МИНИСТЕРСТВО ОБРАЗОВАНИЯ И НАУКИ КЫРГЫЗСКОЙ РЕСПУБЛИКИ

АКАДЕМИЯ ГОСУДАРСТВЕННОГО УПРАВЛЕНИЯ ПРИ ПРЕЗИДЕНТЕ КЫРГЫЗСКОЙ РЕСПУБЛИКИ

КЫРГЫЗСКО-РОССИЙСКИЙ СЛАВЯНСКИЙ УНИВЕРСИТЕТ ИМ. Б.ЕЛЬЦИНА

ДИССЕРТАЦИОННЫЙ СОВЕТ Д.23.17.559

На правах рукописи
УДК: 323 (575.2) (043.3)

МУСУРАЛИЕВА МЭЭРИМ МАМБЕТКАЛЫКОВНА

ПОЛИТИЧЕСКИЕ МЕХАНИЗМЫ ОБЕСПЕЧЕНИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ В КЫРГЫЗСКОЙ РЕСПУБЛИКЕ

Специальность 23.00.02 – Политические институты, процессы и технологии

А В Т О Р Е Ф Е Р А Т
диссертации на соискание ученой степени
кандидата политических наук

Бишкек - 2018

Работа выполнена на кафедре философии и гуманитарных дисциплин Института гуманитарных знаний Кыргызского государственного университета имени И. Арабаева

Научный руководитель: кандидат политических наук,

Официальные оппоненты: доктор политических наук,

кандидат политических наук

Ведущая организация:

Защита состоится « » 2018 года в 14:00 часов на заседании диссертационного совета Д.23.17.559 по защите диссертаций на соискание ученой степени доктора (кандидата) политических и социологических наук при Академии государственного управления при Президенте КР и Кыргызско-Российском Славянском Университете им. Б. Ельцина по адресу: 720000, г. Бишкек,

С диссертацией можно ознакомиться в научной библиотеке

Автореферат разослан « » 2018 г.

Ученый секретарь
диссертационного совета,
кандидат политических наук **Абдыраманова Ч.Ш.**

ОБЩАЯ ХАРАКТЕРИСТИКА РАБОТЫ

Актуальность темы исследования. Распад Советского Союза повлиял на многие аспекты политической жизни бывших социалистических республик. Проблемы безопасности, такие как национальная безопасность, региональная и международная, стали актуальными для вновь образовавшихся государств, в том числе и для Кыргызской Республики. Это было что связано, главным образом, с формированием «нового мирового порядка», что, в свою очередь, было вызвано образованием новых независимых государств, усиливающимся процессом глобализации, а также возрастающей угрозой международного терроризма и т.д. Последние достижения науки и техники привели к тому, что изменения в социальных, экономических, политических процессах проходят очень быстро за счет быстрого 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. Использование информационно-коммуникационных технологий (ИКТ) государственными органами дает возможность эффективно преобразовать процедуры предоставления услуг гражданам, повысить эффективность 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 агенства имеют не только свои вещательные веб-порталы, но и страницы в социальных сетях. По данным исследований, почти 80% всех интернет пользователей в Кыргызстане зарегистрированны в той или иной социальной сети, что автоматически повышает видимость всех статей в такого рода СМИ. Отдельно можно рассматривать так называемые интернет-блоги. Соответственно в результате информатизации общества, в Кыргызстане сформировались предпосылки для построения информационного общества. Однако, вместе с формированием информационного общества появилась также необходимость выработки политических механизмов обеспечения информационной безопасности.

Данная проблема обусловлена тем, что общество прошло к пониманию того что при конфронтации различных государств, можно достигнуть цели не только с помощью физического истребления людских и / или материальных ресурсов противника. 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 направленна на раскол общества. Такого рода информацию условно можно назвать «информационным оружием», и с ее помощью становится возможным нанесение ущерба жизненно значимым интересам государства, причем ущерб этот может быть значительным по своей деструктивности. К сожалению законодательная база в Кырызской Республике оказалась не подготовленной к распространению информации через сети, такие как Интернет, где сигнал распространяется вне зависимости от государственных границ. Например, согласно Статьи 1 Закона Кыргызской Республики «О средствах массовой информации», новостные интернет-порталы определены как «иные способы распространения», и, так как в сети действует другой механизм распространения информации, в законе они не отображены. Удар может быть нанесен практически во все сферы жизне-деятельности государства, а именно: подорвать международный статус страны - по престижу, по системе сотрудничества с другими странами; либо внутри самого государства – например, путем дискредитации органов власти и управления, что может привести к созданию атмосферы нестабильности и напряженности в обществе, что, в свою очередь, может привести к инициации забастовок или других акций протеста; информацией можно спровоцировать конфликты внутри общества, такие как социальные, политические, национальные или религиозные, что в итоге приведет к созданию атмосферы бездуховности и безнравственности, негативного отношения либо игнорирования культурного и исторического наследия общества. Таким образом, разрушительное воздействие информационного оружия 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. Таким образом, изучение теории информационной безопасности и обеспечение ее применения на практике становится актуальной задачей не только для государственных органов, но и для научных кругов в Республике.

Актуальность данной работы состоит еще и в том, что в современной отечественной литературе больше изучаются общие проблемы национальной безопасности на примерах суверенных, переходных обществ, в то время как исследования по информационной безопасности практически отсутствуют. Поэтому попытка диссертанта состоит именно в том, чтобы проанализировать взаимосвязь национальной безопасности с информационной безопасностью,

определить информационную безопасность, как составную часть национальной безопасности.

Итак, в концептуальном виде актуальность данного исследования состоит в том, что на примере суверенного Кыргызстана проанализированы процессы информационной безопасности страны, выявлены политические механизмы в преодолении современных вызовов и угроз, а также рассмотрены методологические, теоретические и практические вопросы исследуемой темы.

Связь темы диссертации с крупными научными программами и основными научно-исследовательскими работами. Выбранная тема диссертационного исследования является инициативной.

Цель диссертационной работы – выявление форм и методов политических механизмов по обеспечению информационной безопасности Кыргызской Республики.

Цель предполагает решение следующих **задач:**

1. Изучить теоретические подходы в исследовании информационной безопасности как составной части национальной безопасности в политической науке и разработать дефиниции ключевых категорий информационной безопасности.

2. Рассмотреть сущность информационной сферы кыргызстанского транзитного общества.

3. Раскрыть содержание информационной политики Кыргызской Республики в условиях демократизации общества.

4. Сделать сравнительный политико-правовой анализ обеспечения информационной безопасности КР и стран СНГ.

5. Выявить определяющие тенденции и перспективные пути безопасности в информационной сфере Кыргызстана.

Научная новизна исследования, в первую очередь обусловлена комплексным подходом к рассмотрению проблемы политических механизмов обеспечения и поддержания состояния информационной безопасности в Кыргызской Республике в условиях демократизации общества:

- на основе теоретического анализа представлено современное понимание информационной безопасности как социально-политического явления;

- впервые в отечественной политической науке исследуется информационная безопасность как структурообразующий элемент системы национальной безопасности, дано теоретическое объяснение этого феномена, раскрыты генезис, содержание и функции;

- раскрыты внешние и внутренние угрозы, влияющие на политику безопасности в информационной сфере;

- сделан сравнительный анализ политико-правового содержания информационной безопасности КР и стран СНГ. Проведен обзор законодательств стран Содружества Независимых Государств по информационной безопасности. Были собраны данные по странам и на основе этих данных проведен сравнительный анализ законодательств. В первую очередь был проведен обзор конституций государств участниц СНГ. В конституции каждой страны были изучены главы, посвященные

обеспечению информационной безопасности не только на уровне государства, но и гарантии обеспечения персональной информации граждан, предприятий и организаций, государственных струкктур и подразделений и государства в целом;

- рассматриваются особенности безопасности в информационной сфере в условиях демократизации кыргызстанского общества;

- раскрыты политические механизмы совершенствования безопасности в информационной сфере и необходимость разработки Концепции информационной безопасности КР.

Практическая значимость полученных результатов. Материалы диссертационного исследования могут быть использованы для дальнейшего изучения проблем политических механизмов обеспечения информационной безопасности, в практической деятельности государственных органов по координации работ в сфере информационной безопасности; при разработке государственной Концепции информационной безопасности, а также в учебном процессе высших учебных заведений на курсах политологии, журналистики и государственному управлению.

Основные положения, выносимые на защиту:

1. На сегодняшний день, в условиях глобализации информационная безопасность каждого отдельного государства приобретает первостепенное значение, причем особо важной она становится в таких сферах жизни общества как политическая, социально-экономическая, военно-техническая и в других сферах. В современных условиях, с учетов темпов развития ИКТ, ее необходимо считать одним из системообразующих компонентов системы национальной безопасности в целом, так как развитие ИКТ привело к повышению значимости информационной сферы в жизни общества. Из вспомогательной сферы она, постепенно переходит в разряд приоритетных сфер политического управления.

2. 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.

3. В качестве основы государственной политики обеспечения и поддержания состояния информационной безопасности должны выступать методологические и научные разработки, которые должны быть систематизированы и объединены в целостную концепцию. Эта концепция может включать в себя совокупность национальных интересов и ценностей общества. Также, должны быть изучены цели информационного взаимодействия органов государственной власти во всех сферах жизнедеятельности общества и государства. В добавок, должны быть изучены тактика и стратегия решений по управлению, внедряемых государственной

властью, методы реализации принятых решений, включая процессы технологического обеспечения информационного взаимодействия.

4. 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 информации 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.

5. С расширением и развитием информационного пространства информационная война в современном мире все больше и больше становится основным видом борьбы за власть, влияние и интересы. Особенности информационной борьбы проявляются и в Кыргызской Республике. Анализ проблемы приводит к выводу о том, что есть попытки установления иностранного контроля над интеллектуально-информационной сферой Кыргызстана.

6. 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.

Личный вклад соискателя определяется основными научными положениями и выводами диссертации на основе политологического анализа такого феномена, как информационная безопасность государства.

Апробация работы была проведена путем обсуждения ее на заседании кафедры философии и гуманитарных дисциплин Института гуманитарных знаний Кыргызского государственного университета им. И.Арабаева, на заседании кафедры политологии Кыргызского национального университета им. Ж.Баласагына и на расширенном заседании Отдела политологии и проблем государственного управления Института философии и политико-правовых исследований Национальной Академии наук Кыргызской Республики и была рекомендована к публичной защите. Ряд положений исследования отражены в докладах и выступлениях соискателя на различных конференциях, круглых столах, семинарах, а именно: Обеспечение информационной безопасности страны – главное условие сохранения государства // Становление и развитие психологической науки в Кыргызстане: проблемы и перспективы психологии в системе образования: Материалы международной научно-практической конференции. – Вестник КГУ им. И. Арабаева. – Вып. № 3. − Бишкек, 2015;

Психологические аспекты создания имиджа в политике // Таможенная политика и национальная безопасность: Сборник материалов международной научно-практической конференции, посвященной 75-летию доктора политических наук, проф. Шалтыкова А.И.– Алматы, 2014; Роль политического менеджмента в современных условиях // Актуальные проблемы педагогического образования и науки в Кыргызской Республике: Материалы научно-практической конференции молодых ученых КГУ им. И.Арабаева. – Вестник КГУ им. И.Арабаева. – Бишкек, 2014; Государственное управление как основная функция государственной службы // Религия и образование: современное состояние и перспективы развития: Материалы международной научно-практической конференции. – Вестник КГУ им. И. Арабаева. – Вып. № 5. – Бишкек, 2012; Разработка управленческих решений в системе менеджмента // Проблемы и перспективы устойчивого развития независимого Кыргызстана: Научно-практическая конференция, посвященная 20-летию независимости Кыргызской Республики. – Вестник КГУ им. И. Арабаева. – Вып. № 3. – Бишкек, 2011; Основные объекты информационного пространства// Проблемы совершенствования управления природными и социально-экономическими процессами на современном этапе: IV международная научно-практическая конференция. – Вестник КГУ им.И.Арабаева.- Вып. №.- Бишкек, 2018.

Полнота отражения результатов диссертации в публикации. Основные положения диссертации нашли отражение в 12 публикациях автора. Из них 3 статьи опубликованы в зарубежных научных журналах.

Структура диссертационного исследования. Диссертация состоит из введения, трех глав, шести параграфов, заключения, списка использованной литературы. Общий объем диссертационной работы составляет 170 страниц.

ОСНОВНОЕ СОДЕРЖАНИЕ ДИССЕРТАЦИИ

Во **введении** обосновывается актуальность избранной темы исследования, приводится обзор источников и литературы по исследуемой проблеме, раскрывается теоретико-методологические аспекты исследования, даются цель, задачи, научная новизна, практическая значимость работы, излагаются основные положения, выносимые на защиту, а также показаны результаты их апробации.

Первая глава **«Теоретико-методологические основы исследования информационной безопасности»** раскрывает теоретико-методологические основы исследования информационной безопасности, и состоит из двух параграфов.

В первом параграфе **«Теоретические аспекты исследования информационной безопасности»** осуществлена концептуализация понятий «безопасность», «информация», «информационная безопасность», «национальная безопасность», «информационная сфера», «угрозы», «информационная война», «информационное общество». Для этого были использованы труды Э. Шеннона, И.Л. Бачило, С.И. Семилетова, А.А. Фатьянова, А.А.Стрельцова, В.Л.Пирумова, К.С.Гаджиева , Н.А.Нартова,

А.Г.Дугина , О.А.Судоргина, Шерстюка В.П. Черешкина Д.С. , Смолян Г.П., Панарина И.Н., Почепцова Г.Г., Прохожева А.А., Расторгуева С.П. и др.

Некоторые аспекты проблемы национальной и информационной безопасности Кыргызстана раскрываются в работах таких кыргызстанских ученых как: А.А.Акунова [20-21], М.Т.Артыкбаева [24-25], К.Б. Бектурганова [29], Ж.Б.Бокошова [31], А.Д.Дононбаева [45], К.И.Исаева [138], А.К.Керимбековой [139], О.А.Молдалиева [75], Дж.А. Омукеевой [84], Б.Орунбековым [83], Ж.С. Сааданбекова [102], Н.А.Сейдакматова [151], Р.Т.Улукова [116-117]. А.Б.Элебаевой [158].

В первой половине XX века известный американский ученый Г.Моргентау определил состояния безопасности через анализ его угроз и интересов. Такой подход при анализе национальной безопасности заложен во многих стратегических документах, в частности в Законе Кыргызской Республики от 26 февраля 2003 года № 44 «О национальной безопасности», где понятие безопасности раскрывается через такой же угол зрения.

Можно сформулировать следующие основные определения «информационной безопасности», встречаемые в литературе:

– состояние защищенности информационного пространства, обеспечивающее его формирование и развитие в интересах граждан, организаций и государства;

– состояние инфраструктуры системы (объекта, государства), при котором информация используется строго по назначению и не оказывает негативного воздействия на систему (объект, государство) при ее использовании;

– состояние информации, при котором исключается или существенно затрудняется нарушение таких ее свойств, как секретность, целостность и доступность.

Как было показано выше, с термином информационной безопасности непосредственно связанны такие понятия, как информационная война, информационное противоборство, информационное пространство (инфосфера), информационная преступность и т.д., причем, все эти понятия можно применять к различным уровням анализа системы. Интересно заметить, что информационная безопасность является довольно таки хрупким качеством системы, т.к. набор угроз безопасности информации и ее носителей, варьируется от информационных агрессий и войн, информационного и кибертерроризма до нарушения прав человека как угрозы информационной безопасности человека и общества.

Автор, под информационной безопасностью понимает состояние защищенности наиболее существенных интересов личности, общества и государства от внешних и внутренних угроз информационного характера во всех сферах общественной жизни.

Таким образом, автором на основании исследования теоретических аспектов информационной безопасности, были сделаны следующие выводы:

-безопасность государства содержит в себе различные аспекты, в число которых входит и информационная безопасность. Обеспечение информационной безопасности именно в начале XXI века, во времена,

характеризующиеся все усложняющимся применением методов пропаганды, становится еще более актуальной задачей, чем ранее. Это обусловливается включением стран в то или иное информационное пространство: глобальное, региональное или образующееся при взаимодействии отдельных стран.

- с наступлением новой эпохи развития человеческой цивилизации, связанной со становлением информационного общества, происходят постепенные изменения во всех сферах жизни человека и общества. Важными составляющими содержания наступающей эпохи являются информация, информационные технологии, преобразующие внутреннюю структуру, содержание и внешний облик человеческой цивилизации.

- информационное пространство представляется гибкой социальной субстанцией: с одной стороны, формирующейся извне, а с другой – оказывающей колоссальное воздействие на охваченных ею индивидов. Структурными компонентами являются СМИ, посредством которых и происходит его формирование, и общественное мнение, отражающее рефлексию общественно значимых фактов населением.

- изменяется представление о соотношении факторов могущества государств. Если раньше считалось, что именно военная сила определяет уровень могущества государства, то в XX веке мы уже наблюдали выдвижение на первый план экономической силы. Сегодня же складывается новое представление о главном факторе могущества государства, которым в XXI веке становится информация. Обладание государством такой способностью открывает для него путь к дальнейшему наращиванию на совершенно новой основе своей экономической, политической и военной мощи. Наряду с традиционным вооружением и военной техникой во многом являющимися факторами сдерживания, вследствие глобализации, становления глобального информационного пространства закономерным явлением в начале XXI века явилось информационное противоборство, целью которого является воздействие на население с целью манипуляции общественным мнением. Таким образом, реальным оружием в XXI веке становятся информация и информационное оружие, что заставляет говорить о всевозрастающих угрозах в сфере информационной безопасности.

Всё вышеперечисленное и изложенное убедительно свидетельствует, с одной стороны, о всеобъемлющем характере международной информационной безопасности, а с другой, - о неразрывной связи информационной безопасности каждого отдельного государства с безопасностью всего международного сообщества в целом. Последняя реальность подтверждается логикой и тенденцией современных интеграционных процессов. Говоря другими словами, стало очевидным, что в нынешних условиях под информационной безопасностью уже недостаточно понимать лишь физическую и морально-политическую способность государства защитить себя от внешних источников угрозы враждебной пропаганды, поскольку обеспечение информационной безопасности во многих отношениях стало производным от международной безопасности и оказалось с последней в диалектической взаимосвязи. Следует также констатировать, что успешное решение проблемы безопасности сегодня

требует применения комплексного подхода и участия в этом процессе практически всех государств вне зависимости от их различия в общественно-политическом строе и социально-экономическом развитии.

Во втором параграфе первой главы **«Методологические основы информационной безопасности»** рассматриваются методы исследования информационной безопасности. При анализе проблемы использовались общенаучные и специальные методы исследования.

Так следует подчеркнуть, что явление - информационная безопасность представляет собой интегрированное, междисциплинарное «образование, а потому было трудно» осознать, какими научными методами можно было бы определить его сущность. Научными методами оказались: системный анализ, политико-культурный подход, междисциплинарный анализ, сравнительный метод, социологический метод.

Поскольку информационная безопасность, является междисциплинарным объектом изучения, соискателем был использован междисциплинарный анализ. Важное место в арсенале политических исследований занимает междисциплинарный подход. Его необходимость определяется, прежде всего, тем, что политология представляет собой научную дисциплину, располагающуюся на стыке других социальных и гуманитарных наук.

Содержание информационной безопасности в контексте системного анализа представляет собой комплекс взаимосвязанных структурных элементов. К ним относятся - предмет, угрозы, субъекты, объекты, принципы и механизм обеспечения информационной безопасности. Исследование информационной безопасности с позиций системного подхода позволяет увидеть сколь сильно отличается научное, пусть и предварительное, понимание этой безопасности от обыденного. В повседневной жизни, вплоть до настоящего времени, информационная безопасность понимается лишь как необходимость борьбы с утечкой закрытой (секретной) информации и распространением ложной и враждебной информации. Новые информационные опасности, особенно технического плана, в общественном сознании, к сожалению, отражены не адекватно их растущей роли.

Также в работе был использован сравнительный метод. Сравнительный метод предполагает сравнение объекта изучения по какому либо признаку. Так как предметом исследования являются политико-правовые механизмы обеспечения информационной безопасности в Кыргызской Республике, то за свойство, по которому ведется сравнение, были приняты нормативно-правовые данные по информационной безопасности в странах, входящих в состав Содружества Независимых Государств. Также, в рамках данного сравнения, применялся контекстный метод исследования.

Для изучения безопасности как таковой, в мировой практике используется также так называемый контентный анализ. В данном виде анализа изучается контент, то есть содержание того или иного источника. С развитием информационных и коммуникационных технологий, роль данного вида исследования выходит на первый план, особенно если учесть, какой 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 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 коммуникационной инфраструктурой оказались не готовыми к угрозам такого рода информационной, и, как следствие, национальной безопасности.

Глава вторая **«Политико-правовой анализ обеспечения информационной Кыргызской Республики»** рассматривает отдельные аспекты информационной безопасности в системе национальной безопасности, учитывающие интересы личности, общества и государства в информационной сфере и создающие политико-правовое содержание информационной политики Кыргызской Республики. Также в данной части работы проведен обзор законодательств стран Содружества Независимых Государств по политико-правовым механизмам обеспечения информационной безопасности. Были собраны данные по странам СНГ и на основе этих данных проведен сравнительный анализ законодательств.

В первую очередь был проведен обзор конституций государств участниц СНГ. В Конституции, законах касающихся обеспечения информационной безопасности каждой страны были изучены главы, посвященные обеспечению информационной безопасности не только на уровне государства, но и гарантии обеспечения защиты персональной информации граждан, предприятий и организаций, государственных структур и подразделений, и государства в целом.

Однако многие источники отмечают, что политико-правовое обеспечение все же не достаточное. Согласно [201], на формирование политико-правового базиса в области обеспечения информационной безопасности влияют существующие культурные традиции, социально-психологическихе архетипы, инерции политического опыта, разные модели функционирования масс-медиа и многое другое. Не последнюю роль при этом играет вопрос компьютерной грамотности населения, и в первую очередь – представленность ИТ специалистов в государственных структурах.

Политико-правовое содержание информационной безопасности страны как неотъемлемая часть единой системы противодействия угрозам национальных интересов страны в информационной сфере достаточно не развито, что существенно сокращает возможность Кыргызстана по противостоянию вызовам информационной безопасности и усилению национальной безопасности государства в целом.

В первом параграфе **«Сравнительный анализ политико-правового содержания информационной безопасности Кыргызской Республики и стран СНГ»** рассматриваются нормативно-правовые документы Кыргызской

Республики. В частности проводит анализ следующих нормативно-правовых документов: Конституции Кыргызской Республики, Концепции национальной безопасности Кыргызской Республики, Законов Кыргызской Республики: «О защите государственных секретов», «Об информатизации», «О гарантиях и свободе доступа к информации», «О средствах массовой информации», «О правовой охране программ ЭВМ и баз данных», «Об электрической и почтовой связи», «Об электронной цифровой подписи», «Об информации персонального характера», «О доступе к информации».

Проведен обзор законодательств стран Содружества Независимых Государств по политико-правовым механизмам обеспечения информационной безопасности. Были собраны данные по странам СНГ и на основе этих данных проведен сравнительный анализ законодательств. Современный этап развития общества для Кыргызской Республики характеризуется возрастающей ролью ее информационной сферы, представляющей собой арену для деятельности органов государственной власти и управления, связанную с созданием, преобразованием и потреблением информации.

Информационная безопасность Кыргызской Республики обеспечивается следующими органами государственной власти: Президентом; законодательным органом; судебной властью; Советом безопасности; исполнительной властью, включая межведомстсвенные государственные комиссии, создаваемые Президентом и Правительством; органами местного самоуправления, общественными объединениями, гражданами, принимающими в соответствии с законодательством Кыргызской Республики участие в решении задач обеспечения информационной безопасности Кыргызской Республики.

В Кыргызской Республике, также были образованы специальные государственные органы, для совершенствования обеспечения информационной безопасности: Национальное агентство информационных ресурсов (2006г.); Межведомственная комиссия по вопросам обеспечения информационной безопасности (2007г.); Консультативный совет Государственного агентства связи при Правительстве Кыргызской Республике (2010г.); Совет по информационной политике при Министерстве культуры, информации и туризма (2014г.); Государственный Комитет информационных технологий и связи (2016 г.).

Однако отмечает автор, очевидно, что этого недостаточно, поскольку все доступные нормативно-правовые акты и проект концепции рассматривают информационную безопасность больше в технологическом аспекте, подразумевающем обеспечение защиты национальных ресурсов, систем и инфраструктуры от неавторизованного доступа, использования, раскрытия, изменения, уничтожения или подобных действий. В вышеприведенных документах четко не прописаны механизмы и превентивные меры, по защите от негативных целенаправленных информационных атак, связанных с деструктивным информационным воздействием на общественное сознание и государственные институты, распространением недостоверной или умышленно

искаженной информации, что может нанести ущерб национальным интересам Кыргызской Республики.

В законе Кыргызской Республики «О защите профессиональной деятельности журналиста» описана ответственность журналистов за распространении недостоверной или умышленно искаженной информации, однако этот закон регулирует ответственность только журналистов, и не учитывается ответственность пользователей интернет пространства и блогеров, которые приобретают все большую популярность и могут нанести ущерб не только отдельно взятым гражданам Кыргызской Республики, но также обществу и национальным интересам Кыргызской Республики. Также, в нашей стране не предусмотрены стандарты по шифровке данных, стандарты цифровой подписи. По умолчанию в Кыргызстане действуют стандарты, пронятые ГОСТ Российский Федерации. Учитывая данные обстоятельства, соискатель предлагает рассматривать информационную безопасность страны, как обеспеченное политическими, организационными и правовыми мерами, состояние защищенности жизненно важных интересов личности, общества и государства в информационной сфере от внутренних и внешних угроз, способных нарушить фундаментальные, материальные и духовные ценности, их устойчивое развитие.

Данным определением, соискатель четко показывает неделимость информационной безопасности государства, которая должна быть равной для всех субъектов информационного взаимодействия. Автор считает, что принятие Концепции информационной безопасности, специального Закона «Об информационной безопасности», устранит недостатки действующего законодательства, а также будет способствовать развитию политических механизмов обеспечения информационной безопасности в Кыргызской Республике.

Во втором параграфе второй главы **«Информационная безопасность − составная часть национальной безопасности КР»** рассматривается особое место информационной безопасности в системе национальной безопасности страны.

В современных условиях становления мирового информационного пространства, перед Кыргызстаном остро встает задача надежной защиты собственного информационного пространства от любого вида информационной агрессии.

В диссертационной работе соискатель уточняет, что информационная безопасность страны является выражением национальных интересов Кыргызской Республики. По мере развития ИКТ, во всех составляющих национальной безопасности вес информационных факторов непрерывно растет. Частично это обусловлено и ростом интернет технологий, так как в интернет пространстве, как известно, нет физических границ, с помощью которых можно было бы оградить национальные интересы. Интернет стал не просто системой, а социально-технической системой систем. Все аспекты человеческой жизни, а также информационный поток в государственных структурах и ведомствах в большей или меньшей степени зависят от

программного обеспечения и информационно-коммуникационных технологий. С растущей ролью этой системы растет число преступлений, совершенных с помощью компьютерных технологий, и таким образом, когда речь идет об обмене информацией государственного значения, растут риски для информационной безопасности государства.

Хотя были предложены многие модели для анализа киберпреступности, в человеческом сознании преступление, совершенное в киберпространстве, не является преступлением, которое должно быть наказано.

Сам термин «киберпреступление» был определен как «событие, которое происходит на компьютере или в сети, которое должно привести к не разрешенному действию», то есть как любое действие инсайдера или аутсайдера, который ставит под угрозу безопасность человека, организации или государства. Согласно западным источникам по техническим наукам, кибер-атаки могут влиять на данные, процессы, приложения и компьютерную сеть.

Хотя кибер-атака и может быть определена, до сих пор нет общепринятого определения киберпреступности. По данным Управления Организации Объединенных Наций по наркотикам и преступности, «киберпреступность – это акты против конфиденциальности, целостности и доступности данных, компьютеров и компьютерных систем». Однако, в целом, любое преступление, совершенное через Интернет или другую какую либо компьютерную сеть может быть определена как киберпреступность.

В настоящее время из-за развития информационных технологий многие преступления имеют цифровой «след». Незаконные действия, проводимые в киберпространстве, являются относительно новыми формами преступности.

По мнению соискателя, обособление информационной безопасности в качестве нового вида национальной безопасности, является следствием рассмотренных процессов, так и необходимым условием осуществления государственной политики обеспечения безопасности страны в целом. Эффективно противостоять информационным угрозам по отношению последним может лишь хорошо организованная государственная система обеспечения информационной безопасности, осуществляемая при полном взаимодействии всех государственных органов, негосударственных структур и граждан. Такой подход может быть реализован лишь после разработки своевременной Концепции информационной безопасности Кыргызской Республики. В противном случае выявление и устранение сложных информационных угроз национальной безопасности, будет сопровождаться большими трудностями, особенно если эти задачи выполняют отдельные структуры без эффективного взаимодействия.

Рассматривая информационную безопасность в системе национальной безопасности, стоит отметить об их сложной взаимосвязи и взаимодействии. Ибо, информационная безопасность затрагивает многие проблемы национальной безопасности: военную, экономическую, политическую, этническую, идеологическую и другие сферы безопасности государства.

Глава третья **«Информационная безопасность – фактор безопасности в политической сфере Кыргызстана»** рассматривает политические механизмы,

предопределяющие угрозы информационной безопасности, раскрывает основные внешние и внутренние факторы, влияющие на политику безопасности в информационной сфере Кыргызстана, а также анализируются политические механизмы обеспечения информационной безопасности и возможные пути ее реализации.

Первый параграф - **«Основные внешние и внутренние факторы, влияющие на политику безопасности в информационной сфере Кыргызстана»**

Сегодня информация имеет непосредственное отношение к политическим процессам в мире. В свете развития ИКТ информация стала восприниматься как продукт или товар, чья ценность определяется ее содержанием. Это может быть научная информация, личная информация, статистическая или экономическая информация. В зависимости от ценности ее содержания это может быть информация для общего доступа, для служебного доступа, секретная информация (по уровням) и т.д. Государство, в лице структур политического и иного управления, всегда находится в процессе сбора, накопления, переработки и распространения информации. Вся эта информация необходима для осуществления эффективных политических воздействий или решения экономических задач. Информация сама по себе не может быть определена как хорошая или плохая, однако информация может быть применена как для положительного, так и дестабилизирующего, негативного влияния на общество. Опыт новейшей истории показывает, что информация вполне может служить источником политической и социальной угроз. Именно для этого и необходимы политико-правовые механизмы регулирования информации и информационных потоков. Основной акцент при этом делается на деятельность средств массовой информации (СМИ). Поэтому отдельным пунктом идет Закон Кыргызской Республики "О защите профессиональной деятельности журналиста" где описана ответственность журналистов за распространении недостоверной или умышленно искаженной информации от 5 декабря 1997 года N 88. Для деятельности иностранных журналистов было разработано Положение об аккредитации корреспондентов средств массовой информации иностранных государств на территории Кыргызской Республики от 19 апреля 2000 года N 215, где в пункте 2 главы I прописано, что правовое положение и профессиональная деятельность аккредитованных в Кыргызской Республике иностранных корреспондентов регулируются нормативными правовыми актами Кыргызской Республики и международными договорами Кыргызской Республики.

До этого автор попытался собрать и систематизировать потенциальные угрозы информационной безопасности кыргызстанского общества. Обзор литературы и анализ контента информационных порталов позволил выявить следующие угрозы:

-Многонациональность и многоконфессиональность – угроза напряженности между разными группами. Кыргызстан является многонациональной и многоконфессиональной страной. Согласно данным национального статистического комитета КР, у нас проживает более 80

народностей. При этом именно по этой причине обеспечение информационной безопасности приобретает особую важность и требует повышенного внимания и внимательности, так как недостаточное регулирование информационных потоков может стать причиной напряженности между этническими группами.

-Эфирная (информационная) экспансия информационного пространства Кыргызстана зарубежными каналами или финансовая зависимость некоторых локальных информационных агентств от иностранных спонсоров – опять-таки информация может оказывать эмоционально-психологическое воздействие на те или иные события, что может негативно повлиять на граждан страны. Сюда же можно отнести и влияние через информационные потоки религиозно-экстремистских и террористических организаций.

-Технологическая зависимость – обусловлена тем, что все технологии в области сбора, хранения, обработки и передачи информации проводятся на технологии, разработанной и собранной за рубежом. Особенно остро этот тип угроз может ощущаться, когда речь идет о технике и технологиях, используемых государственными структурами. Автор хотел бы еще раз подчеркнуть важность образования и развития науки как одну из мер для устранения угроз. Необходимо развитие отечественных наукоемких, высокотехнологичных отраслей промышленности.

-Несовершенство законов по распространению информации. Например, согласно Статьи 1 Закона Кыргызской Республики «О средствах массовой информации», новостные интернет-порталы определены как «иные способы распространения», и, так как в сети действует другой механизм распространения информации, в законе они не отображены.

К сожалению, степень опасности, суть которой состоит в неограниченной возможности влияния на человека, еще не вполне осознана в кыргызстанском обществе. Новейшая информационная технология позволяет не только «подключиться» к каждому, но и «выключить» каждого из активного процесса социальной деятельности, личной жизни - любое обращение к средствам связи и средствам передачи информации фиксируется в памяти вычислительных машин, что позволяет проследить за работой, коммерческими операциями, покупками и т.п. каждого человека. И это не гипотетические предположения, а уже существующая реальность.

Учитывая опыт других стран - соседей соискатель считает, что угрозы информационной безопасности Кыргызской Республики представляют собой множество условий и факторов, совокупность которых представляет реальную или потенциально существующую опасность нанесения ущерба субъектам и объектам информационного пространства страны. Угрозы информационной безопасности могут содержать субъективный и объективный характер. Они выражаются в действиях, явлениях, процессах (или их совокупности). Могут исходить от внутренних и (или) внешних источников по отношению к информационной сфере Кыргызской Республики.

Внешней составляющей информационной угрозы является совокупность мероприятий информационного воздействия на распространение идеологии другого государства и иноэтничного населения, передачи по телевидению и

радиовещанию, показывающие превосходство своего государства и осуждающие политическую, экономическую и социальную ситуацию в Кыргызской Республике и т.д.

Как отмечалось выше, огромное влияние на состояние защищенности национальных интересов в информационной сфере оказало развитие ИКТ, благодаря которым появилось такое понятие как электронные масс-медиа, социальные сети и блоги. Если деятельности электронных масс-медия подпадает под действие закона Кыргызской Республики «О защите профессиональной деятельности журналиста», бесконтрольность информации на личных страницах и блогах интернет пользователей может оказать негативное влияние на состояние информационной безопасности страны, тем более что пользователями в основном являются молодежь и образованные люди с активной жизненной позицией. Однако автор считает необходимым подчеркнуть, что в Законе Кыргызской Республики «О средствах массовой информации», «к средствам массовой информации относятся газеты, журналы, приложения к ним, альманахи, книги, бюллетени, разовые издания, предназначенные для публичного распространения, имеющие постоянное название, а также теле- и радиовещание, кино- и видеостудии, аудиовизуальные записи и программы, выпускаемые государственными органами, информационными агентствами, политическими, общественными и другими организациями, частными лицами», но нет упоминания новостных интернет порталов [10]. Электронные масс-медиа попадают только под раздел «… иные способы распространения». Все же, особое беспокойство вызывают социальные сети в Кыргызстане, которые могут быть использованы и используются в качестве площадки для вербовки в религиозно-экстремистские организации. К тому же в интернет пространстве Кыргызстана функционируют новостные порталы, которые придерживаются сторон каких-либо мировых держав, при этом явно или косвенно пропагандируются их взгляды. Проблема усугубляется тем, что в популярных социальных сетях можно делится и обсуждать новости новостных порталов. Конституция КР гарантирует «…что каждый имеет право свободно искать, получать, хранить, использовать информацию и распространять ее устно, письменно или иным способом» [1], однако государство должно защищать свои интересы и обеспечить информационную безопасность, что тоже не подлежит сомнению.

В связи с этим автор еще раз отмечает важность специального образования и подготовки кадров по информационной безопасности. Опять-таки, для подготовки кадров необходимо чтобы была проработана нормативно-правовая база, на основе которой будут подготовлены административные кадры, и с учетом которых будут разрабатываться технические средства для защита информации и информационного пространства Кыргызской Республики. Недостаток грамотных кадров приведет к дальнейшему усугублению информационной опасности.

Во втором параграфе третьей главы **«Построение политических механизмов обеспечения информационной безопасности и методы ее воплощения в жизнь»** раскрываются политические механизмы

информационной безопасности в Кыргызской Республике и пути ее реализации, в условиях трансформации кыргызстанского общества.

Во многих странах разработка и применение технологий и методов информационно-психологических операций, является важной задачей. Противоборство с помощью информационных атак, рассматривается как основной элемент обеспечения национальной безопасности и закреплено в специальных госпрограммах США, Великобритании, России, КНР, а также в некоторых странах ЕАЭС. К примеру, в соседнем Казахстане, в Концепции информационной безопасности до 2016 года, были четко сформулированы задачи государственной информационной политики, которая позволяет решать проблемы адекватного отражения информационно-психологической агрессии.

Следует, на наш взгляд, признать объективную необходимость законодательного ограничения (регулирования) свободы массовой информации, чем только и возможно обеспечить правовое равенство в информационных отношениях. Средствам массовой информации, выступая инструментом взаимодействия, не следует встревать между государством и обществом на пути их конфронтации, особенно ради цели - демонстрации собственной независимости, что порой и происходит в кыргызстанской действительности. Не подвластность, самостоятельность прессы вовсе не является залогом ее объективности. Общеизвестно, что пресса, поддерживающая лишь идеи собственной свободы и независимости, в перспективе перестает отражать интересы личности, общества, государства, что именно такая пресса создает ситуации информационной опасности.

В целом изучение проблем в информационной сфере, в том числе развития и формирования механизмов информационной безопасности, позволит сформулировать научно обоснованные требования к самой государственной власти, институтов, которые функционируют внутри нее. Государственным органам в данном случае необходимо осуществлять задачи стратегического плана, вести активную информационную политику, которая имеет цель - формирование в общественном сознании позитивного образа государства.

Исследования, проведенные в [205] выявили, что население не знает основ безопасности хранения и передачи, а также сбора информации в сети интернет. Также, в работе автора были выявлены факторы, влияющие на решение граждан пользоваться информационными услугами государства через интернет, готовы ли и хотят ли потребители государственных услуг – граждане КР, передавать свои данные через интернет, и какие критерии определяют готовность граждан использовать электронное правительство. Этот вопрос стал важным в свете недавнего сбора биометрических данных в Кыргызской Республике и проекта перехода к системе электронного голосования, поскольку участие в выборах зависит, наряду с другими факторами, и от восприятия гражданами электронного правительства, и естественно, оказывают огромное влияние на обеспечение информационной безопасности в стране. Что касается достоверия, респонденты с более низким уровнем доверия к правительству имеют более низкие намерения

использовать электронное правительство, в то время как у лиц с более высоким уровнем доверия есть более высокая потребность в его использовании. Кроме того, люди, которые доверяют интернету, более склонны использовать его, в то время как те, кто не доверяет интернету, не хотят использовать электронное правительство. Этот результат подтверждает наличие взаимосвязи между осознанием безопасности граждан и их готовностью использовать правительственные онлайн-сервисы. Как уже отмечалось выше, для повышения доверия необходимо разработать правовые механизмы, повышающих доверие к этой глобальной информационной инфраструктуре, ужесточения статей уголовного кодекса и создание механизмов, которые должны обеспечивать проведение расследования и уголовное преследование киберпреступности. Также включая киберпреступления, которые совершены в рамках юрисдикции одной страны, но имеющих последствия в другой стране.

Находим целесообразным определить следующие направления:

— создать единый орган, координирующий безопасный сбор, хранение, обработку, передачу и распространение данных. Для этого необходимо в первую очередь разработать нормативно правовую базу, в которой были бы определены уровни секретности информации, определены какого рода информация относится к тому или иному уровню, необходимо также рассмотреть и стандартизировать криптографические средства защиты конфиденциальности и целостности информации. На основе этой базы необходимо разработать политико-правовые механизмы, регулирующие деятельность данных структур;
— подписать соглашения с другими государствами в области сотрудничества по предотвращению киберпреступлений, а также воздействия религиозно-экстремистских и террористических группировок через ИКТ;
— с возрастанием роли Интернета в информационном пространстве возникает необходимость защиты прав и свобод человека и общества от информации, пропагандирующей насилие и жестокость, навязывания им ложной и недостоверной информации, от целенаправленного формирования негативного мировоззрения молодого поколения. При этом источники внешних угроз могут находиться вне юрисдикции законодательства КР, что существенно затрудняет применение системы правовых мер;
— как было отмечено много раз, необходимо провести подготовку кадров по противодействию техническим разведкам, защиты от информационного оружия и совершенствования законодательной базы в данной сфере.

ВЫВОДЫ

Подводя итоги нашего исследования, необходимо отметить, что нами не ставилась цель объять все многообразие проблем, поднятых под избранную тематику в ее развернутом виде.

В заключении подведены итоги проведенного исследования и сделаны следующие выводы:

1. В конце XX века проблема безопасности обретает все более актуальный научно-практический интерес. Появившиеся независимые, суверенные государства после распада Советского Союза, сформировали свою концепцию национальной безопасности, одним из главных видов которой представляется информационная безопасность.

2. Обеспечение эффективной национальной безопасности в информационной сфере кыргызстанского общества, является одной из приоритетных задач государства. Это возможно через усиление процессов общенационального единства, укрепление государственности и структурирование интересов и целей различных групп.

3. Современные вызовы и угрозы, представляют опасность для национальной безопасности во всем мире, в том числе и для Кыргызстана. В условиях глобализации можно также наблюдать проявления экспансии некоторых стран в информационной сфере, на идеологическом, финансово-экономическом уровнях. В этих условиях необходима защита информационной безопасности через формирование и развитие политических механизмов.

4. Современная информационная безопасность государства, в том числе и Кыргызской Республики – это состояние защищенности национальных интересов страны в информационной сфере. Под данное определение подпадают не только интересы самого государства, а также ее граждан и общества в целом. Эффективность государственной политики в области информационной безопасности, зависит от комплексного использования всей палитры средств и методов предупреждения, ликвидации современных внутренних и внешних вызовов и угроз. Такой подход может быть реализован лишь после разработки своевременной концепции информационной безопасности Кыргызской Республики.

5. В современных условиях, процесс развития феномена информационной безопасности и политики национальной безопасности, находится в условиях постоянного изменения. Говоря о современном определении понятия «безопасность», необходимо подчеркнуть, что оно связано, как показало исследование, напрямую с современным порядком мироустройства в области безопасности.

Исходя из вышеизложенного, можно заключить, что для успешного обеспечения сферы информационной безопасности государства ее граждан, необходимо принять во внимание, следующее:

1. Обеспечение информационной безопасности Кыргызской Республики – это обеспечение возможностей и способностей в кыргызстанском обществе

осуществлять внутреннюю и внешнюю политику во имя интересов личности, общества, государства.

На основе авторского сравнительного политико-правового анализа кыргызской и стран СНГ по обеспечению информационной безопасности был проведен обзор законодательной базы государств участниц СНГ. В Конституции, законах касающихся обеспечения информационной безопасности каждой страны были изучены главы, посвященные обеспечению информационной безопасности не только на уровне государства, но и гарантии обеспечения защиты персональной информации граждан, предприятий и организаций, государственных структур и подразделений, и государства в целом.

Однако многие источники отмечают, что политико-правовое обеспечение все же не достаточное. Так на формирование политико-правового базиса в области обеспечения информационной безопасности влияют существующие культурные традиции, социально-психологическихе архетипы, инерции политического опыта, разные модели функционирования масс-медиа и многое другое.

2. Теория и практика либеральной демократии, показывает в реальной политической действительности, что создание необходимых условий для защиты независимости, поддержания законности и правопорядка в стране, является основной целью безопасности в информационной сфере. Для повышения доверия необходимо разработать правовые механизмы, повышающих доверие к этой глобальной информационной инфраструктуре, ужесточения статей уголовного кодекса и создание механизмов, которые должны обеспечивать проведение расследования и уголовное преследование киберпреступности. Также включая киберпреступления, которые совершены в рамках юрисдикции одной страны, но имеющих последствия в другой стране.

3. Главную роль при обеспечении информационной безопасности играет вопрос компьютерной грамотности населения, и в первую очередь – представленность IT специалистов в государственных структурах. Очень важно поддерживать уровень компетентности ответственных лиц за информационную безопасность Кыргызской Республики. Так как налаженная безопасная информационная среда, способствующая обратной связи между народом и властью, создает предпосылки для политической стабильности, повышения конкурентности государства в глобальном мире. А это в свою очередь, приводит к соответствующей моменту корректировке целей или постановке совершенно новых задач.

4. Поддерживать и поощрять возможности государственных и общественных средств массовой информации, для того чтобы своевременно предоставлять достоверную и сбалансированную информацию для всех граждан Кыргызстана и зарубежной аудитории. А также обеспечить государственную поддержку деятельности отечественных информационных агентств по продвижению их продукции на внешний рынок. Но также следует, на наш взгляд, признать объективную необходимость

законодательного ограничения (регулирования) свободы массовой информации, чем только и возможно обеспечить правовое равенство в информационных отношениях. Средствам массовой информации, выступая инструментом взаимодействия, не следует встревать между государством и обществом на пути их конфронтации, особенно ради цели - демонстрации собственной независимости, что порой и происходит в нашей действительности. Не подвластность, самостоятельность прессы вовсе не является залогом ее объективности. Общеизвестно, что пресса, поддерживающая лишь идеи собственной свободы и независимости, в перспективе перестает отражать интересы личности, общества, государства, что именно такая пресса создает ситуации информационной опасности.

5. Усовершенствовать законодательную базу по средствам массовой информации, так как законодательная база в Кырызской Республике оказалась не подготовленной к распространению информации через сети, такие как Интернет, где сигнал распространяется вне зависимости от государственных границ. Например, согласно Статьи 1 Закона Кыргызской Республики «О средствах массовой информации», новостные интернет-порталы определены как «иные способы распространения», и, так как в сети действует другой механизм распространения информации, в законе они не отображены.

6. Развивать отрасль информационного права и кадровую политику по данной проблеме в Кыргызстане. Крайне необходимо организация такой системы подготовки кадров, работающих в сфере информации и информационных технологий (госзаказ), чтобы они не были подвержены недружественному влиянию извне и теоретически подкованы в области информационной безопасности.

Соискатель считает, что основными задачами по обеспечению информационной безопасности Кыргызской Республики на современном этапе являются разработка комплексных целевых программ и совершенствование законодательной базы, регулирующей отношения в области обеспечения информационной безопасности страны; совершенствование системы реализации законов, которые регламентируют деятельность в информационном поле; создание необходимых условий для того чтобы права граждан, а также общественных объединений деятельность в информационной сфере были реализованы (стоит отметить что речь идет о деятельности, которая разрешена законом); разработка долгосрочной программы, направленной на развитие и поддержку отечественного производства в важнейших областях информатизации, телекоммуникаций и связи, средствах защиты информации, определяющих информационную безопасность страны. Необходимо проведение фундаментальных научных и прикладных исследований в области обеспечения информационной безопасности в государстве.

Считаем необходимым осуществление международного сотрудничества в сфере обеспечения информационной безопасности государства, и представлять интересы Кыргызской Республики в соответствующих международных организациях.

В заключение позвольте подчеркнуть, что в исследовании рассмотрен лишь завершенный авторский взгляд на данную проблему, являющийся определенным рубежом, который предполагает дальнейшее осмысление и исследование политических механизмов обеспечения информационной безопасности государства.

Основные публикации по теме диссертационного исследования:

1. Мусуралиева, М.М. Методика информационной безопасности и ее место в системе обеспечения национальной безопасности Кыргызской Республики [Текст]/ М.М. Мусуралиева // Гуманитарные проблемы современности. − Бишкек, 2014.– Вып. 20. – С.569-576.

2. Мусуралиева, М.М. Международные аспекты информационной безопасности [Текст]/ М.М. Мусуралиева // Гуманитарные проблемы современности. − Бишкек, 2014. – Вып. 20. − С.564-569.

3. Мусуралиева, М.М. Мировое информационное пространство как фактор интеграции [Текст]/ М.М. Мусуралиева // Наука и новые технологии. − 2015. – № 2. − С.272-274.

4. Мусуралиева, М.М. К вопросу о содержании информационной безопасности [Текст]/ М.М. Мусуралиева, Р.Исмаилова // Наука и новые технологии. − 2015.– № 2. − С.261-263.

5. Мусуралиева, М.М. Информационная война: цели, виды, методы [Текст]/ М.М. Мусуралиева // Наука и новые технологии. − 2016. – № 6. − С.179-181.

6.Мусуралиева, М.М. Информационные ресурсы – как инструмент обеспечения политической безопасности Кыргызской Республики [Текст]/ М.М. Мусуралиева // Известия НАН Республики Казахстан. – Алматы, 2015. − № 2. – С. 227-231.

7. Мусуралиева, М.М. Информационная безопасность: системный анализ [Текст]/ М.М. Мусуралиева // Путь науки. – Волгоград, 2016. – С. 86-89.

8. Мусуралиева М.М. Доверие граждан электронному правительству в КР [Текст]/ М.М.Мусуралиева// Информатизация образования и науки. – Москва, - 2015.- №4.- С.157-166.

9. Мусуралиева М.М. Обеспечение информационной безопасности страны-главное условие сохранения государства [Текст]/ М.М. Мусуралиева// Вестник КГУ им. И.Арабаева. – Бишкек, 2015. - №3. - С.307-312.

10. Мусуралиева М.М. Информационная безопасность и ее место в системе обеспечения национальной безопасности КР [Текст] / М.М. Мусуралиева // Наука и новые технологии. − 2016. – № 6. − С.200-203.

11. Мусуралиева М.М. Тенденции развития информационного пространства Текст]/ М.М.Мусуралиева//Известия вузов Кыргызстана. – 2016.- №6.-С.158-160.

12. Мусуралиева М.М. Понятие и сущность информационной войны Текст]/ М.М.Мусуралиева//Известия вузов Кыргызстана. – 2015.- №1.-С.227-229.

РЕЗЮМЕ

Мүсүралиева Мээрим Мамбеткалыковнанын “Кыргыз Республикасында маалыматтык коопсуздукту камсыз кылуунун саясий механизмдери “ темасына жазылган 23.00.02 –саясий институттар, процесстер жана технологиялар адистиги боюнча саясий илимдердин кандидатынын окумуштуулук даражасына талапкерликке диссертациясына

Түйүндүү сөздөр: коопсуздук, маалымат, маалыматтык коопсуздук, улуттук коопсуздук, саясий сфера, маалыматтык сфера, саясий механизмдер.

Изилдөөнүн объектиси – маалыматтык коопсуздук мамлекеттин улуттук коопсуздугунун бир бүтүн системасынын курамдык бөлүгү катары.

Изилдөөнүн предмети – Кыргыз Республикасынын саясий-маалыматтык мейкиндигинде маалыматтык коопсуздукту камсыз кылуунун механизмдери.

Диссертациялык иштин максаты –Кыргыз Республикасынын маалыматтык коопсуздугун камсыз кылуунун саясий механизмдеринин формаларын жана методдорун табуу.

Изилдөөнүн методдору –диссертациянын методологиялык негизи болуп социалдык саясий жана башка гуманитардык маселелерди изилдөөнүн жалпы илимий жана ошондой эле атайын методдорунун системасы эсептелет. Саясат таануунун алкактарында маалыматтык коопсуздуктун проблемаларын талдоонун маанилүү методологиялык аспекттери болуп, маалыматтык коопсуздуктун категориясын структуралаштыруу жана маалыматтык саясаттын концептуалдык негиздерин иштеп чыгуу болуп саналат. Изилдөөнүн атайын методдору болуп системдик, институционалдык, салыштырма жана структуралык –функционалдык методдору эсептелет.

Алынган натыйжалар маалыматтык коопсуздукту камсыз кылуунун саясий механизмдеринин проблемаларын мындан ары изилдөө үчүн, маалыматтык коопсуздук чөйрөсүндө иштерди координациялоо боюнча мамлекеттик органдардын практикалык ишинде, маалыматтык коопсуздуктун мамлекеттик Концепциясын иштеп чыгууда, ошондой эле жогорку окуу жайларынын окуу процессинде, саясат таануу, журналистика жана мамлекеттик башкаруу курстарында пайдаланылышы мүмкүн.

Изилдөөнүн илимий жаңылыгы эң алды менен Кыргыз Республикасында коомдун демократиялануу шарттарында маалыматтык коопсуздукту камсыз кылуунун саясий механизмдеринин проблемасын кароого комплекстүү мамиле жасоо менен шартталган, глобалдашуунун шарттарында маалыматтык сферадагы азыркы замандын чакырыктары жана коркунучтары конкреттештирилген, Кыргызстандын маалыматтык сферасындагы коопсуздук саясатына таасир берүүчү тышкы жана ички факторлор аныкталган, КМШ

өлкөлөрүнүн жана Кыргыз Республикасынын маалымат коопсуздугуна саясий-укуктук мазмундагы салыштырмалуу анализин жүргүзүлдү.

РЕЗЮМЕ

диссертации Мусуралиевой Мээрим Мамбеткалыковны на тему: «Политические механизмы обеспечения информационной безопасности в Кыргызской Республике» на соискание ученой степени кандидата политических наук по специальности 23.00.02 – политические институты, процессы и технологии

Ключевые слова: безопасность, информация, информационная безопасность, национальная безопасность, политическая сфера, информационная сфера, политические механизмы.

Объект исследования – информационная безопасность как составная часть системы национальной безопасности государства.

Предмет исследования – механизмы обеспечения информационной безопасности в политико-информационном пространстве Кыргызской Республики.

Цель диссертационной работы – выявление форм и методов политических механизмов обеспечения информационной безопасности Кыргызской Республики.

Методы исследования – методологической основой диссертации является система, как общенаучных, так и специальных методов исследования социально-политических и иных гуманитарных проблем. Важными методологическими аспектами анализа проблем информационной безопасности в рамках политологии являются, структурирование категории информационной безопасности, и разработка концептуальных основ информационной политики. исследования Специальными методами являются системный, институциональный, сравнительный и структурно-функциональный подходы.

Полученные результаты могут быть использованы для дальнейшего изучения проблем политических механизмов обеспечения информационной безопасности, в практической деятельности государственных органов по координации работ в сфере информационной безопасности, при разработке государственной Концепции информационной безопасности, а также в учебном процессе высших учебных заведений, на курсах по политологии, журналистике и государственному управлению.

Научная новизна исследования, прежде всего, обусловлена комплексным подходом к рассмотрению проблемы политических механизмов обеспечения информационной безопасности в Кыргызской Республике в условиях демократизации общества, конкретизированы современные вызовы и угрозы в информационной сфере в условиях глобализации, определены внешние и внутренние факторы, влияющие на политику безопасности в информационной сфере Кыргызстана, сделан сравнительный анализ политико-правового содержания информационной безопасности стран СНГ и КР.

SUMMARY

Of Meerim Mambetkalykovna Musuralieva's thesis on the theme: "Political Mechanisms to Ensure Information Security in the Kyrgyz Republic" for assignment of Philosophy Doctor degree in Political Sciences in the major "23.00.02 – Political Institutions, Processes and Technologies"

Keywords: security, information, information security, national security, political sphere, information sphere, political mechanisms.

Object of the research is information security as a constituent part of the state integral system of national security.

Subject of the research includes the mechanisms to ensure information security in the political and information space of the Kyrgyz Republic.

Goal of the these is to identify the forms and methods of political mechanisms to ensure information security of the Kyrgyz Republic.

Methodology of the research –methodological basis of the thesis is the system of both general scientific and special methods of social and political and other human issues.Majormethodologicalaspectsoftheinformationsecurityissuesanalysiswithinthep oliticalscienceincludestructuring of the information security category and development of conceptual basis of the information policy. Special methods are systemic, institutional, comparative and structural-functional approaches.

Theresultsobtainedcanbeappliedforfurtherstudyingofthepoliticalmechanismstoe nsureinformationsecurity,
inpracticalactivityofthestateauthoritiestocoordinatetheworksintheinformationsecuritys phere, in development of the state Information Security Conception, as well as in the educational process of higher education institutions, in courses of Political Science, Journalism and Public Administration.

Scientific novelty of their search is, first fall, determined by the complex approach to consideration of the issue of political mechanisms to ensure information security in the Kyrgyz Republic in conditions of the society democratization. Modern challenges and threats in the information sphere caused by globalization are also detected, foreign and domestic factors of influence on the security policy in the information sphere of Kyrgyzstan are identified, comparative analysis of the political and legal content of the information security of the CIS countries and the Kyrgyz Republic has been made.