

Какешов Б.Д., Шаршенева Н.З.

КЫРГЫЗ РЕСПУБЛИКАСЫНЫН МААЛЫМАТТЫК КООПСУЗДУГУН КАМСЫЗ
КЫЛУУ КӨЙГӨЙЛӨРҮ: САЯСИЙ-УКУКТУК АСПЕКТТЕР

Какешов Б.Д., Шаршенева Н.З.

ПРОБЛЕМЫ ОБЕСПЕЧЕНИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ
КЫРГЫЗСКОЙ РЕСПУБЛИКИ: ПОЛИТИКО-ПРАВОВЫЕ АСПЕКТЫ

B. Kakeshov, N. Sharshenova

PROBLEMS OF ENSURING INFORMATION SECURITY OF THE
KYRGYZ REPUBLIC: POLITICAL AND LEGAL ASPECTS

УДК: 343.13 (575.2) (04)

Улуттук коопсуздукту камсыз кылуунун теориялык аспекти каралды, алардын анализинин негизинде бул түшүнүктүн аныктамасы такталды. Жогорку көңүл бурууну талап кылган көйгөйлөргө өткөн жана азыркы кылымдын акыркы он жылдыгында региондордун бирдей эмес экономикалык өнүгүүсү, жаратылыш ресурстарынын түгөнүшү жана айлана-чөйрөнүн бузулушу, мыйзамсыз миграция, этникалык жана диний чыр-чатактар, трансулуттук уюшкан кылмыштуулук жана эл аралык терроризм кирет. Башкача айтканда, «катуу», милитаристтик коопсуздук чакырыктарынан, негизинен гуманитардык мүнөздөгү «жумшак», мамлекеттин чегинен тышкары «агып» өтүүгө өтүү болду. Толуктуугу үчүн «жумшак» коопсуздук коркунучтарынын эволюциясын көрсөтүү керек. 90-жылдардын башында мыйзамсыз миграция менен катар экологиялык жана жаратылышты коргоо маселелери биринчи орунда турган. 2000-жылдардын башында трансулуттук уюшкан кылмыштуулук жана эл аралык терроризм сыяктуу дүйнөлүк коопсуздук чакырыктарына басым барган сайын өзгөрүүдө. Мунун түздөн-түз даңгы болуп экономикалык жана социалдык теңсиздиктин булактарынын бири болгон терроризм түрүндөгү зомбулук көрүнүштөрүнүн бардык жерде өсүшү саналат. Эл аралык коопсуздук системасын калыптандырууда баштапкы чекит катары эл аралык мамилелердин келечеги жөнүндө маселе дагы актуалдуу бойдон калууда. Дискуссиялар анын келечегине болгон ар түрдүү көз карашы менен мүнөздөлүп, бул проблематиканын узакка созулган талкуусунун башталышы болду.

Негизги сөздөр: улуттук коопсуздук, коркунуч, маалыматтык коопсуздук, максаттар, милдеттер, субъекттер, саясий механизм, коопсуздукту камсыз кылуу, коркунуч.

Рассмотрены теоретические аспекты обеспечения национальной безопасности, на основе анализа которых уточняется определение данного понятия. К проблемам, требующим повышенного внимания, в последнее десятилетие прошлого и настоящего века отнесены неравномерное экономическое развитие регионов, истощение природных ресурсов и разрушение окружающей среды, нелегальная миграция, этнические и религиозные конфликты, транснациональная организованная преступность и международный терроризм. Иначе говоря, произошел переход от «жестких», милитаристских вызовов безопасности к «мягким», носящим преимущественно гуманитарный характер, «выплескивающимся» за пределы государства. Для полноты картины необходимо указать на эволюцию «мягких» угроз безопасности. В начале 90-х годов на первом месте по значимости находились экологические и природоохранные проблемы, наряду с нелегальной миграцией. К началу 2000-х годов акцент все более смещается на такие вызовы мировой безопасности как транснациональная организованная

преступность и международный терроризм. Прямым подтверждением тому служит повсеместный рост проявлений насилия в виде терроризма, имеющего одним из источников усиливающееся экономическое и социальное неравенство. Не менее актуальным остается и вопрос о будущем международных отношений как исходной точки в формировании системы международной безопасности. Дискуссии характеризовались разноречивым видением ее будущего, положив начало продолжительному обсуждению данной проблематики.

Ключевые слова: национальная безопасность, угроза, информационная безопасность, цели, задачи, субъекты, политический механизм, обеспечения безопасности, угроза.

The theoretical aspects of ensuring national security are considered, based on the analysis of which the definition of this concept is clarified. In the last decade of the last and present centuries, the uneven economic development of the regions, the depletion of natural resources and the destruction of the environment, illegal migration, ethnic and religious conflicts, transnational organized crime and international terrorism have been identified as issues requiring increased attention. In other words, there was a transition from "hard", militaristic security challenges to "soft" ones, which are mainly humanitarian in nature, "spilling out" of the state. To complete the picture, it is necessary to point out the evolution of "soft" security threats. In the early 1990s, environmental and environmental issues, along with illegal migration, were in first place in importance. By the early 2000s, the emphasis was increasingly shifting to such global security challenges as transnational organized crime and international terrorism. A direct confirmation of this is the widespread increase in the manifestations of violence in the form of terrorism, which has one of the sources of increasing economic and social inequality. No less relevant is the question of the future of international relations as a starting point in the formation of an international security system. The discussions were characterized by a contradictory vision of its future, laying the foundation for a long discussion of this issue.

Key words: national security, threat, information security, goals, objectives, subjects, political mechanism, ensuring security, threat.

Последние достижения науки и техники привели к тому, что изменения в социальных, экономических, политических процессах проходят очень быстро за счет развития информационной сферы и технологий. В то же время, информационные технологии становятся одним из основных факторов, влияющих на жизнь людей, обществ и даже целых стран. В развитых странах, информационное общество формировалось постепенно, последовательно, по мере развития информационных технологий. Развитие технологий, а также

их использование государственными структурами предполагает, что они будут помогать реализации конституционных прав граждан, способствовать улучшению благосостояния населения за счет повышения конкурентоспособности бизнеса в стране, что окажет положительный эффект в деле укрепления государственности.

Реализуя систему мер национальной безопасности, создаются благоприятные условия для поступательного развития страны, укрепления ее совокупного потенциала, международных позиций и значимости в мировом пространстве [1, с. 13].

Экстремистскими и террористическими организациями и группами все активнее используются возможности глобальных информационно-коммуникационных сетей для пропаганды своей идеологии, вербовки и обучения единомышленников, поддержания связи и финансирования различных террористических групп. Вызывает озабоченность распространение радикальных идей различного характера среди молодежи Кыргызстана. Известны случаи, когда граждане под влиянием целенаправленной пропаганды, в том числе через Интернет, участвуют в противоправных действиях в различных регионах мира (пункт 13) [2].

В связи с этим возникает необходимость разработки эффективной государственной политики в информационной сфере для сохранения суверенитета и укрепления политической, экономической и военной стабильности страны.

Некоторые российские юристы также считают, что «не будет ошибочным мнение о том, что создание правового пространства, охватывающего государства ЕАЭС, в котором будут действовать единые и эффективные механизмы борьбы с преступностью, – это прежде всего, залог безопасности и процветающего развития этих государств» [3, с. 147].

В целом государственная система защиты информации в СССР функционировала в первую очередь в интересах обороноспособности страны Военно-промышленного комплекса Минобороны. Практически вся информация о государственной безопасности и интересах страны являлась секретной. После распада СССР и обретения Кыргызской Республикой независимости в сфере обеспечения информационной безопасности появились существенные проблемы, связанные с незащищенностью сведений, представляющих определенный интерес для иностранных спецслужб.

С учетом этого была проведена работа по реализации национальной политики в области информатизации, были созданы концептуальные документы, программы и законодательные основы развития информационных отношений.

Так постановлением Правительства Кыргызской Республики от 8 ноября 2001 года №697 утверждена

«Программа развития информационно-коммуникационных технологий в Кыргызской Республике», а в марте 2002 года экс-Президентом КР была утверждена Национальная стратегия: «Информационно-коммуникационные технологии для развития Кыргызской Республики». Приоритетными были обозначены три основных направления: электронное правительство, электронное образование и электронная экономика [4, с. 133].

В последние годы были приняты меры по обеспечению информационной безопасности, в частности образованы: в 2006 г. - Национальное агентство информационных ресурсов, технологий и коммуникаций; в 2007 г. - Межведомственная комиссия по информационной безопасности; в 2010 г. - Консультативный совет Государственного агентства связи при Правительстве КР; в 2014 году - Совет по информационной политике Министерства культуры, информации и туризма; Государственный комитет по информационным технологиям и связи - в 2016 году.

Государственная политика в области информационной безопасности основана на соблюдении Конституции и законодательства КР: «Об информации», «О гарантиях и свободе доступа к информации», «О связи», «Об авторском праве и смежных правах», «Об обязательном экземпляре документов», «О защите государственных секретов КР, «О средствах массовой информации», а также Уголовный кодекс, Гражданский кодекс Кыргызской Республики и т.д.

Кроме того, Правительство КР принимает комплексные меры по повышению информационной безопасности. В частности, формируется база правового обеспечения информационной безопасности и механизмов ее реализации, ведется работа по подготовке законопроектов, регулирующих общественные отношения в информационной сфере с учетом современных потребностей.

Однако анализ состояния информационной безопасности показывает, что действующая нормативно-правовая база недостаточна, поскольку многие вопросы не имеют адекватного законодательного регулирования, не решен вопрос создания системы защиты национального информационного пространства, обеспечивающий защиту от тайных атак со стороны «внешних игроков», применяющих для этих целей новейшие IT-технологии [5, с. 35-36].

В наиболее общем виде информационная безопасность государства представляет собой «состояние сохранности информационных ресурсов государства и защищенности законных прав личности и общества в информационной сфере [6].

За последние 15-20 лет произошло значительное расширение пространства и методов обеспечения информационной безопасности. Этот процесс хорошо представлен в специальных исследованиях по проб-

леме глобальной безопасности с учетом сдвига в сторону ориентации на так называемую "мягкую силу 2.0" и вызовов, формирующих глобальное информационное общество, а также появления новых источников угроз и преступлений [7].

И вместе с тем использование информационно-коммуникационных технологий (ИКТ) государственными органами дает возможность более эффективно предоставлять услуги населению, повысить качество обслуживания и прозрачность работы его аппарата, и, соответственно, уровень доверия граждан по отношению к государству. Также, развитие ИКТ привело к формированию нового формата средств массовой информации (СМИ) - в качестве аудитории СМИ теперь выступают все пользователи сети Интернет. Многие информационные агентства имеют не только свои впечатительные веб-порталы, но и страницы в социальных сетях. По данным исследований, почти 80% всех интернет-пользователей в Кыргызстане зарегистрированы в той или иной социальной сети, что автоматически повышает видимость всех статей в такого рода СМИ. Отдельно можно рассматривать так называемые интернет-блоги.

При нынешнем развитии технологий цели достигаются намного быстрее и эффективнее в результате новых видов борьбы, а именно - борьбы за информационное пространство. В результате этой борьбы появляется новый спектр так называемых информационных угроз. Угрозы данного типа в основном осуществляются с помощью специального подбора информации, которая направлена на раскол общества. Такого рода информацию условно можно назвать «информационным инструментом», и с ее помощью становится возможным нанесение ущерба жизненно важным интересам государства, причем ущерб этот может быть значительным по своей деструктивности.

Таким образом, разрушительное воздействие информационного инструмента может затронуть все сферы функционирования общества. На сегодня, информационная сфера Кыргызской Республики, как и любого другого современного государства, оказывает активное влияние на все составляющие национальной безопасности государства, а именно – политическую, экономическую, военную, социальную, экологическую и другие сферы. А так как развитие информационно-коммуникационных технологий идет быстрыми темпами, наблюдается прямая зависимость между обеспечением национальной безопасности и информационной сферой государства, то есть обеспечение информационной безопасности государства становится одним из особо приоритетных направлений обеспечения, причем по мере развития ИКТ эта зависимость будет прослеживаться еще больше. И поэтому, изучение теории информационной безопасности, и обеспечение ее применения на практике стано-

вится актуальной задачей не только для государственных органов, но и для научных кругов в республике.

Одним из важнейших факторов оптимизации государственного управления является целевое управление информационной сферой в домене государства. Оно включает в себя формирование и распространение разного рода информационных воздействий, и управление информационными ресурсами и потоками информации. Наравне с этим, управление включает в себя развитие как информационно-коммуникационной инфраструктуры страны, так и рынка информационной продукции, услуг и технологий.

Идея формирования открытого информационного общества, в виде пространства суверенного государства, которое смогло бы интегрироваться в мировое информационное пространство, и при этом, сумев соблюсти национальные интересы и особенности, обеспечив информационную безопасность страны – вот такова цель политики обеспечения информационной безопасности Кыргызстана. Создание развитого информационного пространства подразумевает активное использование сетей обмена информацией и телекоммуникационных систем, массовую компьютеризацию процессов сбора и обработки информации во всех сферах деятельности. Данный процесс охватил фактически все страны мира и является в настоящее время одним из основных факторов их социального, научно-технического и, как следствие, экономического развития.

Необходимым условием для эффективного осуществления политики обеспечения и поддержания состояния информационной безопасности является разработка технологических и организационных мер по защите структур государственного управления от несанкционированного воздействия на государственные коммуникационные системы, проводимым с целью причинения ущерба особо важным интересам как государства в целом, так и общества, и каждого гражданина.

С развитием информационных и коммуникационных технологий, особенно если учесть, какое влияние оказывают так называемые социальные сети на информационное пространство любого государства, особенно это стало актуальным в ходе последних событий в Сирии, когда террористические организации активно использовали социальные сети, такие как Facebook, Instagram, Tik Tok и другие для вербовки. Так, в социальных сетях подобного рода, разработчики ставят приватность (секретность, то есть защиту от несанкционированного доступа) переписки пользователей и сообщения в закрытых группах на первый план, отследить противозаконную деятельность таких организаций становится практически невозможным. Тем более что не только Кыргызская Республика, но и страны с более развитой информационной и комму-

никационной инфраструктурой оказались не готовыми к угрозам такого рода информационной, и, как следствие, национальной безопасности.

Сегодня Интернет – это не просто технико-операционная система, он стал социально-технической надстройкой. Информация вполне может служить источником политических и социальных угроз. Для этого необходимы политические и правовые механизмы, регулирующие поток информации и информирование общества.

Каждый аспект человеческой жизни, а также поток информации в государственных структурах и ведомствах в большей или меньшей степени напрямую зависят от программного обеспечения и ИКТ. С повышением роли этой системы увеличивается количество преступлений, совершенных с помощью компьютерных технологий, а что касается обмена информацией национального значения, было предложено множество моделей для анализа национальной киберпреступности, но к сожалению в правоохранительной сфере преступления, совершенные в киберпространстве, еще не достаточно хорошо выявляются и расследуются, так как раскрытие подобных преступлений требует профессионального подхода и подготовки.

Подводя итоги, определим следующие шаги:

- создать единый орган, который координирует безопасный сбор, хранение, обработку, передачу и распространение данных. Для этого, прежде всего, необходимо разработать нормативную базу, в которой определяется уровень конфиденциальности информации, определяются типы информации, относящиеся к определенному уровню, а также должны быть рассмотрены и стандартизированы средства шифрования, защищающие конфиденциальность и целостность информации. На основе этого фундамента необходимо разработать политико-правовые механизмы, регулирующие деятельность этих структур;

- с возрастанием роли Интернета в информационном пространстве необходимо защищать права и свободы человека и социума от информации, пропагандирующей насилие и жестокость, от преднамеренного формирования негативного мировоззрения подрастающего поколения. В то же время причины внешних угроз могут находиться вне юрисдикции законов КР, что может существенно усложнить применение системы юридических действий;

- как уже неоднократно отмечалось, необходимо обучать сотрудников правоохранительных органов борьбе с технической разведкой, защиты от «информационного оружия» и совершенствовать законода-

тельную базу в этой области.

- в целях своевременного предоставления достоверной и сбалансированной информации всем гражданам Кыргызстана и иностранным лицам, необходимо обеспечить государственную поддержку деятельности отечественных новостных организаций по продвижению их продукции на внешние рынки. Однако, на наш взгляд, важно признать объективную необходимость законодательных ограничений (регулирования) свободы массовой информации, что является единственным способом обеспечения правового равенства в информационных отношениях.

- средства массовой информации, выступая инструментом взаимодействия, не должны стоять на пути конфронтации между государством и обществом, особенно с целью демонстрации своей независимости, иногда независимость нашей прессы вообще не гарантирует ее объективности. Пресса, которая поддерживает только идею собственной свободы и независимости, в будущем больше не будет отражать интересы отдельных лиц, общества и государства, создавая ситуацию информационной опасности.

- совершенствование законодательной базы в области средств массовой информации. Развивать сферу информационного права и кадровую политику по этому вопросу в Кыргызстане. Организовать систему подготовки персонала, работающего в области информации и информационных технологий, с тем чтобы они не подвергались недружественным воздействиям извне и были теоретически знакомы с областью информационной безопасности.

Мы считаем необходимым осуществлять международное сотрудничество в области обеспечения информационной безопасности государства и дальше представлять интересы Кыргызской Республики в соответствующих международных учреждениях.

Литература:

1. Концепции информационной безопасности Кыргызской Республики на 2019-2023 годы развития. Приложение (к постановлению Правительства Кыргызской Республики от 3 мая 2019 года № 209).
2. У.С. Жумабаев. Понятие обеспечения национальной безопасности в законодательстве Кыргызской Республики: Проблемы и пути решения // Вестник КРСУ. 2015. Том 15. № 5. - С. 13. - 211 с.
3. Рудич В.В., Абрамов А.Б. К вопросу об унификации уголовного и уголовно-процессуального законодательства, и основной цели такой унификации для государств ЕАЭС. / Наука, новые технологии и инновации Кыргызстана, № 1, 2022. - С. 147. - 262 с.
4. Токсоналиева Р.М. Мусурманова Г.С. Влияние современ-

- ных информационно-коммуникационных технологий на развитие информационного общества Кыргызстана / Теория науки, 2018. № 5. С. 133.
5. Токсоналиева Р.М. Государственная политика Кыргызской Республики в сфере информационно-психологической безопасности. / Вестник КРСУ. 2015. - Том 15. № 5. С. 35-36. – 211 с.
 6. Безопасность: теория, парадигма, концепция, культура: словарь-справочник 2-е изд., доп. и перераб. / авт.-сост. проф. В.Ф. Пилипенко. - М.: ПЕР СЭ-Пресс, 2005.
 7. Смирнов А.И. Глобальная безопасность и «мягкая сила 2.0»: вызовы и возможности для России / А.И. Смирнов, И.Н. Кохтюлина. - М., 2012. - С. 98-103.
 8. Сейдахматов Н.А. Участие органов национальной безопасности Кыргызской Республики в обеспечении информационной безопасности // Диссертация кандидата юридических наук Академия ФСБ РФ. - М., 2015. С. 36-40. - 325 с.
 9. Адилов А.Н., Какешов Б.Д., Бобушев С.Р. Использование сил и средств организации договора о коллективной безопасности в борьбе с международным терроризмом. / Наука, новые технологии и инновации Кыргызстана. 2022. №. 4. С. 180-184.