основным внешним источникам террористической угрозы в Республике Беларусь относятся, в частности, открытость и уязвимость информационного пространства Республики Беларусь для внешнего воздействия, позволяющие распространять идеологию терроризма через глобальную компьютерную сеть Интернет и средства массовой информации.

В пункте 16 главы 3 вышеуказанного акта установлено, что основными мерами по выявлению и пресечению террористической деятельности являются, в частности, информационные – использование возможностей средств массовой информации и глобальной компьютерной сети Интернет для выявления и непосредственного предотвращения актов терроризма, создания и деятельности террористических организаций, незаконных вооруженных формирований, доведение до населения информации об актах терроризма и другой террористической деятельности, а также о принимаемых государственными органами и иными государственными организациями мерах по ее выявлению и пресечению.

В Республике Беларусь был принят Закон Республики Беларусь от 4 января 2007 года № 203-З «О противодействии экстремизму».

Статьей 19 данного закона установлено, в частности, следующее: «Копия вступившего в законную силу решения суда о признании символики и атрибутики, информационной продукции экстремистскими материалами направляется в республиканский орган государственного управления в сфере массовой информации для включения этих символики и атрибутики, информационной продукции в республиканский список экстремистских материалов, который подлежит размещению на сайте этого органа в глобальной компьютерной сети Интернет и опубликованию в средствах массовой информации. Содержание информационной продукции, включенной в республиканский список экстремистских материалов, разглашению не подлежит. Ведение республиканского списка экстремистских материалов, его размещение в глобальной компьютерной сети Интернет и опубликование в средствах массовой информации осуществляются в порядке, установленном Советом Министров Республики Беларусь».

Исходя из приведенных норм можно сделать вывод о том, что руководство Республики Беларусь всерьез обеспокоено разрушительным потенциалом современных глобальных информационных технологий, прежде всего сети Интернет: особо остро этот вопрос встает именно сейчас, когда геополитическое положение Республики Беларусь в силу географических причин (близость государства к «театру» СВО) осложнилось, и четыре из пяти

стран, граничащих с республикой, занимают по отношению к ней довольно враждебную позицию.

Сейчас в мире, особенно в Европейском регионе, нередко сами враждующие страны платят завербованным их спецслужбами лицам за совершение террористических актов на территории страны, являющейся геополитическим противником. Являясь коммуникационными инструментами, сеть Интернет и другие технологии, которые обусловлены ее существованием (например, различные мессенджеры и социальные сети), помогают террористам добиваться своих целей, а потому нуждаются в контроле со стороны любого ответственного перед своим населением государства.

С другой стороны, сеть Интернет – это огромное хранилище ценной информации, которое может помочь и помогает, в частности, белорусским спецслужбам выявлять лиц, причастных к террористической деятельности и ее финансированию, а также заказчиков такой деятельности; осуществлять деятельность в сети Интернет в целях профилактики терроризма; заблаговременно информировать население республики о возможных рисках в этой части.

Ведение республиканского списка экстремистских материалов позволяет всем заинтересованным лицам убедиться, какое огромное количество подобных материалов размещалось и продолжает размещаться в сети Интернет, включая ее белорусский сегмент (в особенности речь идет о различных телеграм-каналах, -чатах, -группах, -стикерах и т. п.). Размещение подобного списка для всеобщего обозрения демонстрирует открытость государственной информационной политики Республики Беларусь в части противодействия контенту, оказывающему негативное влияние на общественное и индивидуальное сознание белорусских граждан и гостей республики.

В Республике Казахстан был принят Закон Республики Казахстан от 13 июля 1999 года № 416-I «О противодействии терроризму».

В соответствии с пунктом 18 статьи 1 указанного закона под террористической деятельностью понимаются, в частности, пропаганда идей терроризма, распространение террористических материалов, в том числе с использованием средств массовой информации или сетей телекоммуникаций, а также публичные призывы к совершению акта терроризма.

Согласно части 1 статьи 12-1 данного закона в целях профилактики, выявления и пресечения терроризма государственный орган, осуществляющий в пределах своей компетенции статистическую деятельность в области правовой статистики и специальных учетов, на основании решений судов ведет учет террористических организаций, информационных материалов, признанных террористическими, и лиц, привлеченных к ответственности за осуществление террористической деятельности.

Часть 3 этой же статьи устанавливает следующее: «Государственный орган, осуществляющий в пределах своей компетенции статистическую деятельность в области правовой статистики и специальных учетов, ведет единые списки организаций и информационных материалов, признанных судом террористическими.

Указанные списки подлежат размещению на интернет-ресурсе государственного органа, осуществляющего в пределах своей компетенции статистическую деятельность в области правовой статистики и специальных учетов».

В 2005 году был принят Закон Республики Казахстан «О противодействии экстремизму».

Часть 3 статьи 9 Закона Республики Казахстан от 18 февраля 2005 года № 31-III ЗРК «О противодействии экстремизму» устанавливает следующее: «Государственный орган, осуществляющий в пределах своей компетенции статистическую деятельность в области правовой статистики и специальных учетов, ведет единые списки организаций и информационных материалов, признанных судом экстремистскими.

Указанные списки подлежат размещению на интернет-ресурсе государственного органа, осуществляющего в пределах своей компетенции статистическую деятельность в области правовой статистики и специальных учетов».

В соответствии со статьей 12 данного закона на территории Республики Казахстан запрещаются использование сетей и средств связи для осуществления экстремизма, а также ввоз, издание, изготовление и (или) распространение экстремистских материалов.

Заслуживает внимания подход Республики Казахстан к определению перечня средств (технологий) распространения террористического контента. В связи с тем, что зарегистрированные традиционные средства массовой информации республики находятся под особым контролем со стороны государства, 99% всего террористического контента, рассчитанного на население Республики Казахстан, распространяется через сеть Интернет (из-за технологической сущности сети Интернет контроль за информационными потоками внутри нее реализовать значительно сложнее). И, разумеется, Республика Казахстан не может не бороться с подобной вредной, опасной для государства и населения республики информацией.

Ведение в Республике Казахстан государственного учета террористических и экстремистских организаций и материалов свидетельствует о политике открытости государства в части противодействия вышеуказанным деструктивным проявлениям.

Норма о том, что сеть Интернет не может быть использована в целях размещения экстремистского контента, демонстрирует нацеленность государства на развитие казахстанского сегмента сети Интернет как виртуальной территории, в отношении которой действуют республиканские

законы и которая выступает средой для осуществления конструктивного человеческого взаимодействия.

В Кыргызской Республике был принят Закон Кыргызской Республики от 4 июля 2022 года № 55 «О противодействии терроризму».

Согласно подпункту «а» пункта 13 статьи 5 указанного закона под террористической деятельностью понимаются, в частности, публичные призывы к осуществлению террористической деятельности или публичное оправдание терроризма, в том числе с использованием средств массовой информации или сети Интернет.

В соответствии с пунктом 5 статьи 7 этого закона Кабинет Министров обеспечивает реализацию мер по противодействию терроризму путем распределения и наделения подчиненных ему органов компетенциями, в том числе по противодействию информационному терроризму и использованию для целей терроризма локальных и глобальной информационно-телекоммуникационной сетей.

Согласно части 6 статьи 16 рассматриваемого закона перечень организаций, признанных судами террористическими, подлежит ежегодному опубликованию в периодических печатных изданиях, а также на официальном сайте Генеральной прокуратуры Кыргызской Республики.

В 2023 году был принят Закон Кыргызской Республики «О противодействии экстремистской деятельности».

На основании пунктов 8 и 9 статьи 8 Закона Кыргызской Республики от 24 февраля 2023 года № 40 «О противодействии экстремистской деятельности» государственные органы исполнительной власти в рамках своих компетенций проводят работу, в частности, по обеспечению выполнения обязательств, возложенных на операторов электросвязи и службы электросвязи общего пользования, по ограничению доступа к информации, запрещенной к распространению на основании вступившего в законную силу судебного акта; по осуществлению мониторинга пространства сети Интернет с целью недопущения распространения в данной сети экстремистских материалов.

Статья 12 указанного закона устанавливает следующее: «1. На территории Кыргызской Республики запрещается использование сетей электросвязи в целях осуществления экстремистской деятельности. Запрет на распространение информации, содержащейся в сетях электросвязи и средствах связи, осуществляется на основании решения суда.

2. В случае если сети электросвязи используются для осуществления экстремистской деятельности, определенные настоящим Законом меры применяются в соответствии с установленными нормами законодательства Кыргызской Республики в области связи».

В соответствии с частью 4 статьи 15 рассматриваемого закона информационные материалы, включенные в список экстремистских материалов, не подлежат распространению на территории Кыргызской

Республики. Данные информационные материалы подлежат изъятию, уничтожению либо ограничению доступа к ним в сети Интернет.

Частью 5 этой же статьи закреплено, что реестр информационных материалов, признанных судом экстремистскими, ведется Генеральной прокуратурой Кыргызской Республики и подлежит систематическому обновлению на ее официальном сайте.

Частью 7 статьи 18 Закона Кыргызской Республики «О противодействии экстремистской деятельности» закрепляется, что реестр организаций, признанных судом экстремистскими, ведется Генеральной прокуратурой Кыргызской Республики и подлежит систематическому обновлению на ее официальном сайте.

Также в связи с производимым анализом целесообразно упомянуть Постановление Кабинета Министров Кыргызской Республики от 15 марта 2023 года № 141 «Об утверждении Программы Кабинета Министров Кыргызской Республики по противодействию экстремизму и терроризму на 2023–2027 годы».

Согласно разделу 4.2 указанной Программы большое значение имеет работа по противодействию использованию различных интернет-ресурсов, СМИ и информационных технологий в экстремистских и террористических целях. Для этого разрабатываются необходимые государственные механизмы и нормативная правовая основа по обеспечению информационной безопасности, к деятельности в данной сфере привлекается гражданское общество, ведется работа по усилению координации между ними. При этом в целях повышения эффективности работа уполномоченных государственных органов по противодействию экстремистской и террористической деятельности должна быть направлена, в частности, на формирование эффективной системы предупреждения и пресечения распространения идей экстремизма и терроризма через информационно-коммуникационную сеть Интернет.

В разделе 4.4 Программы отмечается, что «возможности социальных медиа и мессенджеров используются экстремистскими и террористическими организациями для распространения своей идеологии, пропаганды и вербовки. В связи с этим важными становятся вопросы мониторинга социальных сетей, привлечения активных пользователей для продвижения информации по предупреждению экстремизма и терроризма и альтернативных нарративов».

Одним из основных рисков при реализации указанной Программы в разделе 5.5 называется изменение характера и активизация деятельности экстремистских и террористических организаций в неконтролируемых государством сферах, таких как интернет-пространство, социальные сети и мессенджеры, которые создают новые очаги напряженности.

Законодатель Кыргызской Республики под террористической деятельностью понимает не только собственно террористические акты, но и разнообразные информационные вбросы, направленные на оправдание подобной деятельности или пропагандирующие такую активность.

Сущностно с таким подходом нельзя в полной мере согласиться. Террористические акты, безусловно, относятся к категории «террористическая деятельность». Вместе с тем информационные вбросы в целях пропаганды терроризма к непосредственной террористической деятельности не относятся, их можно считать деятельностью, сопутствующей совершению террористических актов, подготавливающей потенциальных террористов к совершению одного из самых тяжких преступлений.

В качестве положительного примера следует отметить положения законодательства Кыргызской Республики в части блокировки запрещенной информации. Такая блокировка осуществляется в соответствии с судебным решением, а не безапелляционно на основании распоряжения какого-либо сотрудника (начальника подразделения) правоохранительных органов или спецслужб Кыргызской Республики. Наличие судебного решения предполагает, как правило, до момента его вынесения, соблюдение законной процедуры судебного разбирательства (что означает состязательность сторон и позволяет владельцам соответствующих интернет-ресурсов высказать свою позицию по существу дела, быть услышанными судьями, принимающими решения), в ходе которого будет дана оценка имеющимся в деле доказательствам, а кроме того, дает возможность владельцу того или иного сайта (ресурса) воспользоваться прозрачной процедурой обжалования вынесенного судебного акта.

Согласно Закону Кыргызской Республики от 24 февраля 2023 года № 40 «О противодействии экстремистской деятельности» государство (в лице своих властных структур) производит мониторинг сети Интернет на предмет недопущения распространения экстремистских материалов (проактивный подход). Представляется, что такая работа не может пройти бесследно. Национальный сегмент сети Интернет Кыргызской Республики не является очень объемным (с точки зрения количества активных, то есть актуализируемых, сайтов), и существующих государственных возможностей должно хватить на то, чтобы поддерживать его чистоту, осуществлять мониторинг в целях предотвращения появления в нем радикального информационного контента. Разумеется, такую работу целесообразно проводить на регулярной основе, особенно применительно к контенту, распространяемому в мессенджерах.

Так же, как и применительно к террористическому контенту, сведения об экстремистских материалах доступны населению республики на сайте Генеральной прокуратуры Кыргызской Республики.

В Постановлении Кабинета Министров Кыргызской Республики от 15 марта 2023 года № 141 «Об утверждении Программы Кабинета Министров Кыргызской Республики по противодействию экстремизму и терроризму на 2023–2027 годы» отмечается, что к деятельности по противодействию использованию сети Интернет в целях террористической и экстремистской пропаганды привлекается гражданское общество.

Представляется, что компетентным органам Кыргызской Республики было бы целесообразно активизировать более тесное сотрудничество с общественными организациями, которые на добровольной основе реализуют деятельность по выявлению противоправного контента в сети Интернет.

Помимо этого, Кыргызская Республика, как это следует из упомянутой Программы, заинтересована в появлении тех субъектов информационной среды, которые будут продвигать в национальном сегменте сети Интернет информацию по предупреждению пропаганды экстремизма и терроризма, а также альтернативные нарративы. В связи с этим становится крайне важным воспитание молодежи (а именно она чаще всего является социальной базой для выборки террористического актива) в патриотическом ключе, формирование у молодежи понимания того, что подобные радикальные методы (в любых их проявлениях) – не средство решения существующих экономических, социальных, политических проблем.

В Российской Федерации был принят Федеральный закон от 6 марта 2006 года № 35-ФЗ «О противодействии терроризму». Указанный закон не содержит норм, увязывающих противодействие террористическим угрозам с необходимостью установления особых правил контроля за информационными потоками в российском сегменте глобальной сети Интернет или потоками, рассчитанными на население России.

Также был принят Федеральный закон Российской Федерации от 25 июля 2002 года № 114-ФЗ «О противодействии экстремистской деятельности».

Согласно статье 9 данного закона «перечень общественных и религиозных объединений, иных организаций, в отношении которых судом принято вступившее в законную силу решение о ликвидации или запрете деятельности по основаниям, предусмотренным настоящим Федеральным законом, и описание символики указанных объединений, организаций подлежат размещению в информационно-телекоммуникационной сети “Интернет” на сайте федерального органа государственной регистрации». А согласно статье 10 «перечень общественных и религиозных объединений, деятельность которых приостановлена в связи с осуществлением ими экстремистской деятельности, подлежит размещению в информационно-телекоммуникационной сети “Интернет” на сайте федерального органа государственной регистрации».

В соответствии со статьей 12 рассматриваемого федерального закона запрещается использование сетей связи общего пользования для осуществления экстремистской деятельности. «В случае, если сеть связи общего пользования используется для осуществления экстремистской деятельности, применяются меры, предусмотренные настоящим Федеральным законом, с учетом особенностей отношений, регулируемых законодательством Российской Федерации в области связи».

Согласно статье 13 того же закона федеральный список экстремистских материалов подлежит размещению в информационно-телекоммуникационной

сети Интернет на официальном сайте федерального органа государственной регистрации.

Законодательство Российской Федерации в части противодействия экстремизму ограничивается указанием на запрет использования открытого контура сети Интернет для распространения экстремистских призывов и материалов и свидетельствует об открытости государственной информационной политики в части указания на объединения и организации, деятельность которых запрещена, и материалы, признанные судом экстремистскими. В настоящее время ознакомиться с соответствующими перечнями можно на официальном сайте Министерства юстиции Российской Федерации: https://minjust.gov.ru/ru/documents/7822/ (Перечень объединений и организаций), https://minjust.gov.ru/ru/extremist-materials/ (Перечень материалов).

В Республике Таджикистан был принят Закон Республики Таджикистан от 23 декабря 2021 года № 1808 «О противодействии терроризму».

Согласно пункту 12 статьи 1 указанного закона террористическая деятельность – это в том числе пропаганда идей терроризма, распространение материалов или информации, призывающих к осуществлению террористической деятельности либо обосновывающих или оправдывающих необходимость осуществления такой деятельности, в том числе с использованием информационно-телекоммуникационных сетей общего пользования и Интернета.

В соответствии с частью 1 статьи 12 рассматриваемого закона запрещается использование сетей связи для осуществления террористической деятельности.

В соответствии с частью 2 той же статьи при обнаружении в информационно-телекоммуникационных сетях, в том числе в сети Интернет, информации, содержащей призывы к массовым беспорядкам, осуществлению экстремистской и террористической деятельности, участию в массовых мероприятиях, проводимых с нарушением установленного законодательством порядка, а также пропагандирующих экстремизм и терроризм, доступ к таким материалам ограничивается.

В Республике Таджикистан был принят Закон Республики Таджикистан от 2 января 2020 года № 1655 «О противодействии экстремизму».

Согласно части 2 статьи 3 указанного закона активность, связанная с изданием и (или) распространением печатных, аудио-, аудиовизуальных и иных материалов экстремистского характера в средствах массовой информации, Интернете, сетях электрической связи, относится к деятельности, признанной в Республике Таджикистан экстремистской.

На основании части 11 статьи 11 данного закона Служба связи при Правительстве Республики Таджикистан в сфере противодействия экстремизму имеет, в частности, следующие полномочия:

– осуществляет для обеспечения информационной безопасности контроль за деятельностью интернет-сайтов и социальных сетей (интернет-провайдеров);

– проводит мониторинг всех услуг связи Интернета, в том числе социальных сетей, и при необходимости предотвращения экстремистской деятельности ограничивает или приостанавливает деятельность данных сетей (интернет-провайдеров);

– при возникновении чрезвычайных ситуаций (боевые действия, террористические и экстремистские операции, стихийные бедствия), угрожающих безопасности государства, имеет право на приоритетное использование, приостановление или ограничение услуг электросвязи, социальных сетей и других видов связи, независимо от организационно-правовой формы;

– обязует физических лиц и юридические лица, которые осуществляют деятельность по предоставлению услуг связи, в том числе интернет-провайдеров, обеспечить до шести месяцев хранение информации экстремистского характера на своих серверах.

В соответствии с частью 1 статьи 16 рассматриваемого закона в целях предупреждения экстремистской деятельности в Республике Таджикистан запрещается использование коммуникационных сетей общего пользования, сети Интернет и социальных сайтов для распространения экстремистских призывов.

Согласно части 1 статьи 17 Закона Республики Таджикистан «О противодействии экстремизму» в случае выявления в сети Интернет и других телекоммуникационных сетях пропаганды экстремизма, в том числе информации, призывающей к массовым беспорядкам, участию в массовых мероприятиях, приводящих к нарушению общественного порядка, осуществлению иной экстремистской деятельности, доступ к такой информации подлежит немедленному прекращению либо ограничению.

В соответствии с частью 2 той же статьи прекращение либо ограничение доступа к информации для предотвращения пропаганды экстремизма в сети Интернет и других телекоммуникационных сетях обеспечивается Службой связи при Правительстве Республики Таджикистан в сотрудничестве с правоохранительными органами.

Компетентные органы Республики Таджикистан отдают себе отчет в том, что пропаганда терроризма и все то, что ей сопутствует, уже довольно давно проникли в сеть Интернет, и в частности в национальный сегмент Интернета Республики Таджикистан. Недооценка этого обстоятельства неизбежно приводит к трагическим последствиям, ибо молодежь (а именно она, как уже было отмечено выше, является главной социальной базой терроризма) привыкла получать новостную и прочую информацию, как правило, из сети Интернет, а не из традиционных СМИ.

Конструкция статьи 12 Закона Республики Таджикистан от 23 декабря 2021 года № 1808 «О противодействии терроризму» близка конструкции

статьи 12 Федерального закона Российской Федерации от 25 июля 2002 года № 114-ФЗ «О противодействии экстремистской деятельности» в части установления запрета на использование сетей связи для осуществления противозаконной деятельности.

Законодатель Республики Таджикистан, исходя из положений статьи 3 Закона Республики Таджикистан от 2 января 2020 года № 1655 «О противодействии экстремизму», приравнивает экстремистскую пропаганду в сети Интернет к экстремистской пропаганде в СМИ, что вполне оправданно.

Вместе с тем, как представляется, внесудебная процедура ограничения и (или) приостановки деятельности субъектов, являющихся администраторами электронных площадок, на которых население республики имеет возможность размещать различный контент и обмениваться друг с другом сообщениями, отсутствие (применительно к таким ограничениям) обусловленной судебным разбирательством состязательности судопроизводства не способствуют укреплению законности в национальном сегменте сети Интернет Республики Таджикистан.

Статьи 16 и 17 Закона Республики Таджикистан от 2 января 2020 года № 1655 «О противодействии экстремизму» содержат стандартные положения о запрете использования сети Интернет для осуществления экстремистской деятельности, а также о блокировке соответствующего контента.

Анализ государственного регулирования сети Интернет в государствах – членах ОДКБ в целях обеспечения национальной безопасности по направлению «противодействие угрозам в военной сфере»

В Республике Армения был принят Закон Республики Армения от 29 декабря 2006 года № ЗР-258 «О правовом режиме военного положения». Указанный закон никак не увязывает введение подобного режима Правительством Республики Армения с внесением коррективов в параметры функционирования армянского сегмента сети Интернет.

Анализ норм данного закона позволяет сделать вывод о том, что контроль государства за информационными потоками национального сегмента сети Интернет Республики Армения в случае введения военного положения не будет подвергнут каким-либо существенным изменениям. Вместе с тем, как показывают сегодняшние реалии, современные войны – это войны с использованием не только традиционного оружия, но и оружия информационного. Потенциальный противник, если такое ему позволить, постарается использовать слабые места информационного поля страны (куда входят и национальные сегменты глобальной сети Интернет) для того, чтобы дезориентировать население, осуществить вброс недостоверной информации (для ее воздействия на общественное сознание), подорвать доверие общества к военным и властям страны и т. д. С учетом сложности геополитического положения Республики Армения представляется не совсем верным

недооценивать роль электронных коммуникаций в ситуации потенциального военного противостояния.

В Республике Беларусь был принят Закон Республики Беларусь от 13 января 2003 года № 185-З «О военном положении».

Согласно статье 1 указанного закона военная цензура – система государственного контроля за содержанием сообщений и материалов, подготовленных для размещения в средствах массовой информации, сетях электросвязи, а также за содержанием почтовых отправлений, устанавливаемая на период военного положения.

На основании статьи 15 этого закона Президентом Республики Беларусь, государственными органами, органами военного управления, местными советами обороны в период военного положения могут применяться меры по обеспечению военного положения, в частности использоваться деятельность организаций, оказывающих услуги почтовой связи и электросвязи, организаций транспорта, торговли, общественного питания, бытового обслуживания, организаций, осуществляющих издательскую и полиграфическую деятельность, объектов промышленности для нужд обороны.

Статья 46 Закона «О военном положении» закрепляет, что Министерство связи и информатизации Республики Беларусь при обеспечении военного положения осуществляет контроль за работой организаций, осуществляющих деятельность в области связи и информатизации.

Необходимость введения военной цензуры (в том числе и в национальном сегменте сети Интернет) на период военного положения, в принципе, не вызывает вопросов. На период военного положения государством (в лице Министерства связи и информатизации Республики Беларусь) на субъекты, предоставляющие населению республики услуги по обмену электронными сообщениями и размещению информации для всеобщего доступа, могут быть возложены дополнительные обязанности и требования по контролю за соответствующими информационными потоками в сети Интернет с учетом сложившейся обстановки. Информация о характере взаимодействия названного министерства с ключевыми субъектами сети Интернет республики в период военного положения относится к числу государственных секретов.

В Республике Казахстан был принят Закон Республики Казахстан от 5 марта 2003 года № 391-II «О военном положении».

Согласно части 2 статьи 6 указанного закона в период военного положения в целях обеспечения условий для производства продукции, осуществления работ и услуг, необходимых для удовлетворения потребностей государства в интересах обороны, а также нужд населения, могут быть приняты меры, связанные с временными ограничениями, в частности, на осуществление экономической и финансовой деятельности, свободное

перемещение товаров, денег и оказание услуг, поиск, получение, передачу, производство и распространение информации.

В период военного положения происходит максимальная мобилизация властных структур государства и всего населения, государство вынуждено концентрироваться на решении задач, связанных с обороной и защитой мирного населения. В связи с этим понятны и разумны ограничения информационных и иных прав граждан. Такие ограничения обусловлены приоритетом публичного интереса перед частным в особые исторические периоды. Публичный интерес состоит в том, чтобы избежать неоправданных жертв среди мирного населения, организовать работу тыла, перевести экономику страны на «военные рельсы».

В качестве положительного примера следует привести правовые механизмы Республики Казахстан, направленные на противодействие распространению противоправной информации в сети Интернет.

Для своевременного выявления фактов использования сети Интернет в противоправных целях Министерством на постоянной основе осуществляется мониторинг продукции средств массовой информации, в том числе интернет-ресурсов и социальных сетей, на предмет соблюдения законодательства Республики Казахстан. В случае выявления нарушений на интернет-ресурсах в виде распространения информации, запрещенной или иным образом ограниченной к распространению вступившими в законную силу судебными актами или законами Республики Казахстан, выносится предписание уполномоченного органа в области информации в порядке статьи 41-1 Закона Республики Казахстан от 5 июля 2004 года № 567-II «О связи» об ограничении доступа к ним на территории Республики Казахстан.

Согласно Закону Республики Казахстан от 23 июля 1999 года № 451-I «О средствах массовой информации» интернет-ресурсы, в том числе социальные сети, отнесены к средствам массовой информации. Установление требований к интернет-ресурсам на законодательном уровне необходимо в демократическом обществе в интересах обеспечения национальной безопасности, территориальной целостности и общественного порядка, в целях предотвращения беспорядков или преступлений, для охраны здоровья и нравственности. На сегодняшний день ограничение осуществляется исключительно в отношении тех интернет-ресурсов, где были зафиксированы материалы, признанные как национальным законодательством, так и международными документами противоправными, – пропаганда терроризма, экстремизма, суицида, распространение порнографических материалов, продажа наркотиков, оружия и др. В случае несогласия с вынесенным решением предписание уполномоченного органа может быть обжаловано в установленном законодательством порядке лицом или собственником интернет-ресурса, разместившими информацию в сети Интернет.

Вопрос возобновления работы интернет-ресурсов, доступ к которым был закрыт в связи с нарушением ими законодательства, решается уполномоченным органом в случае, если с интернет-ресурса удален

незаконный контент. Для удаления противоправного контента налажены уведомительная работа и рабочие контакты с собственниками и администрациями интернет-ресурсов. На сегодня в таком формате организовано взаимодействие с ведущими зарубежными интернет-платформами: Facebook, TikTok, «ВКонтакте», «Одноклассники» и др.

Закон Республики Казахстан от 10 июля 2023 года № 18-VIII ЗРК «Об онлайн-платформах и онлайн-рекламе» предусматривает правовые основы деятельности онлайн-платформ и инфлюенсеров (блогеров). Законодательной новеллой является регулирование общественных отношений, связанных с онлайн-платформами, функционирующими на территории Республики Казахстан, а также общественных отношений, возникающих в процессе производства, размещения, распространения и хранения онлайн-рекламы на территории Республики Казахстан. Вместе с тем данным законом установлены требование по недопущению распространения ложной информации на онлайн-платформах и основания для отнесения информации к противоправному контенту, приостановления, прекращения размещения и распространения противоправного контента.

В Республике Казахстан под противоправным контентом понимается: призыв, агитация или пропаганда насильственного изменения конституционного строя, нарушения целостности Республики Казахстан, подрыва безопасности государства, войны, социального, расового, национального, религиозного, сословного и родового превосходства, культа жестокости и насилия, суицида, порнографии, наркотических средств, психотропных веществ, их аналогов и прекурсоров, идеи сепаратизма, мошенничества; информация, способствующая нарушению межнационального и межконфессионального согласия, а также высказывания, подвергающие сомнению государственность и территориальную целостность Республики Казахстан; информация, раскрывающая государственные секреты или иную охраняемую законом тайну; иная информация, запрещенная законами Республики Казахстан.

Кроме того, пользователи онлайн-платформ при осуществлении сбора добровольных пожертвований обязаны соблюдать требования, установленные законодательством Республики Казахстан, о противодействии легализации (отмыванию) доходов, полученных преступным путем, и финансированию терроризма. Таким образом, данный закон позволит повысить эффективность борьбы с массовым распространением фейковой информации, бесконтрольной деятельности блогеров и их теневой занятости. Следует отметить, что все ограничения доступа к интернет-ресурсам носят не массовый характер, а применяются только в конкретных случаях в соответствии с нормами международного права и казахстанского законодательства для обеспечения безопасности населения.

В Кыргызской Республике был принят Конституционный закон Кыргызской Республики от 30 апреля 2009 года № 149 «О военном положении».

Согласно пунктам 2 и 14 статьи 5 указанного закона введение военного положения влечет за собой, в частности, введение особого режима работы объектов, обеспечивающих функционирование транспорта, коммуникаций и связи, объектов энергетики, организаций здравоохранения, объектов, представляющих повышенную опасность для жизни и здоровья людей и для окружающей природной среды; а также установление контроля за работой предприятий связи, транспорта, печати, телевидения, вычислительных центров и автоматизированных систем управления, средств массовой информации и радиосвязи общего пользования.

В соответствии с пунктом 1 статьи 9 рассматриваемого закона Президент Кыргызской Республики, как Главнокомандующий Вооруженными Силами Кыргызской Республики, с введением военного положения руководит обороной Кыргызской Республики и в период военного положения устанавливает на территории, на которой введено военное положение, особый режим работы объектов, обеспечивающих функционирование транспорта, коммуникаций и связи, объектов энергетики, а также объектов, представляющих повышенную опасность для жизни и здоровья людей и для окружающей природной среды.

Законодательство Кыргызской Республики не содержит особых норм, устанавливающих специальный режим функционирования национального сегмента сети Интернет и субъектов, предоставляющих населению республики возможность доступа к ресурсам сети Интернет, на период военного положения. Вместе с тем республиканская инфраструктура сети Интернет это не что иное, как совокупность предприятий связи, а потому правила об особом режиме работы будут распространяться и на них.

Российская Федерация и некоторые другие государства – члены ОДКБ давно используют потенциал сети Интернет для взаимодействия со своим населением (информирование населения, предоставление населению возможности направлять обращения в органы государственной власти и получать ответы на них и т. п.), следовательно, и Кыргызской Республике можно рекомендовать поддерживать функциональность своего «электронного правительства» (а вместе с ним и функциональность общедоступного контура национального сегмента сети Интернет), если, конечно, это не противоречит республиканской безопасности.

Также Кыргызской Республике имеет смысл поддерживать безопасность функционирования своей критической информационной инфраструктуры. В государствах – членах ОДКБ многие отрасли хозяйства цифровизированы (в частности, цифровизированы их управление, контроль за процессами, производство и т. д.), успешность этих отраслей в немалой мере определяется тем, как работают информационные системы их производственно-хозяйственных комплексов. Частично работа таких информационных систем замыкается на открытый, то есть общедоступный, контур сети Интернет, а значит, обеспечение его безопасности является приоритетом для государства.

В Российской Федерации был принят Федеральный конституционный закон от 30 января 2002 года № 1-ФКЗ «О военном положении».

В соответствии с подпунктами 2 и 14 части 2 статьи 7 этого закона на основании указов Президента Российской Федерации на территории, на которой введено военное положение, вводится особый режим работы объектов, обеспечивающих функционирование транспорта, коммуникаций и связи, объектов энергетики, а также объектов, представляющих повышенную опасность для жизни и здоровья людей и для окружающей природной среды; вводится контроль за работой объектов, обеспечивающих функционирование транспорта, коммуникаций и связи, за работой типографий, вычислительных центров и автоматизированных систем, средств массовой информации, осуществляется использование их работы для нужд обороны.

Согласно пункту 12 статьи 11 рассматриваемого закона Президент Российской Федерации устанавливает на территории, на которой введено военное положение, особый режим работы объектов, обеспечивающих функционирование транспорта, коммуникаций и связи, объектов энергетики, а также объектов, представляющих повышенную опасность для жизни и здоровья людей и для окружающей природной среды.

На основании подпункта 10 части 2 статьи 14 указанного закона для реализации мер, предусмотренных пунктом 2 статьи 7 этого закона, федеральными органами исполнительной власти на основании указов Президента Российской Федерации, в частности, вводится контроль за работой объектов, обеспечивающих функционирование транспорта, коммуникаций и связи, за работой типографий, вычислительных центров и автоматизированных систем, а также средств массовой информации, осуществляется организация использования их работы для нужд обороны.

Обращает на себя внимание сходство формулировок норм законов о военном положении Российской Федерации и Кыргызской Республики в части установления особого режима работы предприятий связи. Но российский закон дополнен нормами о том, что средства связи (во всем их многообразии), расположенные на территории Российской Федерации, используются в период военного положения целевым образом, то есть для нужд обороны. Категорию «средства массовой информации», используемую законодателем, следует понимать максимально широко и относить к ним и электронные (сетевые) СМИ.

Инициатором установления особого режима работы предприятий связи выступает Президент Российской Федерации, а непосредственный контроль за соблюдением такого режима осуществляют федеральные органы исполнительной власти.

В Республике Таджикистан был принят Закон Республики Таджикистан от 20 июня 2019 года № 1608 «О военном положении».

Согласно статье 6 данного закона на территории, где введено военное положение, в соответствии с законодательными актами и иными нормативными правовыми актами Республики Таджикистан, применяются, в

частности, следующие меры: введение специального режима деятельности объектов, обеспечивающих функционирование транспорта, коммуникации, связи, телевидения, радио, изданий, энергетических объектов, а также объектов, представляющих повышенную опасность для жизни и здоровья людей и для окружающей среды; контроль работы объектов, обеспечивающих функционирование транспорта, коммуникации и связи, работы типографий, вычислительных центров и автоматизированных систем, средств массовой информации, их использование для нужд обороны, запрещение работы приемопередающих радиостанций индивидуального пользования на территории, где объявлено военное положение.

В соответствии со статьей 9 указанного закона Президент Республики Таджикистан – Верховный Главнокомандующий Вооруженными Силами Республики Таджикистан в период действия военного положения имеет, в частности, следующую компетенцию: определяет на территории, где введено военное положение, специальный режим работы объектов, обеспечивающих функционирование транспорта, коммуникаций, связи, телевидения, радио и издательств, энергетических объектов, а также объектов, представляющих повышенную опасность для жизни и здоровья людей и для окружающей среды.

На основании части 1 статьи 12 рассматриваемого закона для обеспечения режима военного положения министерства, государственные комитеты и иные государственные органы в рамках своих полномочий и направления деятельности обеспечивают на территории, где введено военное положение, особый режим работы объектов, обеспечивающих функционирование транспорта, коммуникаций, связи, телевидения, радио и издательств, объектов энергетики, а также объектов, представляющих повышенную опасность для жизни и здоровья людей и окружающей среды.

Конструкция и содержание Закона Республики Таджикистан «О военном положении» примерно повторяют конструкцию и содержание аналогичного российского закона.

Основные направления гармонизации национального законодательства с учетом принципов государственного регулирования сети Интернет в целях обеспечения национальной безопасности

1. ***Принцип соразмерного ограничения информационных прав граждан.*** Во время контртеррористической операции, угрозы осуществления террористического акта, продолжающихся террористических действий государству в лице его компетентных правоохранительных органов и специальных служб дозволено вмешиваться в функционирование телекоммуникационных сетей связи, ограничивать их использование на определенной территории, на время приостанавливать работу цифровых сервисов в отношении тех пользователей, которые находятся в местах, объявленных зоной проведения контртеррористической операции. Органы

государственной власти (специальные службы) следует наделить полномочиями выдавать предписания субъектам, предоставляющим населению государства – члена ОДКБ услуги по обмену электронными сообщениями и размещению информации для всеобщего доступа (администрациям мессенджеров, социальных сетей и т. д.), по ограничению или приостановлению оказания услуг связи. В противном случае ценная с точки зрения специальных служб и правоохранительных органов информация станет достоянием общественности (все граждане, имеющие смартфон, это потенциальные «журналисты» и «блогеры»), которая не всегда задумывается над тем, какой контент она выкладывает в сеть Интернет в разгар противостояния террористической угрозе.

2. ***Принцип информирования граждан государства о субъектах, причастных к террористической и (или) экстремистской деятельности.*** Реализуется в обязанности уполномоченных органов государств – членов ОДКБ размещать соответствующую информацию в открытом доступе в сети Интернет (на сайте ведомства) и регулярно обновлять список террористических организаций (а также лиц, признанных террористами) и экстремистских организаций (экстремистских материалов). С учетом того что не во всех национальных сегментах сети Интернет государств – членов ОДКБ на должном уровне поддерживается информационная безопасность и своевременно пресекается возможность доступа граждан этих государств к описанному выше вредному контенту, граждане государств – членов ОДКБ имеют право знать, кто из активных спикеров в сети Интернет нарушает законы государства и распространяет противозаконный контент.

Также, в целях реализации обозначенного принципа, имеет смысл закрепить обязанность уполномоченных органов государств – членов ОДКБ размещать соответствующую информацию в открытом доступе в сети Интернет (на сайте ведомства) и регулярно обновлять список лиц, причастных к геноциду советского народа в годы Великой Отечественной войны и послевоенный период.

3. ***Принцип перманентной (постоянной) профилактики пропаганды терроризма в сети Интернет.*** Заключается в профилактике и противодействии пропаганде террористической деятельности (вербовке в террористические организации), осуществляемой с использованием сети Интернет. Для его реализации целесообразно систематически осуществлять анализ угроз, исходящих из призывов через сеть Интернет к осуществлению террористических актов, и принимать меры по их купированию.

4. ***Принцип проактивного подхода в части мониторинга национальной информационной сферы.*** Базируется на формировании в уполномоченных органах государств – членов ОДКБ подразделений, которые непосредственно занимались бы вопросами организации мониторинга социальных сетей, мессенджеров, форумов, других площадок на предмет наличия экстремистских, террористических призывов или размещения

информации, противоречащей национальному законодательству государств – членов ОДКБ (призывы к мятежу, массовым беспорядкам и т. д.).

5. ***Принцип опоры на гражданское общество в части профилактики пропаганды терроризма и экстремизма в сети Интернет.*** Предполагается, что представители общественности, бизнеса могут сотрудничать с уполномоченными органами государств – членов ОДКБ в части поиска террористического, экстремистского контента в сети Интернет. При этом следует определить точные критерии информации, подпадающей под категорию «террористической» или «экстремистской», предусмотреть формат и границы такого сотрудничества, меры его стимулирования, а также обеспечить его конфиденциальность.

6. ***Принцип установления точечных ограничений на функционирование социальных сетей и мессенджеров и на доступность информации в них.*** Основывается на том, что ограничение или приостановление деятельности субъектов, предоставляющих населению государства – члена ОДКБ услуги по обмену электронными сообщениями и размещению информации для всеобщего доступа, может осуществляться только в части прекращения всеобщего доступа к какому-либо конкретному контенту внутри соответствующих социальной сети или мессенджера, но не применительно ко всему контенту коммуникационной платформы, в целях недопущения нарушения информационных прав других ее пользователей. Этот принцип применим исключительно по отношению к крупным коммуникационным площадкам. Социальные сети и мессенджеры с небольшим охватом аудитории не должны подпадать под действие данного принципа. В отношении таких агрегаторов интернет-ресурсов должны применяться меры по ограничению доступа к площадке в целом при наличии правовых оснований для принятия соответствующих решений.

7. ***Принцип уведомления органов, осуществляющих надзор за исполнением законов и соблюдением прав и свобод человека и гражданина, в случае приостановки работы сетей и средств связи.*** Базируется на том, что приостановка работы сетей и средств связи, а также доступа к интернет-ресурсам должна сопровождаться обязательным уведомлением об этом уполномоченных государственных органов государств – членов ОДКБ.

Реализация в законодательстве государств – членов ОДКБ предложенных рекомендаций позволит:

– обеспечить комплексность регулирования отношений, формирующихся в национальных сегментах сети Интернет государств – членов ОДКБ, в целях обеспечения национальной безопасности;

– точно определить границы государственного вмешательства (контроля) в сферу цифровых коммуникаций в целях поддержания национальной безопасности;

– предусмотреть оперативную блокировку того или иного контента в национальном сегменте сети Интернет в случае возникновения существенных угроз национальной безопасности.