Министерство образования и науки Кыргызской Республики
Кыргызский государственный университет им. И.Арабаева

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

Мусуралиева Мээрим Мамбеткалыковна

Политические механизмы обеспечения информационной безопасности в Кыргызской Республике

23.00.02 - политические институты, процессы и технологии

Диссертация на соискание ученой степени кандидата политических наук

Научный руководитель:
кандидат политических наук,
доцент Ч.Дуйшеналиев

Бишкек – 2018

СОДЕРЖАНИЕ

ВВЕДЕНИЕ

Актуальность темы исследования. Распад Советского Союза повлиял на многие аспекты политической жизни бывших 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 сообщество 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 жизнедеятельности 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.

Степень научной разработанности темы. Использование источников и литературы в ходе работы над диссертацией показало, что проблема безопасности издавна являлась актуальнейшей темой, как для государства, так и для любого члена общества. Так, Ш.Монтескье, Н.Макиавелли [69], Т.Гоббс, С.Хантингтон, Ф.Ратцель, Г.Киссинджер, Ф.Фукуяма и др. в своих трудах рассматривали противоречия и конфликты в обществе, как составные части политики безопасности.

Термин «безопасность» возник наряду с такими понятиями, как «демократия» или «права человека». Его корни относятся к периоду выхода в свет английского Билля, законопроекта о правах человека (1689) [131], американской Декларации независимости (1776) . Исследователи Западной

Европы посвятили свои труды раскрытию основных тенденций развития проблематики безопасности.

Современные исследования проблем безопасности отражены в работах российских исследователей К.С.Гаджиева [37], Н.А.Нартова [78], А.Г.Дугина [47], О.А.Судоргина [108], Шерстюка В.П. [190] и др. Как показало изучение данного вопроса, они придают большое значение проблеме безопасности независимо от идеологических пристрастий и научных направлений.

К российским исследованиям и разработкам, изучающим политологические аспекты обеспечения информационной безопасности, относятся работы Стрельцова А.А. [106], Цыгичко В.Н. [122], Черешкина Д.С. [123], Смолян Г.П. [152-153], Панарина И.Н. [85-86], Почепцова Г.Г. [90], Прохожева А.А. [94-97], Расторгуева С.П. [101] 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.Орунбекова [83], Ж.С. Сааданбекова [102], Н.А.Сейдакматова [151], Р.Т.Улукова [116-117], А.Б.Элебаевой [158].

Автор отмечает, что в современной отечественной политологической литературе проблема информационной безопасности, как части национальной безопасности практически не исследовалась. Несмотря на фрагментарные исследования, отдельные аспекты информационной безопасности, ее генезис, эволюция и современное состояние в достаточной степени еще не сформированы. В процессе исследования вопросов информационной безопасности пришлось обратиться к источникам, относящимся к законодательным и нормативно-правовым актам.

Особый интерес представляют решения и постановления межведомственных органов по улучшению работы информационной службы, которые позволяют осмыслить в более широком формате суть понимания информационной безопасности в обществе, происходящие изменения в понимании данной концепции и роль государственной политики в их осуществлении. При рассмотрении этой группы источников поднимаются вопросы эволюции государственной внутренней политики, которые привели к осознанию важности обеспечение информационной безопасности, раскрываются всевозможные аспекты социальной деятельности государства во времена переходного периода.

Огромное значение при написании данной работы имели юридические, политико-правовые сборники и журналы, а также содержащиеся в них документы и анализ по конституционному праву, так как обеспечение информационной безопасности является обоюдно-острым мечом, другой стороной которого является конституционные права граждан страны; также были рассмотрены анализы по государственно-политическим институтам и правовому развитию страны. Были также просмотрены и проанализированы парламентские и правительственные сборники, с опубликованными в них официальными документами.

Объектом диссертационного исследования является информационная безопасность как составная часть системы национальной безопасности государства.

Предметом исследования являются механизмы обеспечения и поддержания состояния информационной безопасности в политико-информационном пространстве Кыргызской Республики.

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 в Кыргызстане.

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 структур 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.

Теоретико-методологическая основа исследования. В качестве теоретической базы для данного исследования была взята концепция «информационного общества», а также общая теория информации. Дополнительно были использованы теоретические разработки отечественных ученых, а также работы в области информационной безопасности ученых из ближнего и дальнего зарубежья.

В качестве методологической основы диссертации была применена система как общенаучных, так и специальных методов, применяемых для исследования социально-политических и прочих гуманитарных проблем. Если рассматривать проблемы информационной безопасности в рамках политологии, то важными методологическими аспектами анализа данной задачи являются, во-первых - структурирование категории информационной безопасности, и, во-вторых - разработка концептуальных основ информационной политики государства. Также, были применены специальные методы исследования, такие как исторический, системный, институциональный и психологический методы. Эти методы применяются

для того чтобы изучить эволюции понятия «информационной безопасности» в ретроспективе.

В качестве эмпирической базы исследования были применены: в первую очередь - данные политологических и социологических исследований по теме информационной безопасности, а также разработки экспертов и специалистов в сфере государственной информационной политики и безопасности; наравне с научной литературой были изучены кыргызские и международные нормативно-правовые акты и официальные документы и официальная статистическая информация; также были рассмотрены и применены материалы кыргызских и зарубежных информационных агентств, печатных и электронных средств массовой информации и коммуникации.

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.

Теоретическая и практическая значимость работы. Теоретическая значимость исследования состоит в том, что ее выводы вносят вклад в разработку понятийного аппарата и алгоритмов анализа информационной безопасности Кыргызской Республики. Прикладное значение диссертации проявляется в том, что осмысление проблем политического обеспечения информационной безопасности в Кыргызской Республике позволит органам государственной власти усовершенствовать систему мер противодействия угрозам безопасности в стране.

Материалы диссертационного исследования могут быть использованы при дальнейшем изучении проблем развития информационного общества; в практической деятельности государственных органов по координации работы по обеспечению информационной безопасности; при разработке государственной Концепции обеспечения информационной безопасности; совершенствовании отечественного законодательства и развития договорной практики в области реализации международных механизмов обеспечения информационной безопасности, а также в учебном процессе высших учебных заведений.

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

Апробация работы состоялась при обсуждении на заседании кафедры философии и гуманитарных дисциплин Института гуманитарных знаний Кыргызского государственного университета им. И.Арабаева, на расширенном заседании Отдела политологии и проблем государственного управления Института философии и политико-правовых исследований Национальной Академии наук Кыргызской Республики, а также на заседании кафедры политологии Кыргызского национального университета им. Ж.Баласагына. По итогам обсуждений она была рекомендована к публичной защите. Ряд положений исследования отражен в докладах и выступлениях соискателя на различных конференциях, круглых столах, семинарах: 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.

Основные результаты диссертации изложены в 12 научных статьях, из них 3 статьи опубликованы за рубежом.

Структура диссертационного исследования. Диссертация состоит из введения, трех глав, включающих в себя шесть параграфов, заключения, а также списка литературы. Общий объем работы составляет 170 страниц.

Глава 1. ТЕОРЕТИКО-МЕТОДОЛОГИЧЕСКИЕ ОСНОВЫ ИССЛЕДОВАНИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

1.1. Теоретические аспекты исследования информационной безопасности

Теоретические аспекты исследования – это уточнения теоретических положений сущностных характеристик того или иного явления. В данном разделе рассмотрены основные понятия, тесно взаимосвязанные с термином “информационная безопасность”. Во-первых, будет рассмотрен понятийный аппарат самого термина “информация” и связанных с данным термином понятий “информационная сфера” и “информационное общество”. Так как понятие информационного общества связанно с понятием глобализации, было рассмотрено также понятие глобализации. Далее будет определен термин “безопасность”, а также связанные с данным понятием “государственная безопасность”, “обороноспособность”, понятия “угроза” и "опасность", “внутренняя опасность” и “внешняя опасность” и др. И наконец, даны определения таким явлениям как “кибервойна”, “информационная война” и “сетевая война”.

Информационная безопасность, наряду с экономической, социальной, оборонной, экологической, демографической и иными видами безопасности играет ключевую роль в обеспечении национальных интересов государства. Анализ существующих определений термина «информационная безопасность» показывает, что содержание этого термина в основном раскрывается сквозь призму обеспечения защиты, так называемой информационной сферы (среды) общества. Общеизвестно, что в жизнь любого общества основывается на четырех основных сферах, которые определяются как сфера материального производства, сфера политики, сфера социальной жизни и наконец сфера духовной жизни. Каждая из этих сфер состоит из совокупности общественных отношений, которые как

правило объединяются по определенному признаку. Например, в работе О.В. Бойченко Н.И. Журавленко [193] общественные отношения, объединенные под материальной сферой, были определены как отношения, которые охватывают всю деятельность, связанную с производством материальных благ общества, их результаты и производственную инфраструктуру. Совокупность общественных отношений, которые исторически сложились в связи с борьбой за власть и за возможность управления делами государства, при этом определяя направление общественного развития, контролируя финансовые и другие ресурсы государства, объедены в политическую сферу. Сферу духовной жизни авторы определили, как ту часть жизни общества, охватывающую интеллектуальную деятельность людей, и из результаты – достижения науки и искусства, культурные ценности [193]. Последняя - социальная сфера, была определена как совокупность общественных отношений, в котором реализуется социальная функция общества.

В отличие от вышеуказанных сфер, информационная сфера, выделение которой произошло недавно, формируется совокупностью информации и информационной инфраструктуры общества. В данную совокупность также попадают общественные отношения, объектом которых являются любого рода информация и / или информационная инфраструктура.

Сегодня быстрый рост информационно-коммуникационных технологий и его внедрение в общественную жизнь людей и связанная с этим глобализация процессов общественного развития значительно увеличили и все еще увеличивают зависимость общества от процессов производства, распространения и использования информации, при этом превратив ее (информацию - прим. диссертанта) в объект разнообразных общественных отношений. Информационная сфера тесно переплетена со всеми остальными сферами общественной жизни. Так, создание и внедрение информационных и коммуникационных технологий,

программных продуктов, баз данных и знаний лежит в сфере материального производства. Ощутимые изменения привносятся и в политическую сферу, меняя способы ведения политической борьбы. Государственная власть также пользуется информационной сферой для установления необходимого взаимодействия и диалога между властью и обществом. Влияние информационных технологий в сфере духовной жизни также четко прослеживается: увеличился спрос на наукоемкие технологии, повысилась производительность и изменилось содержание интеллектуального труда, а его результаты доступны более широкому кругу людей так как возросли возможности по распространению научных, политических и религиозных взглядов. Таким образом, изменились методы пропаганды. Самое большое влияние развития ИКТ можно наблюдать в социальной сфере: способы реализации социальных функций, таких как медицинская диагностика, статистический учет и так далее, все больше и больше стали проводиться с помощью информационных технологий. Сократилось время, требующееся для обратной связи. Однако вместе с этим возросла зависимость благосостояния и безопасности человека от правильности и точности информации, собранной и хранящейся в общественных и государственных информационных системах. При этом возросла ответственность государственных органов, так как от их способности обеспечить соблюдение необходимого режима использования информации зависит осведомленность и информационная безопасность общества.

Прежде чем проанализировать все обозначенные вопросы, обратиться к самой сути информационной безопасности современного государства, необходимо определить исходные понятия нашего исследования.

В трудах как отечественных, так и зарубежных философов, социологов, экономистов, правоведов, политологов и иных исследователей единодушно отмечается, что постиндустриальное общество строится на всеобщем знании и синергетической информации, циркулирующей в виде кодов в

открытых системах и как бы имеет свою информационную природу. Результатом информационной революции конца XX века является становление общественного уклада, базирующегося на комплексном, многостороннем знании и неразрывно связанной с ним информацией [19, с.100].

Впервые же понятие «информационное общество» появилось около 50 лет назад, когда в 1966 году группа японских специалистов по научным, техническим и экономическим исследованиям представила доклад, в котором предлагалось определить информационное общество как общество, в котором имеется в изобилии высокая по качеству информация, а также есть все необходимые средства ее распределения. Спустя несколько лет, в 1983 году, в труде японского ученого Y. Masuda (И. Масуда) «Информационное общество как постиндустриальное общество» [161, с.54], были предложены следующие концептуальные положения информационного общества:

- основой нового общества будет являться компьютерная технология, с ее фундаментальной функцией замещать либо усиливать умственный труд человека;
- информационная революция будет быстро превращаться в новую производительную силу и сделает возможным массовое производство когнитивной, систематизированной информации, технологии и знания;
- потенциальным рынком станет «граница познанного», возрастет возможность решения проблем и развития сотрудничества;
- ведущей отраслью экономики станет интеллектуальное производство, продукция которого будет аккумулироваться, а аккумулированная информация станет распространяться через синергетическое производство и долевое использование;

- в новом информационном обществе основным субъектом социальной активности станет «свободное сообщество», а политической системой будет являться «демократия участия»;

- основной целью в новом обществе будет реализация «ценности времени».

По мнению современных исследователей в работе японского ученого предложена новая, целостная и привлекательная своей гуманностью утопия XXI века, названная И. Масудой «Компьютопией», основными признаками которой являются:

1. Преследование и реализация ценностей времени.
2. Свобода решения и равенство возможностей
3. Расцвет различных свободных сообществ.
4. Синергетическая взаимосвязь в обществе.
5. Функциональные объединения, свободные от сверхуправляющей власти [74, с.93].

В целом, идеи формирования информационного общества упоминались в теории постиндустриализма. Согласно данной теории, научно-технический прогресс в конечном итоге воздействует на социум. Именно эта идея привела к появлению большого количества концепций, включая концепции информационного общества. В качестве примера можно рассмотреть работы американского социолога и футуролога Э. Тоффлера, а именно - «Шок будущего» (1970 г.) [163], и более позднюю работу «Третья волна» (1980 г.) [113, с.123], [162, с.300] и другие. В своих работах Тоффлер выделяет три основных стадии (волны) развития человечества, а именно - аграрную, индустриальную и постиндустриальную. Основная метафора, используемая автором - это столкновение волн, что, по мнению автора, приводит к переменам. Идея рассмотрения информации как волны позволяет организовать большое количество данных, созданных и используемых человечеством, но и видеть

то, что находится под «бушующей поверхностью перемен». Данная метафора была также использована автором чтобы объяснить возникновение всевозможных глобальных конфликтов.

После первой и второй волн, которые автор назвал «сельскохозяйственной цивилизацией» и «индустриальной цивилизацией», соответственно, на мир начала «накатываться новая волна» (то есть третья, постиндустриальная). Она основывается на научно-технологических достижениях в области информатики, электроники, молекулярной биологии. По мнению автора эти достижения создают условия для устранения главного противоречия второй волны – противоречия между производством и потреблением.

Тоффлер предполагал, что развитие, в частности, компьютерных технологий, поможет укрепить семейные отношения за счет того, что можно будет иметь доступ к так называемым «электронным коттеджам» в любом месте, в том числе и дома, что, в свою очередь, позволило бы выполнять все работу дома. Это позволило бы сэкономить время и сократить транспортные расходы, а также сократить затраты на обеспечение централизованных рабочих мест. Это особенно актуально, так как на нынешнем этапе развития человечества все большую ценность обретает интеллектуальный труд. При нынешних этапах урбанизации ИКТ, возможно, популяризировало бы жизнь в маленьких городах и сельской местности, поскольку она позволяет работать без привязки ко времени и месту работы.

То же самое касается и средств массовой информации. Тоффлер утверждает, что наступление эпохи не массовых средств информации, приведет к появлению новой техносферы и новой инфосферы, что в свою очередь будет иметь далеко идущие последствия во всех сферах жизни общества, включая сознание людей. Предрекая важную роль, которую ИКТ начинает играть в жизни людей, и учитывая его поступательное развитие,

Тоффлер естественно задается социально-философскими вопросами об самосознании машин: «Не окажется ли, что интеллектуальные машины, особенно объединенные в коммуникационные сети, выйдут за пределы возможностей нашего понимания и станут недоступны для контроля над ними?» [162,с.245].

В добавок к вышесказанному, Тоффлер изучал трансформацию власти при компьютеризации общества, а также перспективы развития демократических принципов. Он предполагал, что при новом обществе принципы демократии не только сохранятся, но и получат дальнейшее развитие.

Д. Белл также предоставил свою концепцию информационного общества. Его концепция считается очень детализированной, так как в нее почти в полном объеме включается теория постиндустриального общества, которая была разработана им в конце 60-х - начале 70-х годов. Белл тоже отмечал, что интеллектуальная работа и информационная индустрия со временем будет цениться все больше и больше, что приведет к уменьшению роли сельского хозяйства и промышленности. При этом ведущая роль будет у компьютерных технологий как основы информационного общества. Он утверждал, что «в наступающем столетии решающее значение для экономической и социальной жизни, для способов производства знания, а также для характера трудовой деятельности человека приобретает становление нового уклада, основывающегося на телекоммуникациях. Революция в организации и обработке информации и знаний, в которой центральную роль играет компьютер, развертывается одновременно со становлением постиндустриального общества». Как и Тоффлер, Белл подчеркивал определяющее значение кодифицированного научного знания, которое послужит базой для реализации технологических нововведений, что, в свою очередь, приведет к превращению новой «интеллектуальной

технологии» в центральный инструмент для проведения системного анализа и в теории принятия решений.

Таким образом, понятие информационного общества неразрывно связанно с развитием ИКТ. Другим аспектом, к которому приводит создание информационного общества – это глобализация. Как отмечалось, условиями для глобализации стало вступление человечества в новую техническую революцию и развитие компьютерных технологий, так как это привело к созданию единого информационного пространства. Единое информационное пространство, в свою очередь, привело к росту ресурсной и технологической взаимозависимости мира и интернационализации всех сторон жизни мирового сообщества.

Основной характеристикой глобализации является перерастание национальных и региональных проблем в общемировые. То есть, глобализация есть «трансформация национальных экономических и хозяйственных структур в целостную и единую мировую геоэкономическую реальность»[173, с.34]. Если говорить о конкретных сферах глобализации, к ним можно отнести производственные технологии и научные достижения, нравственно-этические ценности. К сожалению, глобализация имеет не только позитивные стороны. Новые угрозы, такие как угроза международной безопасности и стабильности, а именно - международный терроризм, транснациональная преступность, глобальное распространение оружия массового уничтожения и другие виды угроз также являются негативными сферами глобализации.

Таким образом, глобализация проникает в буквальном смысле слова во все сферы жизни, и, к сожалению, несет в себе определенный уровень рисков и опасностей. Поэтому на уровне государственной политики понятие «безопасность» становится одним из составляющих компонент. При рассмотрении безопасность с точки зрения государства, для любого государства она имеет как международный, так и национальный аспект,

которые представляют собой неделимую систему, содержащую проблемы, связанные с разнообразными сферами жизни государства.

Однако следует отметить что понятие безопасности появилось задолго до глобализации. Так, в политологическом наследии почти всех государств Востока и Запада найдется немало фактов, свидетельствующих о внимании, которое уделялось еще в глубокой древности проблемам выживания и безопасности как отдельного человека, так и нации, народностей, городов-полисов и государств в целом. Хотя термины, которые использовались для определения такого рода представлений, были самыми разнообразными, суть их сводилась к обеспечению безопасности. В частности, применительно к государству и обществу использовались понятия «обороноспособность», «военная безопасность», «государственная безопасность» и др.

Исследуя исторические предпосылки возникновения представлений о безопасности государства, можно найти немало идей и мнений философов, политиков, военных стратегов древнего мира, рассматривавших те или иные стороны безопасности как человека, так и общества, и государства в целом.

Например, в древнекитайском «Трактате о военном искусстве» Сунь-Цзы, были рассмотрены вопросы безопасности и исследованы вопросы военной неуязвимости государства [110, с.350]. Древние философы поясняли безопасность, как выбор безопасного пути для каждого конкретного человека, однако при этом учитывали, что людям свойственно стремление к истине, власти, достатку, добру, справедливости. Исходя из этого они определяли основные сферы деятельности человека: научную, политическую, экономическую, этическую и моральную, эстетическую.

Мыслители Древней Греции Платон и Аристотель также не оставляли без внимания проблему безопасности городов-полисов. Так, Платон определил совершенное государство как устойчивое, справедливое, а значит и безопасное. А само понятие безопасности философ определил как

предотвращение вреда и соотносится с такими понятиями как «помощь», «спасать-оберегать кого-либо от вреда» [88, с.123]. Аристотель видел модель совершенного государства в высокой нравственности, соблюдении всеми общих ценностей. Древнегреческий мыслитель считал, что общество и государство становится неуязвимыми, совершенными и безопасными, когда качества человека, гражданина, интегрируясь в обществе в некую целостную систему, объединяются общими ценностями [23, с.567].

В XVII - XVIII веках понятие «безопасность» стало использоваться уже в более широком значении. В частности, в трудах известного ученого Зонненфельс безопасность определена как состояние, при котором никому нечего опасаться. Один из основателей политической науки Н. Макиавелли связывал безопасность государства непосредственно с правителем, и предложил разделить государственную безопасность на внутреннюю и внешнюю: «...Государя подстерегают две опасности: одна изнутри или со стороны подданных, другая извне - от сильных соседей. С внешней опасностью можно справиться при помощи хорошего войска и хороших союзников. А если опасность извне будет устранена, то и внутри сохранится мир при условии, что его не нарушат тайные заговоры... Главное средство против них - не навлекать на себя ненависти и презрения подданных и быть угодным народу... Ведь заговорщик всегда рассчитывает на то, что убийством государя угодит народу; если он не знает, что возмутит народ, у него не хватит духа пойти на такое дело, ибо трудностям, с которыми сопряжен всякий заговор, нет числа...» [69, с.50]. Другой деятель того времени, Б. Спиноза, наоборот, видел обеспечение безопасности напрямую в людях, благодаря которым функционировали органы управления: «… да для безопасности государства и неважно, какими мотивами руководствуются люди, надлежащим образом управляя делами, лишь бы эти последние управлялись надлежащим образом. Ибо свобода или твердость души есть частная добродетель, добродетель же государства –

безопасность» [154, с.350]. Как видно из данных высказываний, именно политологические идеи выявляют сценарии будущего развития государства, предопределяя его пути опасного или безопасного развития. При исследовании стратегии обеспечения безопасности государства следует обратить внимание на «оборонительную» направленность, заложенную в ее основе, например, современное понимание безопасности как некоего состояния защищенности. Стратегия обеспечения безопасности может формироваться на различных представлениях, ценностях, целях и интересах. В этом смысле, большое значение ценностей состоит в том, что они дают ориентиры, вехи движения вперед для общества в условиях неопределенности, кризисов, перемен.

Таким образом, понятийный аппарат термина «безопасность» изучается в научной литературе начиная с древних цивилизаций, что привело к существованию большого количества формулировок. Это, в свою очередь, в значительной степени оказывает влияние на разработку и осуществление мер по обеспечению безопасности в рамках государства. Несмотря на такое количество определений, мало внимания уделялось именно методологическим проблемам безопасности при рассмотрении его как социального явления. Так, в толковом словаре живого великорусского языка В. И. Даля безопасность определена как «отсутствие опасности, сохранность, надежность» [41, с.80], тогда как Ожегов С. И. описывает безопасность как «состояние, при котором не угрожает опасность, есть защита от опасности» [82, с.93]. Во времена холодной войны, в недалеком прошлом, в Кыргызской ССР, как и во всем Союзе, под безопасностью понимали лишь защиту страны от нападения внешних врагов, покушения на государственный и общественный строй. Так, в Большой советской энциклопедии описана «безопасность международная», где она определена как состояние экономических, политических и других отношений между государствами, утверждающее мирное сосуществование государств на

началах равноправия, национальную независимость и самостоятельность народов, а также свободное развитие на демократической основе [30, с.78]. В энциклопедических словарях того времени, таких, как Советская военная энциклопедия, Военный энциклопедический словарь и др., практически не встречается понятие "безопасность", есть только прикладные виды безопасности, такие как пожарная безопасность, безопасность полетов, безопасность техники, безопасность плавания и т.д. Для определения таких понятий как "безопасность", "военная безопасность" использовались такие понятия как "оборона" и "защита государства". Даже в данное время в соседней Российской Федерации для руководящего состава Вооруженных Сил России в кратком словаре специальных терминов безопасность определена как "состояние, при котором обеспечивается защита жизненно важных интересов государства и гражданского общества в экономической, политической, военной, экологической, гуманитарной и других областях" [58, с.58]. Прокофьев В.Ф. определил безопасность как систему процессов взаимодействия интересов личности, общества, государства, а также угроз этим интересам, как внутренних, так и внешних [93, с.100].

В западных странах, однако, термины имеют немного другой формат. Например, если сравнить понятия "опасность" - "безопасность" в английском языке, то, во-первых, эти слова имеют разные корни: "danger" – опасность, и "security" - безопасность. Более того, понятия имеют неодинаковый смысл, а именно: "security" - состояние или ощущение безопасности, то есть нечто защищающее и / или гарантирующее защищенность государства от шпионажа, хищений и других видов покушений на состояние защищенности [164, с.700]. в добавок, слово "security" используется при обозначении силовых структур, таких как служба безопасности, Совет безопасности, система коллективной безопасности и т.д.. Современное понимание проблем безопасности характеризуется многообразием подходов к оценке этого явления, недоста-

точной разработкой методологических проблем, отсутствием единой понятийной системы. Одни авторы увязывают безопасность с таким понятием как страна, другие - государство, третьи - нация, понимая под этим термином либо народ, либо государство. Поэтому в научном лексиконе, сегодня существуют такие понятия, как «безопасность страны», «национальная безопасность», «безопасность государства» и многие другие. Вместе с тем многообразие подходов к понятию «безопасность» дает возможность для их анализа и классификации, что является определенным шагом в формировании единых представлений о безопасности государства в рамках соответствующей политологической теории.

Если говорить о понимании этого термина в Кыргызской Республике, то в отечественной политологической практике этот термин применительно к современным политическим процессам в КР появился в начале 90-х годов прошлого столетия, и рассматривались, прямо или косвенно, в трудах известных политологов Ж.Б.Бокошова, А.К.Керимбековой, М.Ж.Жумагулова, И.А.Абдразакова, К.С.Садиева, О.А.Молдалиева, А.А.Акунова, М.Т.Артыкбаева, А.Д.Дононбаева, К.И.Исаева, А.Б.Элебаевой и других исследователей.

Таким образом, как видно из проведенного выше анализа различных концептуальных подходов к определению термина «безопасность», с одной стороны, существует множество трактовок понятия безопасность, но, с другой стороны, это множество трактовок относятся к различным объектам безопасности и, что важно, выводятся на основе различных методологических подходов.

Автор хотел бы предложить следующее определение безопасности: безопасность – это состояние системы, связанное с ее целостностью, со структурными и функциональными особенностями. В состоянии безопасности система функционирует стабильно. Нарушение стабильности функционирования системы является нарушением ее безопасности. А

факторы, повлиявшие на изменение состояния безопасности системы, могут быть квалифицированы как угрозы, вызовы, риски и т.д.

Данное определение также подходит к определению понятия международной безопасности, которое связывают, с особым состоянием мирового сообщества, при котором достигается устойчивость межгосударственных отношений. Под устойчивостью подразумевается именно стабильность при возникновении дестабилизирующих факторов и угроз, то есть, при соответствующем балансе национальных и региональных интересов колебания не должны превышать допустимый уровень, который, в свою очередь, должна быть согласованна с экономической политикой и военной деятельностью [73, с.300].

Если говорить об национальной безопасности, то при определении данного понятия существуют различные точки зрения. Так, Прохожев А.А. видит национальную безопасность в способности государства сдерживать или устранять внутренние и внешние угрозы его суверенитету, территориальной целостности, социальному строю, экономическому развитию, другим важным элементам его жизнедеятельности, своими силами или совместно с другими дружественными странами (народами, нациями) [94, с.78]. Другое, более широкое определение национальной безопасности, гласит как способность государства сохранить и защитить свой суверенитет и территориальную целостность. Также, обеспечение национальной безопасности включает в себя защиту национальных интересов в военной сфере и в области экономики, а также безопасность в экологической сфере. В приоритетное направление национальной безопасности также входит защита таких аспектов жизнедеятельности как культурное и духовно-нравственное наследие, исторические традиции и нормы общественной жизни. И хотя оба определения термина национальной безопасности допустимы при рассмотрении тех или иных аспектов проблемы, в данной работе будет использовано второе, более

широкое определение национальной безопасности, как наиболее полное и приемлемое.

Законодательное оформление понятие национальной безопасности обрело в 2003 г. в законе КР «О национальной безопасности». В этом Законе безопасность определяется как «состояние защищенности важных интересов личности, общества и государства», а национальная безопасность - как «гарантированное состояние защищенности жизненно важных интересов личности, общества и государства от внутренних и внешних угроз» [5, с.3].

Другим важным понятием является проблема обеспечения национальной безопасности. Обеспечению национальной безопасности способствует мирный характер отношений государства (народа, нации) с другими государствами (народами, нациями). В тесной взаимосвязи с данным понятием находится и другое понятие - "укрепление национальной безопасности". Оно означает процесс создания условий, которые необходимы для соблюдения и надежной защиты интересов государства и нации, а также благополучного решения стоящих перед государством задач - политических, экономических, военных или социальных.

Подходя непосредственно к раскрытию темы диссертации, в системе национальной безопасности каждого государства наряду с политической устойчивостью общества, военной безопасностью и социально-экономической стабильностью, важнейшее значение имеет и информационная безопасность.

В процессе развития информационной среды, информация и информационно-коммуникационные технологии становятся характерными явлениями в жизни человека, общества и государства. В этом есть как позитивные, так и негативные стороны. Так, если рассматривать развитие ИКТ с позитивной стороны, информация и информационно-коммуникационные технологии выступают как средство накопления знаний

и опыта предыдущих поколений, сведений об окружающем мире, основываясь на которых люди могут осуществлять выбор линии поведения для удовлетворения своих потребностей, реализации интересов. Однако, с другой стороны, ИКТ можно использовать как средство управления не только человеком и его поведением, а также контролировать деятельность общественных организаций и даже органов государственной власти.

Для анализа термина информационной безопасности необходимо для начала начать с определения термина информации. Так, в современной литературе термин «информация» имеет различные интерпретации, что говорит о сложности этой категории в качестве объекта исследования. Этой проблеме посвящены исследования, например, Э. Шеннона, И.Л. Бачило, С.И. Семилетова, А.А. Фатьянова и других. Например, с точки зрения философии термин «информация» является одним из наиболее общих понятий науки, которое обозначает некоторые познания, совокупность каких-либо данных, сведений и т.п. При этом отмечается, что понятие «информация» охватывает, по меньшей мере, три объекта, а именно – должен быть источник информации, потребитель информации и передающая среда. Как указывает Р.Ф. Авдеев, философская наука различает два противоположных подхода к концепции информации – атрибутивный и функциональный [19, с.34]. Первый определяет информацию как свойство всех материальных объектов, то есть информация является атрибутом материи. Однако многие не согласны с данной концепцией. Например, А.А. Стрельцова предположил что такой подход неосновательно расширяет содержание понятия информации, так как если информация – это атрибут материи, то в отсутствие объектов живой природы встает вопрос о механизмах обмена информацией между объектами неживой природы, или между объектами живой и неживой природы и т.д. [156, с.13]. Согласно второй, функциональной концепции, наоборот, информация связана лишь с самоорганизующимися системами,

однако при таком подходе вопросы о природе информации, условиях ее возникновения и развития остаются без ответа.

С формированием в XX веке т.н. «информационной эпохи», термин «информация» претерпел значительные изменения и наполнился новым содержанием. По мнению Н.Омарова, понятие информации получило новое осмысление при ее изучении в контексте теорий информации и кибернетики, получивших развитие в XX веке. При нарастающих возможностях носителей информации возросло и количество информации, появилось понятие выбора и отрицательной энтропии. Так, основоположник кибернетики и теории искусственного интеллекта Норберт Винер, например, ставил понятие «информация» в ряд фундаментальных характеристик природы, подобно количеству вещества или энергии, связывая понятие информации с понятием выбора и уточнения неопределенной ситуации, то есть энтропии [34, с.145]. Другой исследователь, основатель математической теории информации Клод Шеннон под информацией понимал не любые сведения, а лишь те, которые снимают полностью или уменьшают существующую до их получения неопределенность - энтропию. В теории Шеннона каждому сигналу (или, в случае печатного текста - символу) соответствует вероятность его появления. Чем меньше вероятность появления того или иного сигнала, тем больше информации он несет для потребителя [124, с.300].

Как отмечалось выше, при определении термина безопасность, в определении понятия информации также существуют различные подходы. Например, в кибернетике, науке, которая занимается изучением вопросов управлении в живых, неживых и искусственных системах, понятие информации непосредственно связанна с понятием управления (Н. Винер, Б.Н. Петров) [87, с.52]. Там под информацией понимается то как мы воспринимает объекты внешнего мира посредством наших чувств. То есть информация есть наши знания, то, что может быть использовано при

принятии решений, что есть управление, сохранение, совершенствование и развитие какой либо системы. С точки зрения кибернетики в неживой природе информация не может существовать. Остается открытым вопрос о том, являются ли является ли необработанные данные и неиспользуемые знания информацией. Академик В.П. Афанасьев внедрил понятие так называемых информационных данных. Под данное понятие Афанасьев объединил разного рода сведения, сообщения, знания, которые можно хранить, перерабатывать и передавать. Однако информацией эти сведения могут быть названы тогда и только тогда, когда приобретут содержание и форму, пригодную для управления и смогут быть использованы в управлении.

По мере развития ИКТ, понятийный аппарат термина «информация» также усугублялся, и в настоящее время находит широкое применение не только в точных науках при анализе процессов в самоуправляющихся системах, но и иных, гуманитарных областях знаний, таких как политология, право, лингвистика, социология, экономика, психология и т.д. Так, например, роль и значение информации в политической жизни современного общества непрерывно повышаются, информация становится необходимостью при управленческой деятельности органов государственной власти. А так как речь идет о государственном управлении, то обеспечение безопасного сбора, и самое главное – обработки и передачи информации, что и составляет информационную безопасность, становится приоритетной областью, так как информационная среда является системообразующим фактором развития государства. Таким образом, информационную безопасность можно охарактеризовать как способность государства, общества, социальной группы, личности обеспечить сбор и доступ достаточных и защищенных информационных ресурсов; способность государства противостоять информационным опасностям и угрозам, а также негативным информационным воздействиям на индивиду-

альное и общественное сознание и психику людей со стороны внутренних и внешних оппонентов, а также защиту компьютерных сетей и других технических источников информации, осуществлять информационно-психологическое противоборство.

Конкретизирую сказанное выше, информационную безопасность общества и государства можно охарактеризовать как состояние отсутствия информационных опасностей и угроз, либо, если угрозы существуют, обеспечение состояния устойчивости основных сфер жизнедеятельности (политики, экономики, науки, техносферы, сферы государственного управления, общественного сознания, военного дела и т.д.) по отношению к опасным информационным воздействиям (как внедрению, так и извлечению информации) [107, с. 123].

Проект Концепции информационной безопасности КР определяет информационную безопасность, как состояние защищенности ее национальных интересов в информационной сфере, определяющихся совокупностью сбалансированных интересов личности, общества и государства.

Традиционно так сложилось, что информационная безопасность рассматривается, в первую очередь, с политической точки зрения, далее идет рассмотрение с точки зрения социологии и юридической науки. Однако это не приводит к конфликту в определении информационной безопасности, так как каждая из них разрабатывает различные аспекты информационной безопасности. Если говорить о закономерностях и механизмах обеспечения информационной безопасности, то этим занимается новая междисциплинарная наука - "секьюритология" [126, с.54].

Так как в данной работе рассматриваются именно политико-правовое содержание информационной безопасности, с данной позиции информационная безопасность характеризуется как состояние социальных институтов, при котором обеспечивается их эффективная деятельность,

другими словами, это состояние защищенности наиболее существенных интересов не только личности и общества, но и государства в целом, как от внутренних так и от внешних угроз реального и потенциального характера. Из данного определения становится видно, что в информационной безопасности выделяются три уровня безопасности: личности, общества и государства; их место и роль в основном динамичны, то есть они определяются характером общественных отношений, политическим устройством государства и степенью внутренних и внешних угроз.

Еще одним понятием, которое используется непосредственно с понятием "информационная безопасность" - это информационные интересы государства. Так, американский социолог Уолтер Липпман, определил связь этих двух понятий в следующей формулировке: "государство находится в состоянии безопасности, когда ему не приходится приносить в жертву свои законные интересы..." [66, с.234]. Информационную безопасность также определяют через силу, так как преобладание мощи, включая техническую мощь, воспринимается как обеспечение некоторой безопасности.

Следующими понятиями, связанными с информационной безопасностью, являются опасности и угрозы. Эти два понятия тесно связанны между собой, однако они не являются тождественными категориями.

По мнению М.Д. Гацко, основным отличием угрозы от опасности определяет то, насколько велика готовность к причинению того или иного ущерба. Опасность автор понимает, как стадию зарождения и насыщения противоречий, то есть один из субъектов политики в принципе может, но все еще не готов по той или иной причине применить силу в своих интересах. Угроза же - это стадия крайнего обострения противоречий, когда один из субъектов политики уже абсолютно готов применить силу для достижения своих политических целей, то есть непосредственно предконфликтное состояние. Вторым отличием опасности от угрозы

является то что опасность носит гипотетический, ненаправленный характер, тогда как угроза всегда имеет объект, на который она направлена, то есть всегда есть субъект (источник) угрозы и объект угрозы, на который направлено ее действие. Третье отличие – это временные рамки, то есть, опасность – это ситуация когда для осуществления какого либо ущерба необходимо создание соответствующих условий (накопление возможностей и формирование намерений), под угрозой же подразумевается ситуация, когда возможность нанесения ущерба зависит только от времени, необходимого для принятия решения по реализации этой угрозы [66, с.9].

Помимо непосредственно ущерба О.А. Бельков оценил опасность как негативное воздействие на социальный организм, которые может причинить помимо ущерба еще и вред, ухудшающий его состояние, либо придающий развитию социума нежелательные динамику или параметры (характер, темпы, формы и т.д.) [130, с.92].

Виды опасностей можно классифицировать следующим образом:

- По степени вероятности
    - реальная
    - потенциальная

Тогда как виды угроз имеют более сложную иерархию, их можно классифицировать следующим образом:

- по сферам человеческой деятельности –
    - политическая угроза;
    - экономическая угроза;
    - социальная угроза;
    - правовая угроза;
    - военная угроза;
    - экологическая угроза;
    - демографическая угроза;
    - генетическая угроза;

    - научно-техническая угроза;
    - технологическая угроза;
    - идеологическая угроза;
    - психологическая угроза;
    - интеллектуальная угроза;
    - информационная угроза;
    - сырьевая угроза и др.;
- по источнику угрозы
    - внутренняя;
    - внешняя;
- по отношению к человеческой деятельности:
    - объективная;
    - субъективная;
- по вероятности реализации
    - реальные;
    - потенциальные.

Для устранения опасностей и, в особенности, угроз, обычно объекты угрозы прибегают к той или иной защите – к комплексу мер по предотвращению или нейтрализации посягательств, враждебных действий, опасностей (В.Л. Пирумов). Особо следует отметить что главное - адекватность данных мер угрозам и снижение уровня опасности [150, с.35].

Переходя непосредственно к информационной безопасности, основные виды угроз информационной безопасности можно сформулировать следующим образом:

Во-первых, это контроль над информацией и информационно-технологическими системами со стороны их разработчика. Контроль может распространяться не только на данных, хранящиеся или передающиеся посредством систем, но и непосредственно организации и структур коммерческих и государственных предприятий.

Во-вторых, новые технологии вполне могут быт использованы государством для контроля общества, что ущемляет права личности. По словам Р. Бенджамин Барбера, возможно влияние на «сердца и умы через контроль над образованием, информацией и коммуникацией и, таким образом, превращает субъектов в союзников рабства». К этой же категории относится проблема персональных данных и личной тайны, что приведет к тому что «новые технологии могут стать опасным катализатором для нового вида тирании» - мягкой, а «нет более опасной тирании, чем невидимая и мягкая» [70, с.126].

В-третьих, существует понятие «цифрового неравенства». По мнению автора, данная проблема особенно актуальны при нынешних реалиях Кыргызстана. Угроза данного типа видится в формировании «элиты, обладающей неограниченным доступом к информации и коммуникационным сетям, как на внутригосударственном, так и на международном уровнях, использующей преимущество владения базами данных и связью в своих узких групповых целях и осуществляющей селективное распределение информации. В результате резко возрастают возможности манипулирования общественным мнением, базирующиеся на разных уровнях доступа отдельных людей, социальных групп, государств и т.д. к информации».

В-четвертых, группа угроз информационной безопасности возникла из-за так называемой «информационной милитаризации» [122, с.67]. Выделяются три основных вида конфликтов: кибервойна, информационная война и сетевая война.

Кибервойна является самым маловероятным из опасностей, по крайней мере на данном отрезке времени, так как она характеризуется применением информационных технологий для создания оружия.

Другой вид конфликтов – кибервойна – на данном этапе развития технологий уже не настолько маловероятна и более актуальна. К тому же,

данная угроза возможна как в реальном мире – путем выведения технологий из строя (например, вирусными атаками), так и в виртуальном, а именно – посредством влияния на сознание людей через информационно-коммуникационные технологии. И хотя ранее считалось, что подобные риски актуальны в развитых странах, однако при нынешней зависимости людей в нашей стране от ИКТ, эти риски актуальны и в нашей стране.

Примером этому может служить так называемая «информационная война» В практике в широком смысле чаще всего используется термин «информационная борьба»; в узком смысле - «информационные военные действия».

Согласно мнению одних специалистов «информационная война - это действия, предпринятые для достижения информационного превосходства в интересах национальной стратегии и осуществляемые путем влияния на информацию и информационные системы противника, при одновременной защите собственной информации в своих информационных системах» [132, с.49].

Другие теоретики информационного противоборства предлагают свою концепцию «информационной войны», которая предусматривает [132, с.50]: во-первых – войну на физическом уровне, то есть подрыв ИКТ, электромагнитное воздействие. Во-вторых - перехват и дешифровка информационных потоков, передаваемых по каналам связи, либо при помощи электронных устройств перехвата информации, либо посредством несанкционированного доступа к информационным ресурсам – так называемая радиоэлектронная разведка. В-третьих, создание и массовое распространение дезинформации или тенденциозной информации. Данный вид информационной войны наиболее распространен, и, учитывая развитие ИКТ и интернет, одна из наиболее опасных, так как она направлена на информационные ресурсы и на системы формирования общественного сознания и мнения, базирующиеся на средствах массовой информации и

пропаганды, то есть ресурсы, влияющие на людей, принимающих решения (психологическая война).

В западных странах информационную войну называют «нефизической атакой на информацию, информационные процессы и информационную инфраструктуру», при этом «целью информационной войны является воздействие на системы знаний и представлений внешнего противника» [182, с.4]. Итак, информационная война – это процесс, в ходе которого информация является одновременно оружием, ресурсом и целью.

Автор придерживается мнения, что на данном этапе развития информационное противоборство - это форма борьбы в информационном пространстве, при котором используются как технические, так и политические, экономические, дипломатические, военные и иные методы, способы и средства, для воздействия на информационное поле противника и, естественно, для защиты собственного информационного поля в интересах достижения поставленных целей.

К тому же информационная война ведется все время, независимо от того мирное это время или военное.

Таким образом, вопросы информационной безопасности являются ключевыми для обеспечения стабильности и развития государства в «информационном обществе».

Подводя итоги, 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 воздействие, информационное оружие, 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.

1.2. Методологические основы исследования информационной безопасности

В данном подразделе первой главы будут рассмотрены методология и методы исследования информационной безопасности. Методология исследования – это способ организации исследования, то есть совокупность аналитических методов и приемов, проверки и оценки, концептуального и идейного арсенала, применяемого для решения стоящих перед данной наукой проблем [105, с.234]. Вначале определимся с методологическими основами и методами познания информационной безопасности.

Информационная безопасность – это, как отмечено выше, непрерывный процесс, направленный на обеспечение защищенности национальных интересов в информационной сфере, а также интересов граждан и общества. Исходя из такой позиции, отметим, что в зависимости от информационной сферы формируются стратегические и текущие задачи

внутренней и внешней политики государства, в том числе и по обеспечению информационной безопасности.

В процессе исследования информационной безопасности Кыргызской Республики нами был использован системный метод. Это означает что, чтобы изучить информационную безопасность страны, необходимо было понять и изучить сущность информационной безопасности со всеми его характеристиками: свойствами, признаками, структурой, содержанием. Также, для того чтобы понять сильные и слабые стороны проводимой в нашей стране политики информационной безопасности, был использован сравнительный метод. Рассмотрим данные методы более подробно.

Системный анализ рассматривает любые человеческие сообщества как постоянные образования, действующие в рамках более обширной среды. Сообщества характеризуются как единые системы, которые состоят из определенного комплекса взаимосвязанных элементов. По сути, именно эти элементы вычленяются и анализируются. В данной конкретной области исследования, суть системного подхода сводится к тому, что мир политического изучается как совокупность элементов, где в качестве среды выступает гражданское общество, и рассматривается оно в совокупности с экономико-хозяйственной системой.

Системный метод как нельзя лучше подходит для проведения исследований в политологии, так как политология по своей природе – междисциплинарная наука, которая широко использует междисциплинарные методы исследования. В данной работе, к примеру, изучается политико-правовые механизмы обеспечения информационной безопасности. Само понятие информации связанно с несколькими областями исследования. В контексте поступательного развития информационных и коммуникационных технологий, и в рамках системного анализа, в данной работе был проведен мост для изучения политического вопроса в рамках технологического развития.

Более того, изучение термина «безопасность» также связанна с различными дисциплинами, а так как речь идет о безопасности в рамках государства, были изученны также историческиий понятийных аппарат данного термина.

При исследовании информационной безопасности, пользуясь различными методами, нами были изучены и информационная политика Кыргызской Республики, которая базируется на следующих принципах:

- адекватности информационной политики целям прогрессивного развития общества Кыргызской Республики;
- соответствии информационной политики наиболее существенным интересам государства, общества и личности, национальным интересам страны в целом;
- направленности информационной политики на противодействие возникающим внешним и внутренним информационным угрозам;
- интеграции информационной политики Кыргызской Республики в международное информационное пространства;
- открытости, гласности и доступности информационной политики для понимания ее различными социальными категориями населения Кыргызской Республики;
- демократического порядка формирования информационной политики, ее подконтрольности представительным органам власти и общества в целом;
- обеспечения сохранности информационных ресурсов, их процедурной и юридической защиты как одного из главных элементов стратегических развития государства и общества;
- способности информационной политики создавать необходимые условия для развития и внедрения национальных

информационных систем и технологий, в том числе на региональном уровне.

Основными задачами системы обеспечения и поддержания состояния информационной безопасности Кыргызской Республики является:

- разработка комплексных целевых программ и совершенст вование нормативной правовой базы в области обеспечения информационной безопасности Кыргызской Республики;
- совершенствование системы реализации законов Кыргызской Республики, регламентирующих деятельность в информационной сфере;
- создание необходимых условий для реализации прав граждан и общественных объединений на разрешенную законом деятельность в информационной сфере;
- поддержание баланса между потребностью граждан, общества и государства в свободном обмене информацией и необходимым ограничением на ее распространение;
- разработка долгосрочной программы, направленной на развитие и поддержку отечественного производства в важнейших областях нформатизации, телекоммуникаций и связи, средствах защиты информации, определяющих информационную безопасность страны;
- организация фундаментальных и прикладных научных исследований в области обеспечения информационной безопасности Кыргызской Республики;
- обеспечение контроля за ввозом в страну, -организация и совершенствование единой системы подготовки кадров (госзаказ) в области информационной безопасности Кыргызской Республики;

— осуществление международного сотрудничества в сфере обеспечения и поддержания состояния информационной безопасности Кыргызской Республики, представления интересов Кыргызской Республики в соответствующих международных организациях.

Обеспечение информационной безопасности Кыргызской Республики - это функционирующая на основе межведомственного сотрудничества система мер по выявлению, предупреждению и пресечению угроз информационной безопасности, а также ликвидации их последствий.

Межведомственное сотрудничество, считаем, должно базироваться на следующих основных принципах:

— планирование и реализация всеми государственными органами и органами местного самоуправления, предприятиями, организациями и учреждениями, независимо от форм (далее - субъекты информационных отношений) мероприятий по обеспечению информационной безопасности, с соблюдением норм международного права и национального законодательства;

— реализация взаимной ответственности личности, общества и государства, регулярное информирование общественности о состоянии информационной безопасности Кыргызской Республики и о деятельности по ее обеспечению;

— последовательная реализация субъектами информационных отношений Кыргызской Республики мер по обеспечению информационной безопасности страны, направленных на нейтрализацию существующих угроз в информационной сфере.

Метод исследования информационной безопасности Кыргызской Республики состоит в следующем: угрозы информационной безопасности Кыргызской Республики представляют собой

совокупность условий и факторов, создающих потенциальную или реально существующую опасность нанесения ущерба объектам и субъектам информационной сферы страны. Такие угрозы могут иметь объективный и субъективный характер, который выражается в явлениях, процессах и действиях (или их совокупности) и исходить от внешних и внутренних источников по отношению к информационной сфере Кыргызской Республики. В сфере информационных отношений угрозы информационной безопасности обусловлены наличием противоречий, которые существуют или могут возникнуть между субъектами этих отношений. Внешними угрозами для информационной сферы Кыргызской Республики являются негативные для нее физические явления, политические, экономические, и иные мировые процессы, а также подрывные действия других государств. К таким угрозам относятся:

— разработка рядом стран концепций информационных войн, создание ими информационного оружия, а также ведение этими государствами всевозможных видов разведки в интересах достижения преимущества в информационных сфере;

— увеличение технологического отрыва ведущих мировых держав, усиливающее зависимость Кыргызской Республики от закупок зарубежной техники для обеспечения важных национальных информационных инфраструктур;

— деятельность международных экстремистских, террористических и других преступных сообществ, антиобщественных организаций и групп в информационной сфере Кыргызской Республики, их интерес к обладанию информационным оружием и его применению;

— обострение международной конкуренции за обладание стратегически важной информацией, стремление ряда стран к доминированию в информационном пространстве Кыргызской Республики и получение доступа к информации с ограниченным доступом;

— введение некоторыми государствами на своих информационных рынках всевозможных ограничений, ущемляющих интересы Кыргызской Республики;

— нарушение деятельности по ряду объективных и субъективных причин, имеющиеся потенциальные возможности доступа со стороны криминальных и иных антиобщественных структур Кыргызской Республики к информации с ограниченным доступом и противоправное ее использование.

По своей общей направленности угрозы информационной безопасности Кыргызской Республики подразделяются на следующие виды:

а) угрозы правам и свободам личности в области информационной деятельности и духовной жизни, индивидуальному, групповому и общественному сознанию, обусловленные:

— сдерживанием процессов развития информационной сферы Кыргызской Республики;

— неправомерным ограничением доступа общественности к открытым национальным информационным ресурсам, архивным материалам и другой социально-значимой информации (экологической, санитарно- эпидемиологической, правовой и др.)

— нарушением законных ограничений на производство и распространение в Кыргызской Республике информации, разжигающей расовую, национальную конфессиональную рознь,

а также разрушающей нравственные устои общества; - широкой пропагандой образцов, так называемой, массовой культуры, противоречащей исторически сложившимся менталитету и традициям народа Кыргызской Республики;

б) угрозы информационной поддержке и информационному обеспечению внутренней и внешней политики, реализуемой руководством Кыргызской Республики, обусловленные:

- -недостаточным вниманием со стороны государственных органов к вопросам своевременной разработки проектов нормативных правовых актов;
- -деятельностью в информационном пространстве Кыргызской Республики (включая сеть "Интернет") информационных агентств, средств массовой информации и иных информационных структур, искажающих информацию о внутренней и внешней политике Кыргызской Республики;
- недостаточной эффективностью деятельности национальных информационных агентств и средств массовой информации по противодействию негативному информационному воздействию на население Кыргызской Республики;

в) угрозы функционированию государственных информационных систем, накоплению, хранению, передаче, сохранности информации, а также защищенности линий электросвязи на уровне правительства и оборонных ведомств, а также защищенность линий связи пограничных служб, таможенных служб, налоговых органов и правоохранительных органов; особо нужно подчеркнуть защищенность радио и телевизионных вещательных комплексов;

- программные и технические средства; а также учитывая что в Кыргызской Республике действует государственный и официальный языки, то необходимо учесть защищенность

лингвистических средств; как известно, информационная безопасность обеспечивается не только на техническом уровне, а также и на административном, поэтому необходимо учесть правовые, организационные и иные средства, которые используются или создаются при проектировании и эксплуатации государственных информационных систем; далее, после того как административная часть работ по обеспечению информационной безопасности проделаны, необходим контроль за разработкой компьютерных программ, работой средств вычислительной техники и связи, для избежания саботажа –за эксплуатационной документацией систем, положениями, уставами, должностными инструкциями и т.д.

- помещения, предназначенные для ведения конфиденциальных совещаний и переговоров; помещения с любым техническим оборудованием, которое задействовано для обмена информацией с ограниченным доступом;
- система стандартизации, сертификации и лицензирования в информационной сфере Кыргызской Республики;
- система правового регулирования отношений между субъектами информационной сферы Кыргызской Республики.

Защищаемыми свойствами информации с ограниченным доступом являются ее целостность, доступность и конфиденциальность.

Защищаемыми свойствами открытой охраняемой информации являются ее конфеденциальность, целостность и доступность.

В увеличением уровня секретности информации, устанавливается режим защиты информации:

- в отношении информации с ограниченным доступом - уполномоченными органами в соответствии с законодательством Кыргызской Республики; в некоторых случаях режим защиты

может устанавливаться также международными договорами, вступившими в силу в установленном порядке;

— в отношении открытой охраняемой информации – правообладателем, пользователем (потребителем) данной информации; если информация является частью какого либо информационно ресурса - то режим ее защиты устанавливается собственником (владельцем) данных информационных ресурсов, систем или технологий (в соответствии с законодательством Кыргызской Республики).

Методы и основные направления обеспечения и поддержания состояния информационной безопасности Кыргызской Республики можно разделить на правовые, экономические и организационно-технические.

Правовые методы по обеспечению информационной безопасности КР включают:

— разработку нормативно-правовых актов и нормативно-методических документов, которые регламентируют отношения, взаимоотношения и действия всех субъектов в информационной сфере КР;

— разработку правовых механизмов, направленных на недопущение в КР противозаконных информационно-психологических воздействий на сознание личности и общества;

— активизацию целенаправленной деятельности компетентных правоохранительных органов КР по предупреждению и пресечению правонарушений в информационной сфере страны;

— стимулирование развития в КР производства средств информатизации и защиты информации.

Организационно - технические методы по обеспечению и поддержанию состояния информационной безопасности КР заключаются в непрерывном

совершенствовании технологии защиты информации и государственных информационных систем от потенциальных и реальных угроз.

К таким методам относятся:

Осуществление со стороны уполномоченных органов государственной власти действенного контроля за ввозом, производством и реализацией в КР телекоммуникационного оборудования и оргтехники, средств связи, программного обеспечения;

- Формирование эффективной системы сертификации и лицензирования деятельности в области съема и защиты информации;
- скоординированная деятельность органов власти и управления КР по выявлению и нейтрализации в национальных сегментах государственных информационных систем устройств и программ, представляющих опасность для нормального функционирования этих систем;
- создание эффективной системы защиты и реализация всеми субъектами информационных отношений согласованных мероприятий, направленных на недопущение несанкционированного доступа к информации государственных информационных систем и ее утечки по техническим каналам;
- осуществление в процессе эксплуатации государственных информационных систем эффективного контроля за действиями пользователей и обслуживающего персонала, в том числе за выполнением специальных требований;
- скоординированные действия по обеспечению всеми субъектами информационных отношений защиты конфиденциальной информации и информационных технологий при взаимодействии информационных систем различных классов защищенности, в

том числе взаимодействии этих систем с Интернетом и другими глобальными сетями;

— согласованное построение новых, и модернизация всеми субъектами информационных отношений принадлежащих им сегментов государственных информационных систем и их программного обеспечения;

— совместное создание и стандартизация в рамках межведомственного взаимодействия единых перспективных государственных систем «электронных денег», «электронной торговли» и «электронных платежей»;

— государственная поддержка и координация действий субъектов информационных отношений в подготовке кадров, которые могли бы проводить работы по обеспечению информационной безопасности;

— необходимо ужесточить правоприменительнуюй деятельность органов исполнительной власти КР; работы против правонарушений в информационной сфере должны быть направлены на предупреждение и пресечение, опять таки, необходимо повышать уровень грамотности и техническую базу, чтобы создать условая для выявления и привлечения к ответственности лиц, совершивших киберпреступления или преступления с использованием информации или в информационной сфере;

— необходимо сформировать и внедрить систему мониторинга состояния информационной безопасности КР по ключевым показателям или характеристикам, в наиболее важных сферах жизнедеятельности общества и государства.

При этом необходимо учесть еще и экономические методы, которые включают в себя разработку, соответствующее финансирование и

неукоснительное выполнение государственных целевых программ для обеспечения и поддержания состояния информационной безопасности КР в целом и информационной безопасности в конкретных специфических областях жизнеобеспечения государства (наука, техника, экономика, банковское дело, оборона, правоохранительная деятельность и т.д.)

В каждой из сфер информационных отношений имеются свои особенности, связанные со спецификой защищаемых объектов и степенью их уязвимости в отношении угроз информационной безопасности. В связи с этим, в целях обеспечения и поддержания состояния информационной безопасности таких объектов могут разрабатываться и реализовываться внутриведомственные специальные концепции и соответствующие программы.

Противодействие угрозам, касающимся прав и свобод человека в области информационной деятельности и духовной жизни, индивидуального, группового и общественного сознания, осуществляется преимущественно правовыми методами, а также путем решения органами власти и управления КР экономических, организационных и технических вопросов, связанных с повышением уровня компьютерного образования населения и с расширением доступа общественности к социально значимой информации.

В противодействии угрозам информационной поддержки и информационному обеспечению внешней и внутренней политики, проводимой руководством КР, а также развитию национальной индустрии технических средств, программного обеспечения информации, информатизации и связи, выходу отечественной информационной продукции и услуг на международный рынок используются в основном правовые и экономические методы.

Организационно-технические методы являются основными методами для противодействия угрозам функционирования государственных

информационных систем, накоплению, сохранности и эффективному использованию их информационных ресурсов.

Познание информационной безопасности КР дает возможность Проект концепции информационной безопасности КР (11 июля 2008 года), в котором подчеркнуто, что Концепция информационной безопасности КР представляет собой совокупность официально принятых взглядов и положений, касающихся целей, принципов и основных направлений обеспечения информационной безопасности, включая защиту интересов личности, общества и государства в информационной сфере.

Концепция должна служить основой для выработки предложений по совершенствованию законодательства в сфере обеспечения информационной безопасности Кыргызской Республики; -дальнейшего формирования и совершенствования нормативной правовой базы и разработки целевых программ обеспечения и поддержания состояния информационной безопасности Кыргызской Республики; -развития и совершенствования правового, методического, научно-технического и организационного обеспечения работ, относящихся к этой сфере.

Подытоживая данный параграф, 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, бихевиористский метод.

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 безопсности в Кыргызской Республике, то за свойство, по которому ведется сравнеие, 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 2. ПОЛИТИКО-ПРАВОВОЙ АНАЛИЗ ОБЕСПЕЧЕНИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ КЫРГЫЗСКОЙ РЕСПУБЛИКИ

2.1.Сравнительный анализ политико-правового содержания информационной безопасности Кыргызской Республики и стран СНГ

Для того чтобы обеспечить национальные интересы любой страны, в том числе Кыргызской Республики, необходимо подвести механизмы правового обеспечения. Это касается также и информационной сферы. Привилегия создания общеобязательных правил поведения — правовых норм, закреплена за государством, то есть нормативные правовые акты издаются государством. Как известно, правое регулирование должно удовлетворять, как можно большему количеству внутренних и внешних потребностей государства и первоочередное должно быть направлено на обеспечение защищенности и устойчивого развития как отдельно взятой личности, так и общества, и государства. Таким образом, правовое обеспечение должно охватывать интересы личности, общества и государства, и только тогда мы можем говорить об обеспечении национальных интересов КР в информационной сфере.

В силу того, что информационно-коммуникационные технологии (ИКТ) развиваются ударными темпами, тема информационной безопасности в последние годы становится одной из самых актуальных. При этом данная тема актуальна не только при рассмотрении вопросов защиты персональных данных пользователей, особую важность она обретает при рассмотрении вопросов политико-правового обеспечения информационной безопасности государств. Интернет, как один из основных составляющих ИКТ, развивался начиная с 1966 года как проект Агентства перспективных исследований США в области обороны (U.S. Defense Advanced Research Projects Agency -

ARPA) [202], и изначально было в основном использовано для военных целей - ARPANET была испытательным полигоном для инновационных концепций, таких как коммутация пакетов, распределенная топология и маршрутизация, а также подключение гетерогенных компьютерных систем. Расширяясь к 1994 году, было зарегистрировано почти четыре миллиона хостов [203]. С развитием Интернет росли и методы угрозы безопасности данных, хранящихся в сети, что привело, в свою очередь, к росту числа преступлений, совершенных с помощью компьютерных технологий, и таким образом, когда речь идет об обмене информацией государственного значения, растут риски для информационной безопасности государства. В промышленно развитых странах компьютеризация преступности развивалась медленно, поступательно, наравне с развитием технологий, поэтому у технических работников было время для разработки контрмер, а у государственных законодательных органов – на подготовку нормативно-правовой базы реагирования на киберпреступления. При этом, если говорить о пост-советских странах, компьютеризация была быстрой и люди и государство не были готовы к такому росту киберпреступлений [204]. Многие исследователи согласны с мнением о том, что существующая законодательная база в области обеспечения информационной безопасности не помогает покрыть весь спектр механизмов, необходимых для обеспечения безопасности в информационном пространстве. Так, например, в Кыргызской Республике, политико-правовые основы по обеспечению информационной безопасности не отрегулированы, нет актов, которые бы регламентировали отношения различных министерств и ведомств в информационной сфере [189].

Политико-правовое содержание информационной безопасности определяется Конституцией Кыргызской Республики, Концепцией национальной безопасности Кыргызской Республики; нормативную же базу формируют законы Кыргызской Республики «О защите государственных

секретов Кыргызской Республики», «О гарантиях и свободе доступа к информации», «Об информатизации», «О средствах массовой информации», «О правовой охране программ ЭВМ и баз данных», «Об электрической и почтовой связи», «Об электронной цифровой подписи», «Об основах технического регулирования в Кыргызской Республике», «О доступе к информации, находящимися в введении государственных органов и органов местного самоуправления Кыргызской Республики», также Гражданский и Уголовный кодексы Кыргызской Республики.

Главным нормативно-правовым актом в данной сфере является Закон КР «О средствах массовой информации» № 938-XII от 2 июля 1992 г., определяющий общие социальные, экономические, правовые основы организации вестей через СМИ. Так, например, постановлением Правительства Кыргызской Республики № 722 от 23 сентября 1994 г. была утверждена Концепция создания и развития информационной сети (информатизации) Кыргызской Республики. Базовым законодательным актом в данной сфере является Закон КР «Об информатизации» № 107 от 8 октября 1999 г., регулирующий главные экономические, организационные и правовые отношения, которые необходимы для продвижения развития информатизации в Кыргызской Республике. В этом же направлении действует Закон КР «О системе научно-технической информации» № 108 от 8 октября 1999 г., устанавливающий организационные, экономические и правовые базы функционирования структуры научно-технической информации в Кыргызской Республике. Постановлением Правительства Кыргызской Республики № 143 от 22 марта 2005 г. была одобрена Концепция информационной безопасности Кыргызской Республики, которая позже утратила силу. В данное время не существует подобной концепции, нет доктрины информационной безопасности государства. Для разработки нормативно правовой базы необходимо принятие ряда законов и постановлений.

Всего по теме информационной безопасности в КР было принято 19 Постановлений и Распоряжений правительства, однако, большей частью - это Распоряжения Правительства КР об одобрении проекта Соглашения между правительствами государств-членов Шанхайской Организации Сотрудничества о сотрудничестве в области обеспечения международной информационной безопасности, либо Постановления Правительства КР об утверждении Соглашения об обеспечении информационной безопасности в рамках общих таможенных процессов в государствах-членах Евразийского экономического сообщества. А в УК КР в разделе 9, главе 28 , только 1 статья – 290 [4, ст.290] рассматривает компьютерные преступления. И по данной проблеме наблюдается несовершенство закона. В УК КР не прописаны конкретные виды киберпреступлений.

Следовательно, законодательную основу обеспечения и поддержания состояния информационной безопасности в настоящее время составляют Законы Кыргызской Республики «О гарантиях и свободе доступа к информации», «О защите государственных секретов Кыргызской Республики», «О средствах массовой информации», «Об электрической и почтовой связи», Уголовный кодекс Кыргызской Республики, Концепция национальной безопасности КР.

Безопасность в информационной сфере Кыргызской Республики обеспечивается: Президентом Кыргызской Республики; законодательным органом Кыргызской Республики; судебной властью Кыргызской Республики; Советом безопасности Кыргызской Республики; исполнительной властью Кыргызской Республики, включая межведомственные государственные комиссии, создаваемые Президентом Кыргызской Республики и Правительством Кыргызской Республики; органами местного самоуправления, общественными объединениями, которые принимают согласно законодательству Кыргызской Республики

участие в решении задач обеспечения и поддержания состояния информационной безопасности Кыргызской Республики.

На современном этапе развития общества в Кыргызской Республике все больше и больше возрастает роль информационной сферы как арены для деятельности органов государственной власти и управления, связанная с созданием, преобразованием и потреблением информации.

В последние годы в Кыргызской Республике проделан большой объем работ по совершенствованию обеспечения информационной безопасности. Так, в 2006 году было образовано Национальное агентство информационных ресурсов; в 2007 году – Межведомственная комиссия по вопросам обеспечения информационной безопасности; тремя годами позднее, в 2010 году – Консультативный совет Государственного агентства связи при Правительстве КР; а в 2014 году был построен Совет по информационной политике при Министерстве культуры, информации и туризма; в 2016 году - Государственный комитет информационных технологий и связи.

Тем не менее, очевидно, что создание данных агентств, комиссий и советов недостаточно. Большинство доступных нормативно-правовых актов и концепций рассматривают технологические аспекты информационной безопасности, хотя и без практических рекомендаций и механизмов ее обеспечения. То есть в существующих законах, как и в Конституции, описаны нормы обеспечения защиты национальных информационных ресурсов, систем и инфраструктуры (например – компьютеров и компьютерных сетей в уголовном кодексе КР) от неавторизованного доступа, использования, раскрытия, изменения, уничтожения и других подобных действий. Но нет четко прописанных механизмов и превентивных мер по защите от негативных целенаправленных информационных атак, относящихся к негативным информационным воздействиям на общественное сознание. 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, с также стандарты цифровой подписи. По умолчанию в Кыргызстане действуют стандарты, пронятые ГОСТ Российский Федерации.

Современный опыт борьбы с информационными угрозами показывает, что, несмотря на принципы свободы слова, либерализация информационных пространств является вещью опасной, результатом чего являются современные виды информационных преступлений, таких, как хакерство, нарушение авторских прав, информационный терроризм и т.д. Цивилизованные страны все больше тяготеют к контролю над источниками информации и адресатами, эра подслушивания и подсматривания вновь возвращается.

Нестабильная политическая ситуация во многих регионах мира, угроза распространения международного терроризма, усугубляемая недавними трагическими событиями на Арабском Востоке, Украине, Сирии и активизация международных преступных организаций, высокий уровень преступности в самой республике актуализируют вопросы обеспечения национальной безопасности государства, особенно в информационном пространстве. Так, в последнее время наряду с экономическими, политическими, нравственными, демографическими, военными, экологическими аспектами приобретают актуальность вопросы обеспечения и поддержания состояния информационной безопасности страны.

Согласно Концепции национальной безопасности Кыргызской Республики, принятой 18 февраля 2009 года, ключевое значение для национальной безопасности Кыргызстана имеет поддержание территориальной целостности и независимости на базе общезначимых принципов международного права. При этом Кыргызстан стремится к равноудаленности или равноприближенности к глобальным политическим странам-лидерам и во внешней политике, руководствуясь, прежде всего национальными приоритетами развития и обеспечения национальной безопасности.

В Концепции национальной безопасности Кыргызской Республики выражается сожаление по поводу того, что, несмотря на высокие темпы развития информационно-коммуникационных технологий в последнее десятилетие, а также широкого применения данных технологий на территории Республики, наша страна не смогла в полной мере сократить отставание от развитых стран по уровню информатизации деятельности органов государственной власти, местного самоуправления, экономики и общества. Согласно исследованиям, проводимым раз в 2 года Программой развития ООН, по индексу развития электронного правительства Кыргызская Республика была в 2003 году на 110 месте (из 193 государств). В 2004 наметилась положительная тенденция, и Кыргызстан занял с данном списке 66 место, однако со временем развитие в области разработки и применения электронного правительства сошло практически на нет. Так, по последним данным, в 2014 Кыргызстан занимал 101 место по индексу развития электронного правительства [206-212].

Такое положение вещей отчасти вызвано общеэкономическими причинами (длительный кризис в экономике, низкий уровень материального благосостояния большинства населения).

Также в Концепции упоминается, что в информационной инфраструктуре Кыргызской Республики эксплуатируются устаревшие

технические устройства и оборудования, приобретаются импортные технические и программно-аппаратные средства, средства защиты информации, что в свою очередь привели к не востребованности и простаиванию специализированных производств электронной промышленности. Автор считает, что данная проблема является одной из самых важных, так как речь здесь идет об образовании. Для того чтоб устранить данную проблему необходимо повышать качество образования, особенно в технических направлениях.

Остается открытым вопрос обеспечения доступа населения к официальной информации, так как ряд населенных пунктов Кыргызской Республики, особенно в южных регионах, не охвачены национальными телеканалами и радиовещанием, государственная сеть радиомониторинга развита не достаточно хорошо.

Другая стороны проблемы заключается в том, что не контролируется ввоз и реализация в страну несертифицированной телекоммуникационной техники и средств информационной связи. Средства защиты информации также не регистрируются как спецоборудование при прохождении границ Кыргызской Республики. В стране отсутствует единая государственная политика от защиты информационных угроз, которая регулировала и координировала бы деятельность органов государственной власти и МСУ, что, в свою очередь, объясняется недостатком финансовых ресурсов.

Одной из самых больших проблем в обеспечении информационной безопасности любого государства является подготовка кадров. К сожалению, Кыргызская Республика с данной задачей на этом этапе не справляется. Несмотря на то, что в стране зарегистрировано более 50 высших учебных заведений (по данным Национального Статистического Комитета на начала 2016-2017 учебного года было зарегистрировано 51 ВУЗа), очень мало направлений подготовки специалистов по информационной безопасности.

Все это приводит к тому, что угрозы безопасности Кыргызской Республике в информационном пространстве усиливаются, что приводит к тому что:

— во-первых, соседние государства могут начать доминировать в информационном пространстве Кыргызской Республики, что частично можно наблюдать в южных регионах;
— во-вторых, недостаток, а также низкое качество образования приведут к увеличению технологического отрыва от развитых стран, что, конечно же, приведет к усилению зависимости Кыргызской Республики от закупок зарубежной техники, что, в свою очередь, негативно повлияет на процесс обеспечения важных национальных информационных инфраструктур.

В этой связи государство обязано защищать информационное пространство страны. В Концепции отмечается, что эффективность противодействия существующим угрозам безопасности Кыргызстана зависит от консолидированных усилий и организации комплексных мер государственных органов и гражданского населения. Особо отмечается, что должно быть уделено внимание реформированию спецслужб и правоохранительных структур, а также повышению квалификации сотрудников данных служб по компьютерным навыкам, направленных, прежде всего, на упреждение и пресечение угроз и вызовов безопасности, особенно со стороны террористических и религиозных экстремистских организаций.

Основная цель механизма обеспечения национальной безопасности состоит в создании систем нахождения приемлемых ответов в области национальной безопасности, в том числе и в информационном пространстве, и их практической реализации, а также в разработке правовых основ и формировании организационной структуры органов, всестороннем обеспечении и управлении деятельностью структурных

элементов системы. Разработка правовых основ является базовым требованием, так как, как отмечалось выше, хотя есть Закон об информатизации в Кыргызской Республике, механизмы защиты информации прописаны недостаточно четко.

Руководство системой обеспечения военной безопасности в Кыргызской Республике осуществляется Президентом - Главнокомандующим Вооруженными Силами Кыргызской Республики, другими государственными органами.

Силами обеспечения внешней безопасности являются Вооруженные Силы, правоохранительные и другие органы Кыргызской Республики.

Силами обеспечения внутренней безопасности являются органы и подразделения министерств внутренних дел, чрезвычайных ситуаций, Государственного комитета национальной безопасности, Государственной таможенной службы, Национальной гвардии, а также специальные органы и службы других министерств и ведомств. Силы обеспечения внутренней безопасности привлекаются для обеспечения внешней безопасности.

Контроль за использованием сил обеспечения национальной безопасности осуществляется Президентом Кыргызской Республики и Жогорку Кенешем Кыргызской Республики.

Рассматривая Концепцию национальной безопасности Кыргызской Республики, органами управления национальной безопасности Кыргызской Республики являются органы государственной власти.

Как видно из вышеперечисленных пунктов Концепции национальной безопасности, в ней не прописаны ответственные государственные органы за информационную безопасность государства.

Здесь особо хочется отметить, что безопасность не есть продукт, обеспечение безопасности – это непрерывный процесс, в который должны быть вовлечены все вышеперечисленные органы власти.

Согласно данной Концепции, система обеспечения национальной безопасности должна надежно и непрерывно выполнять свои функции в любых условиях и обстановке, оперативно и эффективно реагировать на возникающие угрозы, своевременно восстанавливать свою способность к нейтрализации угроз.

Однако, как отмечалось выше в этой же концепции, материально-технические средства, с помощью которых можно реагировать на угрозы информационной безопасности, к сожалению, не всегда отвечают требованиям современного мира. В то же время, условиями эффективного функционирования системы обеспечения национальной безопасности являются: нацеленность на предупреждение угроз национальной безопасности, разграничение функций, непрерывное взаимодействие и согласованность усилий всех элементов системы, подконтрольность Президенту Кыргызской Республики, органам законодательной, исполнительной власти и обществу.

И так, обеспечение информационной безопасности Кыргызстана - это комплекс мер и целенаправленной деятельности государственных и общественных институтов, а также граждан, которые принимают участие в выявлении, предупреждении различных угроз безопасности и в противодействии им.

Из содержания предшествующих частей диссертационной работы видно, что проблема информационной безопасности резко обострилась с процессом информатизации на базе внедрения информационной и коммуникационной технологии в сферы жизнедеятельности общества. Как и в других странах, данный процесс в нашей республике оказывает значительное влияние на всесторонность общественного развития. Тем не менее, необходимо признать, что информатизация общества протекает не столь интенсивно, чем скажем, в странах западной Европы, но в ближайшие несколько лет ситуация может измениться. Во многом, подобные прогнозы

оправдываются перспективой интеграции Кыргызстана в мировое информационное пространство, концепция которого исходит из необходимости создания национального информационного пространства, механизмы функционирования и развития которого обеспечивают вхождение государства в глобальное информационное сообщество.

Однако, проблема информационной безопасности уникальное явление, которое в системе национальной безопасности является ключевым элементом обеспечения защищенности личности, общества и государства. Категоричность такой позиции представляется возможным объяснить следующим образом. Как уже указывалось выше, современный этап развития человеческой цивилизации характеризуется высокими темпами, обусловленными процессом информатизации. Широкий диапазон внедрения и эффективность использования информационной и коммуникационной технологии приводят к тому, что тенденция зависимости механизмов развития и обеспечения жизнедеятельности общества от указанной технологии неизменно увеличивается. В частности, функционирование современных банковских и финансовых институтов, транспортной и коммуникационной инфраструктуры, промышленного сектора, а также систем и структур обеспечения внешней и внутренней безопасности отдельно взятой страны реализуется на основе информационной инфраструктуры. В свою очередь, информационная инфраструктура государства является частью формирующейся в настоящее время глобальной информационной инфраструктуры (Global Information Infrastructure - GII), предшествующей, согласно мнению исследователей, созданию глобального информационного общества (Global Information Society - GIS**)** [159, с.5].

Суть вышеизложенного сводится к тому, что современное представление об информационной безопасности должно раскрываться сквозь призму формирования информационного общества, процесс

создания которого не столько трудоемок, сколько неизбежен.

В связи с этим главным преимуществом, на которое ориентируются многие страны, является переход к формированию информационного общества, которое основывается на внедрении современных телекоммуникационных и информационных технологий. Данное направление становится одним из главных составных информационной безопасности ряда государств.

Во многих странах подобные программы уже существуют и составляют приоритетную сферу государственной политики в области национальной безопасности. В этой связи следует отметить, что в Кыргызстане не уделяется должное внимание обсуждаемому вопросу и не ведется работа по разработке и реализации комплекса мер по развитию нормативно-правового обеспечения информационной безопасности страны.

В первую очередь, обращает внимание необходимость существенного совершенствования системы законодательства, которая должна регулировать отношения в области защиты прав и свобод человека и гражданина. Две крайности одной проблемы, такие как отсутствие прав граждан на доступ к информации с одной стороны и злоупотребление свободой массовой информацией с другой стороны, могут вызвать негативную реакцию населения, что может привести к дестабилизации социально-политической обстановки в обществе.

Первые шаги в данном направлении были предприняты с принятием закона КР «Об информации персонального характера» [14], в котором прописаны принципы обработки персональных данных. Однако в законе не прописаны механизмы, с помощью которых данные принципы можно реализовать.

К числу нормативных правовых актов КР в области информационной безопасности принятых одной из последних, относятся Закон Кыргызской Республики от 8 октября 1999 года «Об информатизации» [6].

Среди действующих в настоящее время законов наиболее важным правовым источником регламентации вопросов обеспечения и поддержания состояния информационной безопасности считаем Закон КР «О национальной безопасности» [5] и Закон КР «О защите государственных секретов КР» [7]. Характерной особенностью этих и иных нормативных правовых актов является то, что они устанавливают правовой режим организационных мер защиты информации. Последние выражаются в регулировании вопросов, связанных с определением правового статуса информации, то есть в отнесении информации к категориям открытого или ограниченного доступа, прав собственности на информационные ресурсы, механизмов и полномочий на доступ к информации, ответственности, а также установления круга государственных органов и сферы их деятельности в области защиты информации, включающей вопросы лицензирования, сертификации и стандартизации средств информационной защиты и обеспечения сохранности конфиденциальной информации. Относительно иных мер защиты информации, как показывает анализ, отечественное законодательство нуждается в существенных дополнениях. В частности, на сегодняшний день в республике практически отсутствуют нормативные правовые акты, регулирующие отношения в области создания и применения аппаратно-программных средств и методов информационной безопасности.

Примечательно, что организация информационной безопасности банковских институтов в республике представляет собой систему организационных и технических мер защиты, как информации, так и поддерживающей ее инфраструктуры, в том числе информационной. Вместе с тем, эти нормативные акты в силу известных причин не в состоянии устранить пробелы отечественного законодательства в рассматриваемой области. В этой связи представляется, что в целях совершенствования политико-правового обеспечения информационной

безопасности присутствует необходимость в принятии ряда законов, которые в состоянии установить основополагающие принципы и нормы для урегулирования уже развивающихся отношений в информационной сфере общества.

Исходя из данных обстоятельств, представляется целесообразным предложить собственное определение информационной безопасности:

- информационная безопасность страны - это обеспеченное политическими, организационными и правовыми мерами состояние защищенности наиболее существенных интересов личности, общества и государства в информационной сфере от внешних и внутренних угроз, способных нарушить фундаментальные, материальные и духовные ценности, их устойчивое развитие.

Данным определением нами преследовалась главная цель - показать неделимость информационной безопасности государства, которая должна быть равной для всех субъектов информационного взаимодействия. Представляется, что принятие Концепции информационной безопасности, специального закона «Об информационной безопасности», устранит недостатки действующего законодательства. Кроме того, необходимость специального законодательства в сфере информационной безопасности очевидна.

В странах дальнего зарубежья, особенно в технологически развитых государствах, нормативно-правовое обеспечение информационной безопасности составляет одну из приоритетных сфер государственной политики. Так, например, В 1987 году США первыми приняли специальный закон «О компьютерной безопасности» (*Computer Security Act of 1987, Public Law 100-235*). В данном документе впервые было приведено определение национальной системы информационной безопасности - под которой понимаются телекоммуникации и информационные системы, управляемые Правительством США, и которые содержат секретную

информацию либо применяются в деятельности разведки, криптологической деятельности, управляют или контролируют вооруженные силы, являются частью оборудования, применяемого в вооружении, либо являются необходимыми при выполнении военных или разведывательных операций.

Помимо иных инициатив США в области нормативно-правового обеспечения информационной безопасности особого внимания заслуживает Акт «Об управлении национальной кибербезопасностью» от 16 января 2003 года, №S.187 (National Cyber Security Leadership Act of 2003). Данным законом США преследуют цель обеспечить безопасность информационных технологий федерального правительства от киберугроз и разработать единый правительственный стандарт, применяемый в правительственных информационных технологиях.

В странах западной Европы, в контексте обеспечения информационной безопасности, нормативно-правовое регулирование получила сфера автоматизированной обработки персональных данных. Принятое в данной области законодательство направлено на обеспечение правовой защиты персональных данных в процессе автоматизированной обработки и трансграничной передачи. Подобные акты действуют в Австрии (Закон «О защите данных» 1978 года), Бельгии (Акт 1992 года «О защите данных»), Великобритании (Законодательный акт 1984 года «О защите персональных данных»), Германии (Федеральный закон 1990 года «О защите данных»), Дании (Акты 1979 года «О регистрах публичных органов власти» и «О частных регистрах»), во Франции (Закон 1978 года «Об обработке данных, файлов данных и персональных свободах»).

В целом же, текущее состояние государственного обеспечения и поддержания состояния информационной безопасности страны, особенно нормативно-правовое, показывает, что данная область нуждается в реформировании. Задачей современного этапа является определение

дальнейших направлений формирования политико-правовых механизмов в сфере информационной безопасности с учетом мировых тенденций развития Глобальной информационной инфраструктуры и национальных интересов Кыргызстана в международном информационном обмене. На наш взгляд, основные направления должны быть реализованы в следующих приоритетных областях:

— обеспечения прав и свобод человека и гражданина в информационном пространстве;
— информационного обеспечения государственных структур страны;
— развития национальной информационной инфраструктуры;
— обеспечения безопасности информационно-телекоммуникационных систем и интернет пространства, защиты информационных ресурсов.

Отдельным пунктом здесь можно отметить нормативную базу на реализацию права граждан и государства на объекты интеллектуальной собственности, которые, как правило, имеют информационную природу:

- информационный поток между государственными ведомствами и структурами тоже должен быть урегулирован при помощи специальных нормативно-правовых актов. Защита информации государственной важности должна быть приоритетной: должны быть изучены мировой опыт по внедрению моделей контроля доступа (access control models). Также, должны быть приняты нормативные правовые акты, устанавливающие порядок и условия сбора и использования, открытых государственных информационных ресурсов;

- важную роль при защите информационного пространства страны играют средства массовой информации. Таким образом, совершенствование законодательства о средствах массовой информации, включая уголовный и административный кодексы, для ограничения от распространения СМИ

информации, способствующей нарастанию вражды и дискриминации по расовой, религиозной, политической и другой принадлежности людей, а также вовлечению граждан в преступную и иную антиобщественную деятельность.

Данное законодательство должно:

- регулировать не только работу местных СМИ, но и иностранных физических или юридических лиц;

- формировать государственную структуру надзора за оборотом технических средств негласного и / или несанкционированного получения информации, включая использование данных средств государственными структурами.

Все перечисленное выше также относится и к информационно-телекоммуникационным системам и сетям связи, то есть необходимо обеспечить защиту от несанкционированного доступа (конфиденциальность), сохранность информационных ресурсов (доступность) и защиту данных от преднамеренного искажения (целостность) информации.

Также, необходимо разработать механизмы политико-правового регулирования государственной политики в области формирования информационного пространства, нет нормативно-правового обеспечения электронной торговли, электронного образования. Особо хотелось бы отметить несовершенство законодательной базы по электронному документообороту, так как у нас не прописанны стандарты электронной подписи. До сегодняшнего для стандартизированными у нас считаются алгоритмы, которые прошли государственную стандартизацию Российской Федерации. Открытые электронные ключи для цифровой подписи генерируются только одним (частным) агентством – филиалом Российской компании ДосТек Групп. При этом необходимо отметить что официальные государственные органы Кыргызской Республики не имеют права на

генерацию ключей, поскольку не имеют доступа ко всем параметрам алгоритма шифрования и генерации ключей.

В обществе растет использование иностранных информационных технологий во всех сферах деятельности личности, общества и государства. Это тоже усложняет вопрос защиты информационного пространства Кыргызстана. Необходимо отметить, что в России, с их развитой международной интеграцией в области информационных систем, наблюдаются угрозы использования «информационного оружия» против национальной информационной инфраструктуры [135]. Как отмечено в Доктрине информационной безопасности РФ, деятельность по адекватному сопротивлению этим вызовам регулируется при недостающем контроле со стороны государства.

Работ, анализирующих правовые механизмы по обеспечению информационной безопасности не много. Например, в [215] рассмотрены национальные законодательства государств–участников СНГ в сфере обеспечения информационной безопасности.

В данной части проводится сравнительный анализ законодательств стран-участниц СНГ по обеспечению информационной безопасности. Информация по законодательствам была собрана с использованием интернет источников, а именно – доступ к конституциям стран на русском языке был осуществлен через сайт юридического агентства Legal NS (адрес сервиса: http://legalns.com/). Далее, был проведен анализ законодательной базы стран, за основу были принята база, которая была собрана информационно-аналитическим порталом Digital.Report. Далее, были рассмотрены уголовные кодексы стран; поиск уголовного кодекса каждой из стран проводился вручную.

Несмотря на то, что информационная безопасность является относительно новой отраслью, в законодательных актах многих стран прописаны основные положения по обеспечению информационной

безопасности граждан страны. Так, в области обеспечения прав и свобод человека и гражданина, гарантия неприкосновенности частной жизни, личной и семейной тайны, тайны сообщений в глобальных информационно-телекоммуникационных системах в некоторых государствах прописана в основном законе страны – Конституции.

Например, статья 34 Конституции *Республики Армения*, принятая 6го декабря 2015 года, устанавливает право каждого субъекта на защиту персональных данных – то есть право на конфиденциальность. То есть должен быть разработан действенный политико-правовой механизм на национальном уровне. В статье 24 говорится о свободе обнаружения, приема и распространения идей и сведений с помощью всяких средств информации, независимо от государственных границ – право на доступ.

Согласно статьи 32 Конституции *Азербайджана*, не допускаются «сбор, хранение, использование и распространение сведений о чьей-либо личной жизни без его согласия. Государство гарантирует право каждого на сохранение тайны переписки, телефонных переговоров, почтовых, телеграфных сообщений и сведений, передаваемых другими средствами связи» [215]. Также, согласно статье 50 «каждый обладает свободой законным путем искать, приобретать, передавать, составлять и распространять информацию» [215].

Статья 28 второго раздела Конституции *Республики Беларусь* гласит, что «каждый имеет право на защиту от незаконного вмешательства в его личную жизнь, в том числе от посягательства на тайну его корреспонденции, телефонных и иных сообщений, на его честь и достоинство» [215]. Также, статья 34 гарантирует право граждан Республики Беларусь «на получение, хранение и распространение полной, достоверной и своевременной информации о деятельности государственных органов, общественных объединений, о политической, экономической, культурной и международной жизни, состоянии окружающей среды» [215].

В Конституции *Республики Казахстан*, помимо пунктов о защите информации, также определено понятие государственной тайны. Так, в статье 20 за каждым гражданином РК закреплено «право свободно получать и распространять информацию любым, не запрещенным законом, способом, с указанием того что перечень сведений, составляющих государственные секреты Республики Казахстан, определяется законом» [215]. При этом в статье 18 говорится о «праве на тайну личных вкладов и сбережений, переписки, телефонных переговоров, почтовых, телеграфных и иных сообщений» [215]. Однако оговариваются и ограничения в порядке, прямо установленных законом. Третья часть этой же статьи обязывает органы государственной власти, общественные организации, должностные лица и СМИ гарантировать каждому гражданину реальную возможность ознакомления с касающимися его правами и интересы материалами, выводами и источниками сообщений. Если обратиться к опыту Республики Казахстан, то Постановление Правительства Республики Казахстан «О Концепции единого информационного пространства Республики Казахстан и мерах по ее реализации» № 715 было принято 29 июля 1999 г. Затем последовал Указ Президента Республики Казахстан от 10 октября 2006 года № 199 «О Концепции информационной безопасности Республики Казахстан», который был пересмотрен 14 ноября 2011 года указом №174 Президента Республики Казахстан. На данный момент разработаны 63 постановления и акта по информационной безопасности, из которых 47 – действующие. Например, в Постановлении Правительства Республики Казахстан от 14 сентября 2004 года № 965 «О некоторых мерах по обеспечению информационной безопасности в Республике Казахстан» разъясняется проведение работ, обработка и хранение сведений, составляющих государственные секреты; проводится также разъяснение о подключении компьютеров, содержащих государственные секреты к локальным или глобальным сетям и т.д.

В статье 31 Конституции Кыргызской Республики прописаны права граждан на доступ к информации, в том числе находящейся в ведении государственных органов. Также, в статье 16 Конституции Кыргызской Республики перечислены права граждан на конфиденциальность личной информации.

Согласно статьи 29 Конституции Кыргызской Республики “гарантируется защита, в том числе судебная, от неправомерного сбора, хранения, распространения конфиденциальной информации и информации о частной жизни человека” [1,ст.29], но данная гарантия практически не имеют достаточного правового обеспечения.

В Конституции *Республики Молдова* статья 34 охватывает права граждан на информацию, где они описаны в 5ти пунктах, а именно – право на доступ к общественной информации, и обязанности государственных органов в обеспечении граждан достоверной информацией. Также, в пункте 3 данной статьи говорится о том, что «право на информацию не должно наносить ущерб мерам, направленным на защиту граждан, или национальной безопасности» [215] . Помимо этого, есть две статьи об информировании населения.

В РФ, например, перечень имеющихся нормативных правовых актов в сфере обеспечения информационной безопасности состоит из Доктрины Информационной безопасности РФ [135], Стратегии развития информационного общества в РФ, двадцати двух законов РФ (начиная с закона РФ от 21.07.1993 № 5485-1 «О государственной тайне» до Федерального закона РФ от 29.06.2015 № 162-ФЗ «О стандартизации»), а также девятнадцати Указов Президента РФ, пятидесяти трех Постановлений правительства РФ и девятнадцати документов уполномоченных федеральных органов. Описанные задачи по обеспечению информационной безопасности в Доктрине информационной безопасности РФ, актуальны так

же и для Кыргызской Республики, некоторые в большей, некоторые в меньшей степени.

В Конституции *Российской Федерации* статья 24 устанавливает «запрет на сбор, хранение, использование и распространение информации о частной жизни лица без его согласия и также обязывает органам государственной власти дать гражданам возможность ознакомления с информацией, если иное не предусмотрено законом» [215]. Так же, как и в Конституции Казахстана, статья 29 гарантирует «право свободно искать, получать, передавать, производить и распространять информацию любым законным способом, и при этом указывает, что перечень сведений, составляющих государственную тайну, определяется федеральным законом» [215] . Статья 71 гласит, что в ведении Российской Федерации находятся (пункт «и» Статьи 71) информация и связь.

В Конституции *Таджикистана*, статья 23 гарантирует обеспечение «тайны переписки, телефонных переговоров, телеграфных и иных личных сообщений, за исключением случаев, предусмотренных законом» [215]. Также, в статье 30 записано что сведения, составляющие государственную тайну, определяются законом.

В *Туркменистане*, статья 23 Конституции страны дает «право на защиту от посягательств на тайну корреспонденции, телефонных и иных сообщений» [215]. Также, в статье 5 говорится, что правовые акты общедоступны, за исключением тех, которые содержат государственную или иную, охраняемую законом тайну. В дополнение к этому, согласно статье 26, граждане страны имеют право доступа к не государственной информации и информациям не относящимся к коммерческой и служебной тайнам.

В Конституции *Украины* также прописана тайна переписки, телефонных разговоров и корреспонденции (статья 31) и право на ознакомление с информацией, которая не является государственной или

иной охраняемой законодательством тайной (статья 32), а также право свободно собирать, хранить, использовать и распространять информацию (статья 34). В дополнение к этому, в статье 17 Конституции Украины прописано, что обеспечение информационной безопасности (наравне с защитой суверенитета, территориальной целостности и обеспечением экономической безопасности) являются важнейшими функциями государства.

Во многих странах СНГ была принята концепция информационной безопасности государства, в некоторых был разработан проект данной концепции. Так, в Армении Концепция Информационной Безопасности была принята 26 июня 2009 года. В самой концепции, в главе VII – “Механизмы Защиты Информационной Безопасности Республики Армения”, пункте 1 – “Правовые механизмы по обеспечению информационной безопасности в Республике Армения”, указаны обзацы по созданию и использованию нормативно-правовых актов, которые регулируют отношения по обеспечению инормационной безопасности. Согласно [194], правовую основу Концепции Информационной Безопасности Республики Армения составили следующие законы:

- «О Государственной и служебной тайне»;
- «О свободе информации»;
- «О персональных данных»;
- «Об электронном документе и электронной цифровой подписи»;
- «Об электронной связи»;
- «Об органах национальной безопасности»;
- «Об актах гражданского состояния»;
- «Об архивном деле»;
- Уголовный кодекс Республики Армения;
- Гражданский кодекс Республики Армения

В Азербайжане, в 2014 году было предложено создать концепцию информацинной безопасности [196], на данный момент основным законом, регулирующим вопросы информационной безопасности является Закон “Об информации, информатизации и защите информации” Азербайджанской Республики [197]. Также, действуют законы

- “О персональных данных”;
- “О государственной тайне”;
- «О получении информации»;
- “Об электронной подписи и электронном документе”;
- “О приобретении информации” и др.

В главе 4 Концепции Национальной Безопасности также оговорена политика информационной безопасности Азербайджанской Республики.

В Беларуси, действуют следующие законы, которые регулируют задачи информационной безопасности:

- «О регистре населения»;
- «Об информации, информатизации и защите информации»;
- «Об электронном документе и электронной цифровой подписи» и др.

Также, в Концепции национальной безопасности Республики Беларусь уделяется особое внимание информационной безопасности страны, с учетом тенденций современного мира.

В Кыргызской Республике сама конценция еще не принята, однако в 2008 году был разработан проект Концепции Информационной Безопасности от 11 июля 2008 года. Согласно главе 1 данного проекта, правовую основу Концепции составляли Законы КР:

- "О защите государственных секретов"
- "О средствах массовой информации"
- "О гарантиях и свободе доступа к информации"
- "Об информатизации"

- "О правовой охране программ ЭВМ и баз данных"
- "Об электрической и почтовой связи"
- "Об электронной цифровой подписи"
- "Об информации персонального характера" и другие нормативно-правовые акты Кыргызской Республики;

Угроза информационной безопасности также упоминается в пункте 6 главы о “Внутренних Угрозах” – “Отставание в области создания и внедрения современных информационно-коммуникационных технологий и защиты информационного пространства страны» Концепции Национальной Безопасности страны.

В Молдове действует закон о предотвращении и борьбе с киберпреступностью. Также, закон о службе информации и безопасности Республики Молдова была принята в 1999 году и закон о доступе к информации – в 2000 году. Если говорить о концепции информационной безопасности, то в 2016 году был утвержден законопроект о концепции информационной безопасности Молдовы [198].

В Российской Федерации с декабря 2016 года действует Доктрина информационной безопасности. Также, по сравнению с остальными странами СНГ, очень много научных работ было проведено по анализу нормативно-правовой основы обеспечения информационной безопасности России. Согласно многим источникам, основополагающими документами, рассматривающими вопросы информационной безопасности, являются Конституция Российской Федерации, а также Концепция национальной безопасности. Также, действуют Законы РФ:

- «О государственной тайне»
- «Об информации, информатизации и защите информации»
- «О защите детей от информации, причиняющей вред их здоровью и развитию»
- «О персональных данных»

- «Об электронной подписи» и др., также методические пособия и рекомендации.

Концепция информационной безопасности Республики Таджикистан была утверждена в 2003 году. Также, согласно сведениям портала http://info-center.tj, в республике действуют следующие законы:

- "О Государственных секретах"
- "О защите информации"
- "О праве на доступ к информации"
- "Об информатизации"
- "Об информации"
- "Об электронно цифровой подписи"
- "Об электронном документе" и другие законы и нормативно-правовые акты.

В литературе мало источников касательно законодательства по информационной безопасности Республики Туркменистан. На государственном портале http://turkmenistan.gov.tm опубликован закон Туркменистана «О Правовом Регулировании Развития Сети Интернет и Оказания Интернет-Услуг в Туркменистане» от 29 декабря 2014, которое «определяет правовые основы регулирования отношений, связанных с развитием сети Интернет в Туркменистане, и устанавливает правовые основы деятельности в области оказания интернет-услуг на территории Туркменистана». Несмотря на это, в Уголовном кодексе Туркменистана предусмотрены все виды преступлений в информационном пространстве.

Доктрина информационной безопасности Украины была принята относительно недавно – 25 февраля 2017 года. Также, был принят ряд законов [214]:

- "Об информации",
- "О государственной тайне",
- "О Национальной программе информатизации",

- "О Концепции Национальной программы информатизации",
- "О радиочастот ный ресурс",
- "О телекоммуникациях",
- "О защите информации в информационно-телекоммуникационных системах".

Обзор Уголовных кодексов показал, что наказание за преступления, совершённые в информационной сфере, во всех странах объединены в отдельные главы кодексов. В среднем в главах по 7-9 статей, за исключением Уголовного кодекса Кыргызской Республики и Украины. Так, глава 24 -«Преступление против безопасности компьютерной информации» уголовного кодекса Республики Армения содержит 7 статей; в уголовном кодексе Азербайджанской Республики, в тридцатой главе – «Киберпреступления» собраны 5 статей; в уголовном кодексе Беларуси – 7 статей в главе 31 – «Преступления против информационной безопасности»; в седьмой главе уголовного кодекса Казахстана – «Уголовные правонарушения в сфере информатизации и связи» - 7 статей; Кыргызстана, в главе 28 – «Преступления в сфере компьютерной информации», в действующей версии – 1 статья; девятая глава уголовного кодекса Молдовы «Информационные преступления и преступления в области электросвязи» содержит 10 статей; в России глава 28 «Преступления в сфере компьютерной информации» содержит 3 статьи, а также статьи в главе 19 и 21 относятся к преступлениям в информационной сфере; 7 статей в главе 28 «Преступления в сфере компьютерной информации» Таждикистана; 9 статей в Главе 33 «Преступления в сфере информатики и связи» Туркменистана; в Узбекистане, глава 20-1 о “Преступлениях в сфере информационных технологий” содержит 6 статей; и в Украине 3 статьи в разделе 16 рассматривают преступления в информационной сфере.

Контентный анализ показал, что практически во всех уголовных кодексах присутствуют статьи о несанкционированном доступе к

информации; исключение составляют уголовные кодексы Кыргызстана и Украины. Статья о разработке, использовании и распространении вредоносных программ также присутствует во всех кодексах, за исключением кодекса Украины. С различной формулировкой указаны также преступления, связанные с нарушением работы информационных систем или сетей телекоммуникаций.

Если говорить о наказании за преступления в информационном пространстве, то сроки лишения свободы варьируют от 2 до 10 лет. При этом строгость наказания возрастает с ростом последствий, к которым привело то или иное преступление в информационном пространстве, особенно если оно каким либо образом повлияло на безопасность государства как целого. Самым строгим можно признать уголовные кодексы Казахстана, Туркменистана и Беларуси – в главах уголовного кодекса по информационной безопасности всетречаются статьи со сроком наказания до 10 лет. Минимальный же срок наказания – 2 года или штраф – в уголовном кодексе Армении. Наименее полной по охвату преступлений является уголовный кодекс Кыргызстана.

В уголовном кодексе Кыргызской Республики есть только одна статья, которая звучит как “Создание программ для ЭВМ или внесение изменение в существующие программы, заведомо приводящих к несанкционированному уничтожению, блокированию, модификации либо копированию информации, нарушению работы ЭВМ, системы ЭВМ или их сети, а равно использование либо распространение таких программ или машинных носителей с такими программами, - наказываются публичным извинением с возмещением ущерба или штрафом от пятисот до одной тысячи расчетных показателей либо ограничением свободы на срок до трех лет, либо лишением свободы до трех лет” [4, ст.290].

Не предусмотренно наказание за несанкционированный доступ, незаконное владение или модификацию или удаление информации (то есть

нарушение основных принципов информационной безопасности, таких как доступность, целостность и конфиденциальность информации). Но согласно вошедшим изменениям в УК КР от второго февраля 2017 года (вступит в силу с 1 января 2019 года), в главу 42 УК КР дополнительно вводятся две статьи о неправомерном доступе и компьютерном саботаже. 42 главу УК КР назвали как “Преступления против информационной безопасности”

Как видно из обзора, в странах СНГ идет разработка или уже приняты Концепции Информационной Безопасности. Однако в основном эти концепции рассматриваются исследователями как слабые. Так, в докладе [195] говорится что необходима доработка КИБ РК. Особенно в свете того, что, как показывает статистика, количество преступлений в сфере информационной безопасности только растет [199]. В Российской Федерации, к обеспечению информационной безопасности подходят комплексно. Так, согласно [200], к обеспечениюю информационной безопасности были отнесены правовые, организационно-технические и экономические методы.

Из вышеизложенного становится явным, что, для совершенствования нормативно-правовой базы, есть необходимость создания учебных заведений для подготовки кадров, как административных, так и технических. Нужны специалисты по социологии, политологии для анализа знаний и отношения общества о проблемах и вообще наличии информационных угроз. На основе анализа этих данных можно было бы разработать рекомендации для повышения грамотности населения в вопросах информационной безопасности, а также создания нормативно-правовой основы с учетом национальных интересов государства. Необходимо также на регулярной основе проводить оценку информационного воздействия и механизмов противодействия рискам.

Недостаток грамотных кадров приведет к дальнейшему усугублению информационной опасности.

Подытоживая исследование настоящей части, сформулируем следующие обобщающие выводы.

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.

2.2. Информационная безопасность - составная часть национальной безопасности Кыргызской Республики

Проблема обеспечения национальной безопасности - категория многогранная и является объектом исследования философии, политологии, социологии, экономики, юриспруденции и многих других наук. Актуальность вопроса объясняется тем, что безопасность - это важнейшая и приоритетная потребность человека. Современный этап развития международных отношений характеризуется ориентацией большинства государств на обретение устойчивого развития, создание в мире нового экономического, политического и информационного порядка. Одновременно обостряются и углубляются глобальные конфликты в экологической, политической, экономической, демографической и других сферах международного общения. Остаются нерешенными многие проблемы войны и мира, безопасности и разоружения, отсутствует политическое доверие между рядом стран, что ведет к дисбалансу интересов в современном ультраполярном мире и стремлением к монополизации отдельными державами исключительных прав на принятие окончательных решений при разрешении наиболее острых международных проблем. Совершенно очевидно, что в условиях противоречивости сложившейся к настоящему моменту системы международных отношений обеспечение безопасности национальных интересов становится центральной задачей государства.

Анализ источников показывает, что в ходе исторического развития государства эволюционировала и система взглядов на проблему безопасности, что связывают с усложнением и динамикой социально-экономической жизни многих стран, их государственно-политического

устройства, форм политических режимов и другими факторами. Сегодня на планете примерно 200 стран с разными показателями финансово-экономического развития, формами правления, государственно-политическими режимами и разновидностями политической культуры. Каждая из них имеет собственные систему национальной безопасности, которые дифференцируются по разным принципам. Согласно политической литературе существуют инфантильно-патерналистский и рационально-этатистский типы национальной безопасности. Инфантильно-патерналистский тип реализуется с помощью привития членам общества инфантильного чувства абсолютной социальной безопасности и лишения их объективной, достоверной и полной информации о новостях в мире и в самом государстве. Второй, рационально-этатистский тип связан с сознательным выделением стране функций и задач по обеспечению защиты государства от внешнего вызова. Согласно А.А.Прохожева: «В этом случае национальная безопасность является одной из немногих функций государства, во всех остальных вопросах нация не может рассчитывать на патернализм политического института. Если государство не обладает самодостаточной мощью, то и национальная безопасность в сознании граждан оказывается здесь прочно зависимой от их собственных созидательных усилий» [81, с.65].

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. Однако в промышленно развитых странах компьютеризация преступности развивалась медленно, поступательно, наравне с развитием технологий, поэтому у технических работников было время для разработки контрмер, а

у государственных законодательных органов – на подготовку нормативно-правовой базы реагирования на киберпреступления. Как было отмечено ранее, этот тип преступлений проводится посредством Интернет или в какой-либо другой компьютерной сети. В основном это становится возможным из-за низкого уровня компьютерной грамотности участников процесса обмена информацией, где участниками могут выступать как граждане, так и государственные органы, и структуры. Конечно, уровень тяжести киберпреступления становится гораздо выше, если речь идет об преступлении против информации, хранящейся в государственных органах, органах МСУ, учреждениях и предприятиях. Хотя Конституция Кыргызской Республики гарантирует право каждого гражданина знакомиться с информацией, хранящейся в государственных органах, органах МСУ, учреждениях и предприятиях со сведениями о себе, не являющимися государственной или иной защищенной законом тайной, нет продуманного механизма реализации этого положения. При этом, несанкционированный доступ и кража личных данных также является киберпреступлением. Автор считает, что безопасность начинается с осведомленности о безопасности конечного пользователя, которая может повлиять на все аспекты профиля безопасности организации. Таким образом, в качестве механизмов реализации можно предложить обязательное обучение граждан, особенно сотрудников государственных органов, работающих с информацией, представляющей интерес для КР, компьютерной грамотности и цифровой безопасности.

Как было отмечено выше, несмотря на рост киберпреступности в развитых странах, этот рост был поэтапным и зависел от развития информационных технологий. В Кыргызской Республике, а также во многих других странах постсоветского пространства, к сожалению, люди и государство не были готовы к такому росту киберпреступлений. Уровень проникновения Интернета в Кыргызской Республике составляет 24,17%, и

согласно данным Internet World Stats за 2014 год, из 158 стран наша страна занимает 112 место по уровню обеспеченности доступом к сети интернет. Несмотря на низкий уровень доступа к сети интернет в Кыргызской Республике, люди пользуются Интернетом очень часто. Молодые люди, и даже сотрудники государственных органов, часто пользуются интернетом через мобильные телефоны. Однако, как отмечалось ранее, в республике нет нормативно-правовой базы для защиты интернет пространства страны, то есть ни государство, ни интернет-пользователи не были готовы к кибер-преступлениям. По данным национального статистического комитета, уровень грамотности населения на 2014 год составляет 99,2%, в то время как в мировых рейтингах цифра эта равна 99,52% (по данным службы countrymeters.info) Однако уровень знаний информационной безопасности (ISA) никогда не изучался даже среди студентов. Если говорить об информационно-коммуникационных технологиях в государственных органах, по данным Национального статистического комитета, в 2013 году только 1,9% (то есть 80 из 4198) государственных учреждений были подключены к компьютерным сетям и 6,26% (263 из 4198) государственных учреждений и организаций имеют веб-сайты [213]. Таким образом, информационный поток в республику идет в основном за рубежом, то есть в информационном пространстве Кыргызстана преобладают зарубежные источники. В отчете Лаборатории Касперского за 2015 год сообщается, что жертвами преступления, связанного с отправкой так называемых «фишинговых» сообщений по электронной почте стали в основном пользователи русскоговорящего сегмента интернета, что автоматически повышает риски для граждан Кыргызстана стать жертвой такого рода атак. Как упоминалось ранее, Конституция Кыргызской Республики гарантирует сохранность личной информации, однако механизмы защиты не продуманы, особенно если принять во внимание тот факт, что интернет пространство не имеет физических государственных границ. Таким образом для защиты

интересов государства и граждан в информационной сфере необходимо подписание соглашений с другими государствами и международными организациями. Как отмечалось выше, Правительство КР одобрило проект Соглашения между правительствами государств-членов Шанхайской Организации Сотрудничества о сотрудничестве в области обеспечения международной информационной безопасности. Также, Правительство КР постановило утверждение Соглашения об обеспечении информационной безопасности в рамках общих таможенных процессов в государствах-членах Евразийского экономического сообщества. Таким образом, работы по международным соглашениям для обеспечения безопасности информационного пространства в республике ведутся.

Однако обеспечение политико-правовых механизмов информационной безопасности внутри страны все еще требуют пристального внимания.

Одним из механизмов, как отмечалось выше, автор считает повышение компьютерной грамотности и интернет культуры, так как через средства массовой информации и ИКТ могут вестись информационно-психологические воздействия, что может спровоцировать политическую нестабильность и социальную напряженность в обществе, через религиозные, национальные, социальные конфликты и вызвать массовые беспорядки. В стране также наблюдается рост использования ИКТ банковским сектором, и киберпреступления, направленные на хищение, несанкционированное использование или искажение деловой, например, коммерческой, банковской , а также искажение политической информации неизбежно ведут к большим экономическим или политическим потерям. Как видно из вышеперечисленного, при обеспечении национальной безопасности Кыргызской Республики немаловажную роль играет вопрос обеспечения информационной безопасности, причем, как отмечается во многих источниках, в процессе информационно-технического развития эта зависимость, потребность будет еще более возрастать. Это приобретает еще

больший вес, если учесть, что информационная безопасность является основным связующим звеном всех главных компонентов государственной политики безопасности в единое целое.

Как отмечалось выше, 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. Правовое обеспечение интересов личности в информационной сфере и ее информационная безопасность гарантируются конституционными правами граждан. В статье 31 Конституции Кыргызской Республики прописаны права граждан на доступ к информации, в том числе находящейся в ведении государственных органов. Также, в статье 16 Конституции Кыргызской Республики перечислены права граждан на конфиденциальность личной информации.

Считаем, что интересы государства в информационной сфере должны определяться созданием условий, которые будут способствовать развитию информационной инфраструктуры Кыргызстана, а также защите государственной тайны, развитии международного сотрудничества в информационной сфере на основе партнерства и с учетом защиты интересов государства.

Следовательно, интегративный характер науки о безопасности, формировавшийся на стыке общественных, естественных и технических наук и исследующей закономерности, понятия и методы защиты человека, общества, государства, подразумевает тесную связь с науками, находящимися во взаимодействии с ней. В то же время основополагающая, стержневая задача этой науки нам видится в методологическом обеспечении национальной безопасности государства.

Впервым, кто ввел термин «национальная безопасность» в оборот был Т. Рузвельт, который в 1904 г. выступил с посланием Конгрессу США по

поводу обоснования присоединения к США зоны Панамского канала. С этого периода ведет отсчет теория «национальных интересов», которая, по мнению большинства исследователей современности, является источником концепции «национальной безопасности государства». Теория национальных интересов, важный вклад в разработку которой внес основатель школы «политического реализма» Г.И. Моргентау, получила широкое признание как главная детерминанта внешнеполитической деятельности современных государств. Исходя из данной теории, существуют, по крайней мере, два основных подхода к определению концепции «национальной безопасности». Первый, определяющий национальную безопасность государства через силу, т.е. преобладание мощи над другими государствами, сложился в ситуациях, когда интересы национального значения определялись исходя из требований гарантии защиты населения, природных ресурсов, государственной территории. В тот период военная мощь представлялась в качестве главного знака силы и власти государства. Военная сила являлась главным средством, с участием которой государства осуществляли свои интересы. При современных условиях развития, когда внешнеполитический вектор государства должен учитывать факторы, которые оказывают влияние на характер и форму международной системы, например, такие, как динамика планетарной экономики, усиливающая трудности и нестабильность внутри стран и их взаимоотношениях; быстрый рост транснациональных связей, который стимулирует формирования новых видов коллективного принятия шагов развития при участии государств, международных групп давления, межправительственных организаций; безостановочное развитие транснациональных систем коммуникаций; распространение технологий в военной сфере, становящиеся элементом постоянного характера современной мировой политики. Также и другие концепции «национальной безопасности» рассматриваются с точки зрения взаимодействия государств.

В контексте настоящего исследования представляет интерес точка зрения, касающаяся правомерности применения термина «национальная безопасность». В данном случае проблема заключается в том, что понятие «национальный» содержит признаки, имеющие этнический характер и, соответственно, в многонациональных государствах, к примеру, Франции, России, Кыргызстане и ряде других стран, содержание концепции национальной безопасности практически должна сводиться к обеспечению интересов титульной нации. На наш взгляд, подобная позиция необоснована и чревата межэтническими конфликтами, направлена на раскол общества, подрыв конституционного строя и демократических институтов того или иного государства. Анализ Устава ООН, в частности, п. 2, ст. 1; ст. 55, показывает, что действительными акторами современных международных отношений выступают национальные государства или нации-государства, в то время как термин «народ», как субъект самоопределения, употребляется в отношении населения или граждан, проживающих на территории соответствующего государства.

Таким образом, согласно Закона КР «О национальной безопасности» «…под национальной безопасностью необходимо понимать состояние защищенности интересов личности, общества и государства от внутренних и внешних угроз» [5]. Следовательно, имеется в виду безопасность всего народа определенного государства, а не какой-либо отдельной этнической группы. Кроме того, наряду с национальными интересами главную роль в формировании, развитии и обеспечении национальной безопасности решают национальные цели и национальные ценности.

Под национальными ценностями обычно понимают фундаментальные нравственные нормы, обычаи, традиции, которые в большей степени определяют цели жизни и судьбы людей, достояние общества в направлении материальной и духовной культуры. Из материального, к примеру, к национальным ценностям можно отнести также уникальные

природные богатства государства и общества. Таким образом, национальные ценности – это ценности, которые складываются естественным путем по мере развития общества.

Национальные интересы, в свою очередь, - это официально признанное, выраженное отношение государства к национальным ценностям. Определение вопроса национальных интересов является центральным вопросом для любой страны в мире, потому что только их уровень показывает уровень безопасности и защищенности, как отдельного человека, гражданина, так и государства и общества. Долгосрочные стратегические планы и политика государства должны формироваться только с учетом национальных интересов.

Согласно, теории национальной безопасности выделяют три группы национальных интересов: наиболее существенные интересы, важные интересы и просто интересы [149, с.100].

Наиболее существенными интересами считается система потребностей, удовлетворение которых крепко и надежно обеспечивает существование, развитие и возможности безотрывного, прогрессивного развития личности, общества и государства. Если приводить аналогию теорией с информационной безопасности, и интересы сопостявлять с видами информации, то к первой группе относятся информация, утрата которой подрывает основы существования граждан, общества, государства. Такой информации присуждается уровень высшей секретности. Аналогично можно охарактеризовать важные интересы и просто интересы.

Следует отметить, что в научной литературе дискуссионным является вопрос о государственных и национальных интересах. Суть полемики заключается в том, что наличие связи обеих категорий еще не говорит об их тождестве и, соответственно, речь должна идти о совершенно самостоятельных формах выражения государством отношения к национальным ценностям. По мнению М.В. Ильина, здесь следует брать за

основу «…интерес нации как двуединство суверенного территориального государства и гражданского общества» [217]. Гражданское общество и суверенное территориальное государство не только связаны между собой содержательно с понятием «национальные интересы, но и по большей мере определяют его смысловую структуру.

Далее, национальные цели - один из важных элементов в системе национальной безопасности и непосредственно связаны с интересами государства. Защита национальных интересов в пространственно-географическом плане не ограничивается пределами территории станы, тем более, когда речь идет о национальных целях в информационном пространстве, так как, как известно, ИКТ и интернет не имеют физических границ. Многие процессы, происходящие в разных частях мира, влияют на существование и развитие определенного государства, развитие общества, на формулирование и обозначение национальных целей.

В настоящее время национальная безопасность является многогранной, многоуровневой, сложной системой, образующийся целым рядом подсистем. И эти подсистемы имеют свои собственные структуры. Принято говорить о «системологии национальной безопасности», которая выполняет важную методологическую функцию в содержательном анализе национальной безопасности. Наука о безопасности (секьюритология), определяющая системный подход в качестве основополагающего методологического принципа, содержание его раскрывает в плоскости соотношения части и целого. Целое не тождественно сумме составляющих его частей по своим главным характеристикам, по роли и значению, по заложенным в нем возможностям. В результате взаимодействия частей целому придается новое качество отсутствующие и возникающие в частях. В меньшем масштабе может рассматриваться как целое и часть целого. Потому что она обладает относительной самостоятельностью, присущими

ей качественными особенностями. Так, каждая часть оказывает определенное влияние на развитие, формирование и сущность целого.

Во- первых, явление в сфере безопасности изучается как целое, которое относительно самостоятельно и включает ряд событий с меньшим масштабом. Во-вторых, это явление является частью большого явления, испытывающее его влияние, и которое воздействует на него.

В обобщенном виде целое исследователями представляется в виде системы «Субъект - Объект - Безопасность», при этом, на наш взгляд, ключевым, связующим элементом является центральное звено этой системы - объект. Подобная структура не случайна. Объект есть определяющий фактор, который приводит в действие всю систему безопасности, так как, если отношения субъекта и объекта сводятся к целенаправленной деятельности первого негативно воздействовать на объект, то взаимосвязь и взаимообусловленность объекта и безопасности раскрываются посредством нейтрализации угроз, исходящих от субъекта. В то же время, подразумевая под объектом определенную категорию, которая противостоит субъекту в его предметно-практической или познавательной деятельности необходимо иметь в виду, что данная категория влияет на динамику и тенденцию развития всей системы национальной безопасности. Это является закономерным вследствие того, что объект есть не что иное, как субъективные и объективные потребности личности, государства, общества, которые реализуются во всех направлениях их повседневной деятельности. Переориентация ценностей, что происходит в силу различных факторов, в том числе и временных, непременно отражается на смене приоритетов в целостной системе национальной безопасности. Возникают новые сферы удовлетворения потребностей, в то время как существовавшие наполняются новым содержанием. Соответственно, эволюционирует и система безопасности в государстве, которое, с учетом состояния и условий

протекающих общественных процессов, определяет координаты и направления развития всей системы национальной безопасности.

С точки зрения информационной безопасности, выделяются следующие компоненты информации:

- для реализации прав и обязанностей субъекта в обществе необходимо обеспечить доступ к достаточно полной и достоверной информации;

- безопасность и охрана субъекта от деструктивных информационных воздействий;

- защита и охрана от несанкционированного воздействия на информацию, которая принадлежит субъекту;

-охрана информационной инфраструктуры состава субъектов (организации, объединения, государства) от губительных влияний.

Как видно, первые три составляющих связаны непосредственно с безопасностью знаний, где для защищаемого, охраняемого объекта значима именно информация влияния. При этом главной целью информационного нападения или предметом, бессменно считается информация воздействия, т.е. восприятие субъекта (нападающая сторона) в случае попытки несанкционированного получения информации. Тоже касается и объекта, пытавшегося в попытке совершить дезинформацию, введения отвлекающей информации или искажения информации.

Информационная инфраструктура является одним из важных факторов, которая оказывает влияние на представительную сторону информации, являясь основным средством распространения последней в т.н. среде, которая имеет искусственный и естественный характер. Например, воздух является естественной средой распространения информации. Информационная инфраструктура является искусственной средой распространения информации. Она обеспечивает удовлетворение потребностей человека, общества, государства в хранении, сборе, обработке, передаче и распространении всей надлежащей им информации.

Согласно исследователям, существуют две главные составляющие информационной инфраструктуры современного общества – технологическая и организационная. Организационная образующая состоит из средств связи, информатизации, телекоммуникации; механизма построения и обеспечения защиты, целостности информационных ресурсов. К организационной составляющей информационной инфраструктуры относится и система обеспечения сетей связи, доступа к информационно-телекоммуникационным системам и информационным ресурсам. Также подготовка и переподготовка кадров индустрии информационных услуг и информационного рынка, проведение научных исследований являются самыми важными организационными составляющими информационной инфраструктуры.

Совокупность информационно-вычислительных систем, которые объединены системой передачи данных, являются информационно-телекоммуникационными системами технологической составляющей информационной инфраструктуры.

Современное и, наверняка, будущее состояние развития информационной инфраструктуры с экспансией во все направления жизнедеятельности личности, общества, государства не только выполняет функции передачи сообщения оперативно и без искажений, но и чревато риск-фактором, когда присутствует вероятность искажения необходимой информации, ее потери или несвоевременной доставки промежуточному или конечному адресату. Вследствие этого, защита информационной инфраструктуры - неотъемлемая составляющая информационной безопасности, которая, в свою очередь, обеспечивает целостность (не разрушаемость) среды распространения информации.

Изложенным определяется исключительность информационной сферы в современной системе национальной безопасности, являющийся системообразующим фактором во всех сферах безопасности.

Информационная сфера активно воздействует на состояние экономической, политической, социальной, военной и другие составляющие безопасности государства. И сегодня, когда уже явно наблюдается зависимость национальной безопасности государства от обеспечения информационной безопасности, в дальнейшем, в результате диверсификации развития и распространения современных информационно-коммуникационных технологий, являющихся своеобразной платформой информационной сферы, эта зависимость будет усугубляться. Так, например, политический вес любого государства на международной арене, его возможность воздействовать на события в мире сегодня зависят не только от военной и экономической мощи. Сейчас большую, решающую роль играют информационные факторы. Открываются дороги и возможности эксплуатировать интеллектуальный потенциал других стран. Также существуют возможности распространять и внедрять свои духовные, идейные ценности, свою культуру, язык. Стали доступными и возможными сдерживание духовно-культурной экспансии, трансформирование и подрыв духовно-нравственных устоев других государств, В свою очередь, в экономической сфере - потенциал государства начинает во все большей степени определяться объемом информационных ресурсов и уровнем развития информационной инфраструктуры. Но в то время система разведки, управление войсками, высокоточным оружием, радиоэлектронная борьба становятся зависимыми от уровня информационных технологий и качества добываемой информации.

С исследовательской точки зрения, информационная сфера или информационное пространство представляет собой весьма специфическую среду, в которой заметно меняется содержание таких процессов, как, в частности, взаимодействие в процессе совместной деятельности или конкуренция (через изменение содержания и характера конкурентной

борьбы между действующими в нем субъектами). Кардинальным образом преломляется и характер геополитической конкуренции, выражающийся на современном этапе войной за реализацию информационного превосходства, владение относительно самым развитым информационным ресурсом или технологиями, которые открывают реальные средства и возможности контроля над контрагентом. Более подробно понятие информационной среды было рассмотрено в Главе 1 настоящей диссертации, в теоретических аспектах исследования информационной безопасности.

В целом, информационная сфера является областью фактически любого субъекта деятельности (личности, профессиональных групп, субъектов органов государственного управления и т. д.), осуществляющего таковую целиком или частично с использованием возможностей современных информационных технологий.

Как указывалось, уровень и динамика развития информационной сферы важнейшим образом влияют на социально-политическую, экономическую сферы общества, тем самым оказывая влияние на поведение людей. Более того, информационная сфера влияет на формирование общественно-политических движений и социальную безопасность. Потому что информационная сфера является обладателем национально-специфичных способов построения, разработки (обработки) и распространения информации.

В настоящее время общество испытывает острую потребность активного государственного участия в процессе формирования политики национальной безопасности страны в информационной сфере. Это обусловлено тем, что повышается зависимость общества от степени безопасности используемых им информационных технологий, от которых зависит благополучие и жизнедеятельность людей. А это связано с развитием и усложнением средств, методов и форм автоматизации процессов обработки информации. Актуальность и важность

рассматриваемой проблемы определяется развитием глобальной сети Интернет, которая не позволяет в полной мере обеспечить безопасность систем обработки информации в мире.

Представляется, что инициативы со стороны государства в этой области должны быть реализованы в следующих основных направлениях:

- необходимо найти баланс между свободой обмена информацией и допустимыми ограничениями ее распространения, с учетом, например, уровня секретности информации;

- необходимо совершенствовать саму информационную структуру, то есть структуру ИКТ, дать приоритет наукоемким направлениям в образовании для ускорения развития новых информационных технологий, или хотя бы их широкое распространение и внедрение, а также разработку отечественными разработчиками средств поиска, сбора, хранения, обработки и анализа информации с учетом интеграции государства в глобальную информационную инфраструктуру. Причем количество факультетов технического направления в Кыргызстане способствует развития нашего ИТ сектора:

- разработка законодательства и координации работы государственных органов, которые решают задачи обеспечения информационной безопасности;

-приоритетное развитие государственной индустрии телекоммуникационных и информационных средств, их протекционирование на внутреннем рынке;

- защита государственного и частного информационного ресурса.

Перечисленные объективные факторы или цели информационной безопасности обеспечиваются применением следующих механизмов или принципов, которые могут быть как с использованием технологий, так и без них, а именно:

— с использованием политических механизмов, основываясь на нормативных и правовых актах, которые регламентируют функционирование механизмов, обеспечивающих информационную безопасность;
— использование процесса идентификации, то есть распознавания участников процесса информационного взаимодействия, то есть, если говорить на примере из реальной жизни – это как назвать свое имя;
— использование процесса аутентификации — доказательство того, что участник процесса обмена информацией идентифицирован верно. Опять, по аналогии с реальной жизнью – это предъявление паспорта, т. е. пользователь доказывает, что действительно является тем, чей идентификатор он (она) предъявил(а);
— методы контроля доступа — то есть необходимо разработать свод правил, определяющий какой из участников процесса информационного обмена имеет какой вид доступа к той или иной информации. Под видом доступа имеется в виду доступ с правом прочитать документ, редактировать документ или удалить его. Естественно, перед этим необходимо определиться с градацией информации, то есть необходимо разделить информацию по уровням секретности, и далее определить разрешение каждого участнока на доступ к ресурсам и уровень этого доступа;
— авторизация — понятие, тесно связанное с предыдущим термином – определяет, имеет ли конкретный участник процесса информационного обмена доступ к информации данного конкретного уровня секретности, если есть, то какого рода доступ и т.д., то есть контроль уровня доступа;
— аудит и мониторинг — также является одним из важных механизмов обеспечения информационной безопасности. Аудит и мониторинг представляет собой регулярное отслеживание и запись каждого

процесса при обмене информацией. При этом должно учитываться кто, когда и к какого рода информации обращался, с объязательной регистрацией и анализом подозрительных событий;

— управление конфигурацией — означает обеспечение работоспособности системы, в соответствии с требованиями информационной безопасности. Обычно управление проводится администраторами системы, однако при этом по требованиям информационной безопасности все участники информационного обмена, включая системного администратора, должны подчиняться административным правилам, на основе которых были выработаны модели контроля доступа. Здесь следует отметить, что существует мнение, что у администраторов сетей и программистов, разрабатывающих систему, появляются инструменты влияния на состояние информационной системы. Однако если система была разработана в соответствие с правилами обеспечения и поддержания состояния информационной безопасности и с учетом современных научных подходов к формированию модели контроля доступа, эти риски минимизируются или полностью ликвидируются. К правилам обеспечения и поддержания состояния информационной безопасности на программном уровне относится, например, правило разделения задачи, то есть написание кода по одной процедуре не может быть выполнена только одним программистом во избежание создания так называемых “back doors” – лазеек через механизмы контроля доступа;

— управление рисками и восстановление системы — обеспечение возможности восстановления потерь при нарушениии информационной безопасности или в случае коллапса системы.

Обособление информационной безопасности в качестве нового вида национальной безопасности является как следствием рассмотренных процессов, так и необходимым условием осуществления государственной

политики обеспечения безопасности страны в целом. С методологической точки зрения, выделение информационной безопасности в самостоятельную категорию главным образом связано с необходимостью защиты национальных интересов в информационной сфере, которые определяются тем, что информация и информационная инфраструктура обеспечивают прочное развитие нации в определенных исторических условиях и удерживают национальную общность**.** Тем самым, **с**балансированная совокупность интересов личности, общества, государства, в том числе их интересы в сохранении национальной общности определяются как национальные интересы в информационной сфере. Интересы личности - это поддержание определенного правового статуса человека и гражданина, направленное на пропаганду своих идей, сохранения неприкосновенности своего внутреннего мира, свободу распространения интеллектуального творчества, свободу самосовершенствования и самореализации. Они направлены также на поддержание общения с другими людьми, интеллектуальное , духовное, физическое развитие, охрану личной свободы и информации, которая должна обеспечивать личную безопасность от возможности ее ограничения другими людьми, общественными организациями, государством.

Интересы общества выражаются в упрочении демократии, достижении и поддержании общественного согласия, обеспечении интересов личности в информационной сфере. Также они ориентированы на использование информационной инфраструктуры и информации, чтобы обеспечить устойчивое развитие всех сфер общественной деятельности. Согласно Стрельцову А.А. последнее достигается, с одной стороны, в процессе «…интеграции информационных сфер различных стран мира в единую информационную сферу и формировании единого информационного пространства, создании глобальных информационно-телекоммуникационных сетей и внедрении новых информационных технологий в

инфраструктуру общества, а с другой, преобразованием жизни современного общества, его экономики, системы образования, культуры и тому подобное на основе интенсивного развития информационной инфраструктуры» [218].

А интересами государства являются гармоничное развитие и стабильное функционирование информационной инфраструктуры, реализации конституционных прав человека и гражданина в области получения и пользования информации; политическая, экономическая и социальная стабильность; использование информации и информационной инфраструктуры для обеспечения государственной политики; управление делами общества и защиты его нравственных ценностей и др. При этом деятельность государства по реализации своих интересов имеет как внутреннюю, так и внешнюю направленность. Структурное содержание безопасности национальных интересов в информационной сфере раскрывается следующим образом:

- безопасность сведений и сообщений: гарантия защиты информации;

- безопасность информационно-телекоммуникационных систем и систем массовой информации: безопасность информационной инфраструктуры;

-защита правового статуса человека, гражданина в информационной деятельности;

- безопасность деятельности по реализации национальных интересов.

Возьмем к примеру интернет пространство Кыргызской Республики. Хотя интернет-угрозы в Кыргызской Республике являются «самым низким» уровнем киберпреступности - хулиганством, хакитивизмом и кибермошенничеством, риски растут. Например, за 5 месяцев 2015 года в Кыргызской Республике было 7 атак на государственные веб-сайты, хотя за весь 2014 год - 4 атаки [194]. Поэтому для страны на данном этапе развития

информационно-коммуникационных технологий важно повысить уровень информированности пользователей о безопасности.

Подытоживая исследование настоящей части, сформулируем следующие обобщающие выводы:

Национальная безопасность представляет собой целостную систему, динамика развития которой находится под воздействием различных факторов. Информационная безопасность является неотъемлемой составляющей данной системы и в условиях глобальной информатизации играет решающую роль в обеспечении политической независимости государства. Сформировалась информационная сфера общества, где защита национальных интересов обеспечивается системой информационной безопасности. Сбалансированная совокупность интересов личности, общества, государства, в том числе их интересы в сохранении национальной общности определяются как национальные интересы в информационной сфере. Государственная система обеспечения информационной безопасности должна быть организована на должном, соответствующем уровне. Потому что, государство может эффективно противостоять информационным вызовам только при полном взаимодействии всех органов государственной власти, органов МСУ, а также негосударственных систем. Такой подход может быть реализован лишь после разработки своевременной Концепции информационной безопасности КР. 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.

Глава 3. ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ – ФАКТОР БЕЗОПАСНОСТИ В ПОЛИТИЧЕСКОЙ СФЕРЕ КЫРГЫЗСТАНА

3.1. Основные внешние и внутренние факторы, влияющие на политику безопасности в информационной сфере Кыргызстана

Для того чтобы понять, что является угрозой, необходимо понять, что же такое стабильность системы. В самом деле, без определения принципа стабильности, т.е. слаженного, поступательного развития системы, находящейся под самоконтролем было бы невозможно определить, что является угрозой безопасности, так как при условии постоянной принципиальной изменчивости явлений, любое воздействие, порождающее подобные изменения, могло бы быть определено как угроза, или же, наоборот, опасные явления в условиях хронической нестабильности процветали бы наравне с позитивными. Таким образом, состояние стабильности и безопасности системы - понятие относительное, если его рассматривать в противовес состоянию изменчивости. Например, развал СССР был вызван рядом внутренних и внешних факторов (угроз), которые привели к критическому нарушению безопасности всей системы и ее отдельных структурных компонентов (республик, автономий, этнических групп и т.д.). Такое нарушение состояния безопасности пространства СССР стало прямым следствием нарушения структуры и функций СССР как политической, экономической, социальной, культурной, идеологической системы.

Определение угроз – достаточно трудоемкий процесс. Даже до информационной эры распознание факторов, влияющих на стабильность развития и существования государства было нелегко. Традиционно для государств определяли внешние угрозы и внутренние.

Однако, как было неоднократно упомянуто в предыдущих главах данной работы, в эпоху развития ИКТ и глобализации, с возникновением и

развитием информационной сферы определение того, что есть внутренняя угроза, а что есть внешняя стало еще труднее. Именно поэтому современные угрозы определяются не странами и обществами, в которых царит нестабильность и хаос, и даже не теми, которые считают себя переходными обществами, а странами и обществами со стабильной политической структурой, с развитой экономикой, с далеко идущей стратегией развития своей системы в общем пространстве отношений. Нет ничего удивительного в том, что, например, именно Соединенные Штаты Америки определяют наркобизнес как угрозу для себя, а не Афганистан или Ирак. Чем стабильнее система, тем она чувствительнее по отношению к разного рода угрозам своей стабильности, тем лучше она реагирует на них.

Если говорить об информационной безопасности, то стабильность и в этом случае можно назвать критерием, по которому то или иное явление может быть определено как угроза. Причем, информационные системы не определяются однозначно, в отличие, например, от политических или экономических систем, которые могут быть определены в рамках конкретных субъектов политической и экономической жизни общества. Политические системы классифицируются по таким признакам, как их участие в формировании и осуществлении власти, внутри- и внешнеполитической направленности их деятельности, особенностях их формирования и легитимности функционирования и т.д., Классификация информационных систем, по которым определяется информационная безопасность государства, в том же формате, что и политические системы не представляется возможным, т.к. субъектами-носителями информации являются любые виды систем в живой природе, имеющие значение друг для друга.

Носителем информационной системы является как отдельная личность, так и сообщества, группы, коллективы, институты, организации, общество в целом. Любая информационная система ценна не только сама по себе, но и,

что более важно, ее ценность раскрывается в соотношении с другими информационными системами. Информация меняет источник на носителя, носителя - на хранителя.

Набор взаимосвязанных информационных единиц, имеющих определенное значение и представляющих собой определенную ценность, т.е. имеющих смысл, составляет содержание информационной системы. Кроме того, информационная система предполагает наличие механизма хранения и передачи информации, а также обеспечения целостности и безопасности, как содержания, так и формы самой системы. Так, любая система знаний предполагает наличие механизмов передачи этих знаний, их обновления, защиты авторских прав, и т.д. Системы, хранящие конфиденциальную информацию, наделены усложненной системой защиты и предполагают ограниченный доступ. В этих случаях угроза безопасности такой информационной системы - нарушение режима ограниченности ее доступности.

Информационная безопасность - современная область исследования и обеспечения безопасности информационных систем, структур и функций. Информационная безопасность - это и состояние безопасности информационной системы, и качество защищенности от угроз информационным качествам (структуре и функциям) системы. Так, проблема информационной безопасности возникает не только тогда, когда существует угроза информационной системе (например, базе закрытых данных), но и тогда, когда уязвлены информационные функции неинформационных систем и структур (например, государства).

В современных условиях становления мирового информационного пространства перед Кыргызстаном остро встает задача надежной защиты собственного информационного пространства от любого вида внешней информационной агрессии. Необходимо отметить, что к внешним угрозам

или негативным факторам информационной безопасности государства относятся:

- распространение искаженной информации тем или иным государством с целью осложнения внутриполитической ситуации;
- стремление овладеть информацией государственной важности (посягательство на стратегические государственные информационные ресурсы);
- активизация духовно-культурной и идеологической экспансии и усиление зависимости молодого поколения от внешних информационных воздействий;
- стихийные бедствия.

В целом, вопрос об информационной безопасности Кыргызстана, как правильно считают отечественные исследователи, тесно связан с созданием общекыргызстанского информационного пространства и интеграцией последнего в мировое информационное пространство. Однако здесь возникают проблемы, как материального, так и социального плана:

- значительное отставание в развитии собственных технических средств и разработок;
- отсутствие систематического опыта работы на уровне мировых стандартов;
- несоизмеримость законодательных основ функционирования средств массовой коммуникации в Кыргызстане и в развитых странах;
- опасность информационной экспансии развитых стран и возможность информационной интервенции (духовно-нравственной, экономической, культурной и т.д.).

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 сожержания 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" 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 об технике и технологиях, используемых государственными структурами. Автор хотел бы еще раз подчеркнуть важность образования и развития науки как одну из мер для устранения такиги вида 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.

Отмечая внешние угрозы для информационной сферы Кыргызской Республики, в 2008 году Правительство Кыргызской Республики разработало постановление «О проекте Концепции информационной безопасности Кыргызской Республики» (которого сейчас нет, но и тогда не была утверждена как концепция). К угрозам в проекте были отнесены: «разработка рядом стран концепций информационных войн, создание ими информационного оружия, а также ведение этими государствами всевозможных видов разведки в интересах достижения преимущества в информационной сфере; увеличение технологического отрыва ведущих мировых держав, усиливающее зависимость Кыргызской Республики от закупок зарубежной техники для обеспечения важных национальных информационных инфраструктур; деятельность международных экстремистских, террористических и других преступных сообществ, антиобщественных организаций и групп в информационной сфере Кыргызской Республики, их интерес к обладанию информационным оружием и его применению; обострение международной конкуренции за обладание стратегически важной информацией; стремление ряда стран к доминированию в информационном пространстве Кыргызской Республики и получение доступа к информации с ограниченным доступом; введение некоторыми государствами на своих информационных рынках всевозможных ограничений, ущемляющих интересы Кыргызской Республики; нарушение деятельности по ряду объективных и субъективных причин, в том числе под влиянием отдельных стран и транснациональных корпораций специализированных научно-технических учреждений и производственных мощностей Кыргызской Республики, усложняющих создание собственных технических и программных средств защиты информации и конкурентоспособной информационной продукции; рост

транснациональной преступности в сфере компьютерных технологий и информации, нарушающей сохранность информационных ресурсов и штатное функционирование государственных информационных систем» (Постановление Правительства Кыргызской Республики О проекте Концепции информационной безопасности Кыргызской Республики от 11 июля 2008 года № 372).

К основным внутренним угрозам информационной безопасности относятся: 1. отсутствие в Кыргызской Республике четко сформулированной национальной политики по информационной безопасности; 2. несовершенство нормативно-правовых основ; 3. бесконтрольность частных телерадиовещательных компаний; 4. использование государственных активов и финансовых ресурсов при создании информационных компаний.

Внутренними угрозами информационной безопасности, по мнению соискателя, также являются процессы и действия субъектов информационной сферы, осуществляющих свою деятельность на территории Кыргызской Республики. К таким угрозам относятся: отставание Кыргызской Республики от многих стран мира по уровню информатизации деятельности органов государственной власти местного самоуправления и хозяйствующих субъектов; невостребованность и простаивание специализированных производств электронной промышленности и, как следствие, эксплуатация устаревших технических устройств и оборудования, приобретение импортных технических и программно-аппаратных средств, а также средств защиты информации при создании и развитии информационной инфраструктуры Кыргызской Республики; недостающий интерес к вопросам развития, разработки и реализации единой политики государства по обеспечению информационной безопасности Кыргызской Республики.

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.

К сожалению, у правительства КР нет четкой государственной политики в области формирования и регулирования национального информационного пространства (включая интернет пространство), средств массовой информации и коммуникации (в том числе новостных интернет порталов и пользовательских каналов), организации международного информационного обмена (включая интернет трафик). Из-за того, что в стране нет наукоемкого и инженерного производства и области ИКТ, информационно-(теле)коммуникационные системы являются уязвимым звеном в цепи информационной безопасности. Как отмечалось выше, наблюдается эфирная (информационная) экспансия со стороны приграничных государств, также наблюдается активное использование интернет пространства, особенно социальных сетей, различными религиозно-экстремистскими и террористическими организациями, при этом жертвами негативного информационно-психологического воздействия становятся жители сельской местности и отдаленных регионов республики.
Становится явным, что законодательную базу КР необходимо доработать, так как она не покрывает все возможные ситуации, возникающие в информационном пространстве. Нет единой базы при работе с населением, да и для создания такое базы не проработаны правовые основы для обеспечения безопасного сбора, обработки, хранения и передачи данных между различными министерствами и ведомствами КР. Также отсутствует единый орган по обеспечению информационной безопасности, несмотря на то что есть ряд государственных органов, призванных заниматься сбором, обработкой и хранением информации, которые нередко дублируют друг друга. Однако, по мнению автора, в данных структурах наблюдается

нехватка специалистов по информационной безопасности. 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.

Из вышеизложенного становится явным, что есть необходимость создания единого учебного заведения для подготовки кадров, как административных, так и технических. Нужны специалисты по социологии для анализа знаний и отношения общества о проблемах и вообще наличии информационных угроз. На основе анализа этих данных можно было бы разработать рекомендации для повышения грамотности населения в вопросах информационной безопасности, а также технических заданий для ИТ специалистов, которые будут разрабатывать программное обеспечение для сбора, хранения, обработки, передачи и распространения информации. Необходимо также на регулярной основе проводить оценку информационного воздействия и механизмов противодействия рискам. Недостаток грамотных кадров приведет к дальнейшему усугублению информационной опасности.

Подытоживая данный параграф, сформулируем следующие обобщающие выводы:

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.

К основным внутренним угрозам информационной безопасности относятся: отсутствие в Кыргызской Республике четко сформулированной национальной политики по информационной безопасности; несовершенство нормативно-правовых основ; бесконтрольность частных телерадиовещательных компаний; использование государственных активов и финансовых ресурсов при создании информационных компаний.

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.

Кыргызстан нынче остается в зоне информационной войны других государств, использующие существующую в настоящее время стране ситуацию, чтобы достичь определенные цели. То есть – изменения информационного пространства с тем, чтобы оказывать воздействие на ход явлений и событий. В Кыргызстане должна быть четкая линия по обеспечению информационной безопасности, включающая в себя огромный набор идей, знаний как безопасность [пользовательской] информации, информационная безопасность, кибербезопасность. Так как он является главным аспектом, который касается сохранности технологических моментов, защищенности законных прав и информационных ресурсов.

Следовательно, перед вступлением в Евразийский экономический союз (ЕАЭС) Кыргызстан оказался без собственной стратегии информационной безопасности и теперь не сможет получить необходимые преференции. И это, уже существующие внешние и внутренние угрозы информационной

безопасности Кыргызстана. Можно отметить факт, что если была бы утвержденная стратегия, концепция, которые учитывали бы интересы Кыргызской Республики, то можно было бы принять собственный шаг, то есть создать информационный профилактический, предупредительный набор методов и способов, как это, например, делает соседний Казахстан.

3.2. Построение политических механизмов обеспечения информационной безопасности и методы ее воплощения в жизнь

В современном обществе развитие информационных и коммуникационных технологий (ИКТ) во многом определяет путь развития стран. Глобальная информационная инфраструктура, электронные формы коммуникации, формирование информационной индустрии стали реалиями повседневной жизни и являются основой для построения информационного общества. Переход к информационному обществу на государственном уровне приводит к развитию электронных правительств. Использование электронного правительства значительно облегчает доступ к государственным услугам для граждан, бизнеса и помогает также облегчить взаимодействие между правительственными агентствами.

Наряду с этим растет необходимость в разработке политико-правовых механизмов для регулирования потоков информации для обеспечения информационной безопасности, так как угрозы информационной безопасности не только не уменьшаются, а наоборот только растут. И если для регулирования теле-радио-вещания и печатных потоков информации нормативно-правовая база разработана в более или менее полном объеме, то, согласно результатам анализов, проведенных, например, в РФ и РК показал несовершенство нормативной правовой базы и неготовность органов государственной власти к их применению. Если говорить о законодательной базе Кыргызской Республики, то обзор Уголовного

Кодекса КР, к примеру, показал что есть несколько статей, где упоминаются меры наказания за преступления, связанные с несанкционированным сбором, хранением, обработкой и передачей информации, а именно: Статья 193 - Незаконное получение информации, составляющей коммерческую или банковскую тайну; Статья 226 (3) и 226 (6) - Публичные призывы (одобрение) чтобы осуществить террористическую деятельность или публичное оправдание терроризма, в пункте (2) - совершенные с использованием средств массовой информации или сети Интернет; Глава 28 -преступления в сфере компьютерной информации, Статья 290 - Создание, использование и распространение вредоносных программ для ЭВМ и т.д. Однако данные статьи не покрывают всего спектра киберпреступлений, хотя, с другой стороны, с развитием информационных технологий уровень незаконной деятельности в киберпространстве становится реальной угрозой. Несмотря на рост компьютерной грамотности и уровень доступности интернета, уровень осведомленности об информационной безопасности среди пользователей по-прежнему остается очень низким. В то же время, преступления в киберпространстве больше не требуют сложных навыков или методов. В основном это из-за хакеров так называемого «верхнего» уровня, которые разрабатывают и делают доступными многие методы или инструменты взлома. В частности, по данным западных источников, число молодых людей из развивающихся стран, занимающихся киберпреступностью, увеличило уровень финансового мошенничества в Интернете. Поскольку багаж знаний, необходимых для взлома, становится меньше, необходимо повысить уровень осведомленности в области информационной безопасности, при этом государство тоже должно своевременно реагировать на угрозы информационной безопасности соответствующим уголовно-процессуальными и политико-правовыми механизмами, так как угрозы информационной безопасности могут быть как внутренними, так и

внешними источниками.

Термин «политические механизмы» активно используется в научной, публицистической и политической литературе. Несмотря на это, с точки зрения научного подхода, определение раскрыто недостаточно. В связи с этим рассмотрение понятия «политические механизмы по обеспечению информационной безопасности государства» предполагает уточнение этого термина.

Также, 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.

Термин «механизм» обычно применяется в значении «системы, устройства, определяющего порядок какого-либо вида деятельности» [82, с.123]. Значит «механизм» можно определить как организованную последовательность целенаправленных действий, которые взаимосвязаны между собой и не противоречат друг другу, осуществляемых в определенном порядке определенными субъектами. Отличием политического механизма является то, что он опирается на государственную власть и законодательную базу государства [99, с.300].

И само собой, термин «политический» означает «относящийся к политике», т.е. к деятельности органов государственной власти и государственного управления [82, с.389]. При этом политические механизмы должны быть использованы для защиты интересов государства [50, с.103].

Поэтому важно не столько принятие отдельных решений (законов,

регламентов, программ), находящихся на данном этапе, сколько механизмы создания оригинальных решений, которые позволят жить в ритме технического прогресса.

Под механизмом обеспечения информационной безопасности, как правило, понимается «система, определяющая порядок деятельности законодательной, исполнительной и судебной властей, государственных, общественных и иных организаций и объединений граждан по обеспечению безопасности в информационной сфере», либо «единство организационно-оформленных государством специальных органов, которые в соответствии с интересами человека, общества и государства решают задачи обеспечения безопасности страны в информационной сфере, и в этих целях осуществляют в строго определенных формах государственное руководство и практически реализуют в своей деятельности функции обеспечения информационной безопасности» [146,с.67].

Значит, механизм обеспечения информационной безопасности - это координированный шаг системы специальных органов государственной власти, непосредственно реализующих и проводящих мониторинг политики для обеспечения информационной безопасности государства посредством выполнения своих функций. Политико-правовые нормы призваны определить компетенции, круг задач и обязанностей каждого из государственных органов и структур в сфере обеспечения информационной безопасности.

В связи с этим механизм по обеспечению информационной безопасности представляет собой государственно-правовой механизм реализации политики в области обеспечения информационной безопасности.

Эффективность управления в любом государстве, в том числе и в КР, в немалой степени зависит от информационного обеспечения государственных структур и ведомств. В процессе информационно-коммуникативного воздействия в общественном сознании создается образ

государственной власти, государственных ведомств и структур, людей у власти.

С позиций обеспечения национальной безопасности Кыргызстана и сохранения независимости современная международная обстановка связана с наибольшим риском в отношении реальных источников угроз, приемов и способов дестабилизации в обществе. Новые зародившиеся признаки разного вида насилия, говорят о том, что новые технологии могут категорично поменять формы противостояния между государствами. Эти виды насилия могут изменить базу межгосударственных конфликтов и концепция национальной безопасности страны не станет отвечать реалиям времени. Поэтому возникает объективная необходимость в разработке политико-правовых механизмов по поддержанию информационной безопасности общества. При этом, как уже отмечалось выше, наряду с разработкой политико-правовых механизмов внутри страны, есть необходимость в информационной безопасности современных международных отношений, так как, как уже отмечалось выше, современный уровень развития ИКТ «стирает» государственные границы в интернет пространстве. В этом есть и позитивные стороны, так как государственная политика требует информационного обеспечения. Следовательно, вопросы интеграции отечественной информационной сферы в мировое информационное пространство, как и процесс создания условий информационной безопасности Кыргызстана, должны быть системно отражены в едином документе, определяющем государственную программу реализации информационной политики республики, которая комплексно охватывает все направления развития информационной сферы.

Назрела объективная необходимость создания комплексной, единой и целостной политики, которая должна охватывать все составляющие системы развития и формирования информационной среды.

Так, например, правительство Франции в принятой программе действий по подготовке вхождения страны в информационное общество указывает, что управление главными инфраструктурами и основными обменными сетями в государстве и на международном уровне основывается на сложных и разработанных информационных системах, которые с развитием и растущей взаимосвязью корпоративных и правительственных информационных сетей все больше подвергаются потенциальной уязвимости. Таким образом, наряду с традиционными угрозами высокоточным инфраструктурам, французское общество сталкивается с новыми потенциальными опасностями: «виртуальное» нападение на государственные и частные финансовые информационные системы компьютерными вирусами, или саботаж основной компьютерной системы, которые могут иметь даже более серьезные последствия, чем «обычное» нападение.

Далее указывается, что глобальное измерение информации требует увеличенную международную координацию. Поэтому правительство ставит задачу более активного международного участия в области предотвращения новых угроз, связанных с информационными и коммуникационными технологиями. Эта работа реализуется в рамках:

- Европейского Союза (защита несовершеннолетних и человеческого достоинства; проект европейского соглашения о взаимной судебной помощи);
- Совета Европы (реализация международного соглашения по преступности в киберпространстве);
- планов действий, принимаемых Министрами Внутренних дел и Юстиции стран G7 и нацеленных на укрепление технических возможностей, улучшение взаимной судебной помощи и гармонизации законодательства относительно информационных сетей для защиты граждан.

Далее, Правительство Японии в целях диверсификации глобальных социально-экономических изменений, вызванных бурным развитием информационных технологий, в числе главных приоритетов государственной информационной политики выделяет:

- осуществление всемирного ведущего сетевого пользовательского окружения;

- осуществление гибкого, динамического инфо-коммуникационного сетевого окружения, что позволяет использование инфо-коммуникаций любым гражданином;

- дальнейшее укрепление международных связей и сотрудничества, и внесение вклада в развитие инфо-коммуникации в глобальном масштабе.

При этом, особое внимание уделяется проблемам, сопутствующим прогрессу в информационной сфере и негативно влияющим на функционирование политических и демократических институтов японского общества: цифровое разделение и уязвимость.

Японское правительство проявляет озабоченность относительно увеличения цифрового разделения, как внутри страны, так и между странами и регионами, где первенство держат наиболее развитые страны. По данным проведенных исследований - различия наблюдаются в распространении Интернета и его использования в зависимости от относительного богатства наций. Кроме того, состояние средств обслуживания телекоммуникационных сетей, от которых зависит использование Интернета, является различным между продвинутыми нациями и развивающимися странами. Неутешительный вывод, к которому пришли японские исследователи, заключается в том, что прогресс глобальной социально-экономической революции не только увеличивает потенциальную опасность социального хаоса посредством разрушения правительственных и гражданских информационных сетей, но и расширит цифровое разделение между странами в северных и южных полушариях,

также как и внутри страны в развивающихся странах. Иными словами, социально-экономические различия между развитыми нациями и развивающимися странами не могут быть стерты. Поддержание равных возможностей для развивающихся стран недостаточно. Все развитые нации, включая Японию, должны взять на себя обязанность уничтожить цифровое разделение в развивающихся странах, поддерживая средства обслуживания инфраструктуры информационных технологий и образование человеческих ресурсов в области информационных технологий.

Обзор национальных стратегий некоторых ведущих стран мира в области формирования, развития и дальнейшего совершенствования информационной политики вхождения в информационное общество показывает насущность и объективность системного подхода к регулированию общественных процессов в информационном пространстве.

Для Кыргызстана, учитывая современный уровень формирования национальной информационной сферы, наиболее вероятностным решением является использование опыта России. Это обусловлено не только историческими, культурными традициями, но и геополитической необходимостью развития надежных партнерских отношений в рамках созданных и, на наш взгляд, успешно действующих международных механизмов на постсоветском пространстве.

Сегодня Российская Федерация объективно опережает Кыргызстан не только в области развития национальной информационной инфраструктуры и инфосферы, но и государственного регулирования этими процессами. Так, государственная информационная политика России определяет не только цели, задачи и объекты, но и основные направления и механизмы ее реализации.

Особо обращает на себя внимание то, что формирование информационного общества правительством России концептуально и практически рассматривается как этап формирования мирового

информационного пространства. Из стран бывшего СССР, Российская Федерация обладает хорошо развитой информационно-телекоммуникационной инфраструктурой. Благодаря этому РФ может претендовать на занятие ключевой ниши в мировом информационном пространстве. Достижение этой цели реализуется посредством выполнения следующих основных мер [60, с.98]:

- последовательное реформирование информационного производства;
- практическое овладение населением страны информационными ресурсами, развитой информационно-телекоммуникационной инфраструктуры и новейших информационных технологий в различных видах деятельности;
- приобретение внушительного показателя информационной безопасности;
- обеспечение РФ статуса на международном уровне как полноправного, полновесного участника мирового информационного сообщества.

В отличие от России, Кыргызстан пока не определился с собственной стратегией государственной информационной политики, которая должна отражать множество интересов граждан, общественных организаций и движений, местных органов власти, государственных организаций и коммерческих структур; учитывать уровни социально-экономического, научно-технического и культурного развития регионов государства. На наш взгляд, в структурно-содержательном плане реализация государственной информационной политики страны в условиях интеграции страны в Глобальное информационное общество должна учитывать следующие базовые векторы деятельности:

- информационного суверенитета через вопросы по обеспечению информационной безопасности при помощи усиленного со причастия в

международно-политических механизмах обеспечения международной безопасности в региональном и универсальном масштабах;

- содействие развитию институтов гражданского демократического общества, в том числе дальнейшая интенсификация программ по развитию электронного правительства, обеспечение свободного развития средств массовой информации;

- координация основных информационных потоков;

- развитие информационного законодательства, в том числе обеспечение конституционных прав и гарантий граждан и общества на свободу слова, распространение и получение информации.

В рамках осуществления государственной информационной политики Кыргызстана, особое место занимает международное сотрудничество республики в контексте вопросов по обеспечению информационной безопасности субъектов информационного взаимодействия. Парадигма современного социально-экономического прогресса заключается в интеграции стран мира на основе концепции открытых систем в единое общемировое информационное сообщество, где каждая страна в зависимости от уровня развития собственной информационной сферы займет определенное место в Глобальном информационном обществе. Опережающее развитие транснациональных экономических структур, информационных и телекоммуникационных систем является переходным этапом от индустриального общественного развития к информационной тенденции формирования экономики и общества. Глобальные информационные системы уже связали мир в единую систему. Глобальные информационные системы делают все государства информационно взаимозависимыми и заставляют проявлять множество внимания к качеству информационного взаимодействия во всех сферах жизнедеятельности социума. С этой точки зрения, международное сотрудничество Кыргызстана в области обеспечения информационной

безопасности представляет собой часть военного, политического, культурного, экономического взаимодействия государств-членов мирового сообщества.

Немаловажен также и поток информации о деятельности органов власти. Конституция КР гарантирует, что граждане имеют право на доступ к информации, находящейся в ведении государственных органов (естественно, к той категории, которая не относится к секретной). При информировании населения, информация от государственных органов должна отвечать целому ряду требований:

1. информация должна быть точной и адекватной (доступность)

2. информация должна быть полной (сохранение целостности информации).

3. информация должна быть не опасной для государства (конфиденциальность)

Поскольку информированность означает обладание информацией, предполагающей принятие решений и последующие действия, то эта информация должна содержать и данные о тех предметах деятельности власти, которые оказывают свое влияние на сферы их материальной и духовной жизни.

В настоящее время, самым важным требованием для Кыргызстана считается создание национальной концепции информационной безопасности, которая должна стать фундаментальным концептуальным документом. Этот документ должен рассматривать границы и условия обеспечения информационной безопасности и свободы, который служит для разработки задач преодоления негативных тенденций в информационной сфере современного кыргызстанского общества. Выработка Концепции информационной безопасности является жизненно необходимым. Как было сказано выше, нужны специалисты по социологии, политологии для анализа знаний и отношения общества о проблемах и

вообще наличии информационных угроз. На основе анализа этих данных можно было бы разработать рекомендации для повышения грамотности населения в вопросах информационной безопасности, а также технических заданий для IT специалистов, которые будут разрабатывать программное обеспечение для сбора, хранения, обработки, передачи и распространения информации. Необходимо также на регулярной основе проводить оценку информационного воздействия и механизмов противодействия рискам. Недостаток грамотных кадров приведет к дальнейшему усугублению информационной опасности.

В современном мире все идет онлайн. Развитие технологии привносит каждый аспект жизни в интернете, включая правительство. Использование технологий, особенно интернет-приложений в интернете для повышения доступности и предоставления государственной и правительственной информации для обслуживания гражданам, деловым партнерам, сотрудникам, другим учреждениям и государственным структурам, определяется как электронное правительство.

Как видно из определения, государственные услуги ориентированы не только на граждан, но также на предприятия, агентства и т. д. Согласно определениям, данным электронному правительству в западной литературе, категории электронного правительства включают:

1. Государство, предоставляющее услуги физическим лицам (G2IS - Government Delivering Services to Individuals);
2. Государство для отдельных лиц как часть политического процесса (G2IP - Government to Individuals as a Part of the Political Process);
3. Государство для бизнеса как гражданина (G2BC - Government to Business as a Citizen);
4. Государство для бизнеса на рынке (G2BMKT - Government to Business in the Marketplace);
5. Государство для сотрудников (G2E - Government to Employees);

6. Государство для государства (G2G - Government to Government)

При таком разнообразии онлайн-сервисов возникает необходимость в стандартизации, для чего были разработаны некоторые требования. В научной литературе было предложено сгруппировать факторы, влияющие на качество порталов электронного правительства на шесть основных категорий: (1) Безопасность и конфиденциальность; (2) Юзабилити; (3) Контент; (4) Услуги; (5) Участие граждан; и (6) Особенности.

Как видно, на первом месте находятся вопросы обеспечения информационной безопасности, особенно структур, работающих со специальной информацией с уровнями доступа «секретно» и выше, такие как специализированные научно-исследовательские организации, Министерства обороны и внутренних дел, иностранных дел Кыргызстана и т.д. Безопасность является решающим моментом при разработке электронного правительства. Государственные инфраструктуры должны поддерживать аутентификацию, конфиденциальность и целостность, инфраструктуру открытых ключей (PKI), следует использовать для разработки модели доверия. Кроме того, есть проблемы, связанные с разработкой программных продуктов государственного значения. Плохая практика кодирования может сделать государственные информационные порталы уязвимыми для таких атак, как SQL-инъекция и межсайтовый скриптинг, что может привести к сбою службы, потере данных или полной остановке информационных служб и порталов. На правительственных и государственных информационных службах и порталах последствия таких атак могут быть катастрофическими.

Поэтому, автор еще раз хотел бы подчеркнуть важность нормативного правового механизма обеспечения информационной безопасности, которые должны отвечать реалиям существующих информационных угроз и служить административным сводом правил при разработке ИКТ для государства.

Все вышеперечисленное обязывает разработать и реализовать комплекс мер и средств защиты информации от несанкционированного доступа и на микроуровне. С этой целью необходимо, прежде всего, создать службу информационной безопасности, т.е. назначить должностных лиц, которые будут ответственны за организацию и осуществление практических мероприятий по обеспечению безопасности информации и процессов ее обработки. Служба информационной безопасности должна быть самостоятельным подразделением и подчиняться напрямую первому лицу организации.

Государственные ведомства, ответственные за обеспечение информационной безопасности, по мнению автора исследования, должны обеспечивать эффективное решение следующих задач:

• Защиту от вмешательства в процесс сбора и обработки статистических и иных, являющихся стратегически важными для государства, данных посторонних лиц, допуск к ее ресурсам должны иметь те лица, которые прошли регистрацию в установленным порядке;

• Разграничение обязанностей разработчиков аппаратного, программного и информационного ресурсов, т.е. нельзя поручать разработку одного модуля от начала до конца одному сотруднику без контроля программного продукта, так как возможно создание непреднамеренных или преднамеренных ошибок кода, которые бы сделали возможным несанкционированный доступ к аппаратным, программным и криптографическим средствам защиты;

• аудит и мониторинг – то есть регистрацию всех действий пользователей при использовании защищаемых ресурсов информационной системы в системных журналах и периодический контроль действий пользователей системы путем мониторинга содержимого этих журналов специалистами подразделений безопасности;

• контроль целостности (неизменности) как данных, хранящихся в

системе, так и среды исполнения программ;

• защита системы от внедрения несанкционированных кодов, компьютерных вирусов и программ-шпионов;

• обязательная идентификация, аутентификация и проверка авторизации пользователей (и получателей, и отправителей информации), участвующих в информационном обмене;

• обязательное создание так называемых «точек возврата» - копий систем для восстановления системы в случае нарушения целостности системы;

• соответствующее моменту выявление источников вызовов безопасности информации, причин и условий, которые способствуют нанесению ущерба заинтересованным субъектам информационных отношений, создание методов и приемов оперативного реагирования на негативные тенденции и угрозы безопасности информации.

Также к вышеперечисленным задачам обычно причисляют и обеспечение живучести криптографических средств защиты информации, однако в КР использование средств криптографической защиты находится в зародышевом состоянии, так как нет законодательной базы по использованию данных средств. Стандартами шифрования в республике приняты только те алгоритмы, которые прошли ГОСТ РФ.

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.

Подытоживая настоящий параграф, 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;

Следовательно, постановка задач информационного обеспечения внутренней и внешней политики Кыргызстана на высшем государственном уровне требует существенно усилить механизм ее реализации. Под такой механизм целесообразно создать государственный орган и поручить ему разработку общего замысла информационного обеспечения внутренней и внешней политики, планирование и координацию практической деятельности, подбор журналистов и экспертов, которые будут на постоянной основе выполнять эту функцию.

Вывод проблемы информационной безопасности на уровень государственной политики конечно, должен привлекать в их решение государственную власть и ресурсы политических сил кыргызстанского общества. Такой подход будет отражать интересы политических организаций, политических элит, государства и, в конечном счете - граждан КР.

ЗАКЛЮЧЕНИЕ

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 от внешних и внутренних угроз 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 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); необходимо, чтобы соблюдался баланс между правом граждан, общества и государства на свободный обмен информацией и необходимым ограничением на ее распространение; 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.

СПИСОК ИСПОЛЬЗОВАННОЙ ЛИТЕРАТУРЫ

Нормативно-правовые акты

1. Конституция Кыргызской Республики [Текст]: принята референдумом всенародным голосованием 27 июня 2010 г. // Эркин-Тоо. – 2010. – 6 июля. (В редакции Закона КР от 28 декабря 2016 года № 218)
2. Конституция Кыргызской Республики [Текст]: от 5 мая 1993 года № 1 185-XII // Слово Кыргызстана. – 1993. – 21 мая.
3. Гражданский кодекс Кыргызской Республики [Текст]: от 8 мая 1996 г. № 15 // Эркин-Тоо. – 1996. – 5 июня.
4. Уголовный кодекс Кыргызской Республики [Текст]: от 1 окт. 1997 г. № 68 // Эркин–Тоо. – 1997. – 24 окт.; Слово Кыргызстана. – 1997. – 14 окт.; Ведомости Жогорку Кенеша Кырг. Респ. – 1998. – № 7. – С. 229.
5. О национальной безопасности [Текст]: закон КР от 26 февр. 2003 г. № 44 // Эркин-тоо. – 2003. – 4 марта.
6. Об информатизации [Текст]: закон КР от 8 окт. 1999 г. № 107 // Эркин-Тоо. – 1999. – 6 нояб.
7. О защите государственных секретов Кыргызской Республики» [Текст]: закон КР от 14 апр. 1994 г. №1476-XII // Ведомости Жогорку Кенеша Кырг. Респ. – 1994. – №5. – С. 153.
8. О гарантиях и свободе доступа к информации [Текст]: закон КР от 5 дек. 1997 г. № 89 // Эркин-Тоо. – 1997. – 19 дек.
9. Об электронной цифровой подписи [Текст]: закон КР от 17 июля 2004 г. №92 // Эркин –Тоо. – 2004. – 30 июля.
10. О средствах массовой информации [Текст]: закон КР от 2 июля 1992 г. №938-XII // Эркин-Тоо. – 1992. – 4 авг.
11. О правовой охране программ для ЭВМ и баз данных [Текст]: закон КР от 30 марта 1998 г. №28 // Эркин – Тоо. – 1998. – 4 апр.

12. О доступе информации, находящиеся в ведении государственных органов и органов местного самоуправления Кыргызской Республики [Текст]: закон КР от 28 дек. 2006 г. № 6 // Эркин –Тоо. – 2007. – 23 янв.
13. Об авторском праве и смежных правах [Текст]: закон КР от 14 янв. 1998 г. № 6 // Эркин-Тоо. – 1998. – 23 янв.; Наша газ. – 1998. – 28 янв.
14. Об информации персонального характера [Текст]: закон КР от 14 апр. 2008 г. №58 // Эркин-Тоо. – 2008. – 18 апр.
15. Об электрической и почтовой связи [Текст]: закон КР от 2 апр. 1998 г. № 31 // Норматив. акты Кырг. Респ. – 1998. – №8. – С. 3-18.
16. О системе научно-технической информации [Текст]: закон КР от 8 окт. 1999 г. № 108 // Эркин-Тоо. – 1999. – 20 окт.
17. О министерстве культуры, информации и туризма КР [Текст]: положение утверждённого Постановлением Правительства КР от 03.05.2013 г. №236. // Норматив. акты Кырг. Респ. – 2013.

Специальная литература

18. Абилдаев, Э.Е. Политическая система Кыргызстана: проблемы и перспективы [Текст] / Э.Е.Абилдаев. – Бишкек: Илим, 2001. – 320 с.
19. Абдеев, Р.Ф. Философия информационной цивилизации [Текст] / Р.Ф.Абдеев. – М.: ВЛАДОС, 1994. – 162 с.
20. Акунов, А.А. Права человека и демократия [Текст]: учеб. пособие / А.А.Акунов, Т.О.Ожукеева, В.Г.Прытков. – Бишкек: Б.и., 1996. – 163 с.
21. Акунов, А.А. Государственное управление Кыргызстана в транзитный период [Текст] / А.А.Акунов. – Бишкек: КГНУ, 1999. – 268 с.

22. Арабаев, Ч.И. Гражданское право Кыргызской Республики [Текст]: учеб. / Ч.И.Арабаев. – Бишкек: Просвещение, 2004. – Ч.1. – 400 с.
23. АРИСТОТЕЛЬ. Сочинения [Текст]: в 4 т.: пер. с древнегреч. / общ. ред. А. И. Доватура. – М.: Мысль, 1983. – Т.4. – 830 с.
24. Артыкбаев, М.Т. Политическая система в «открытых» и «закрытых обществах» (сравнительный анализ) [Текст] / М.Т.Артыкбаев, А.М. Артыкбаев.– Бишкек: КГНУ, 1998. – 121с.
25. Артыкбаев, М.Т. Институализация политических систем постсоветских республик [Текст]: методы исслед. / М.Т.Артыкбаев. – Бишкек: Б.и., 2002. – 1134 с.
26. Асанканов, А.А. Кыргызы: рост национального самосознания [Текст] / А.А.Асанканов. – Бишкек: Б.и., 1991. – 225 с.
27. Асмус, В.Ф. Античная философия [Текст]: учеб. / В.Ф.Асмус. – М.: Б.и., 2003. – 345с.
28. Батурин, Ю.М. Проблемы компьютерного права [Текст] / Ю.М.Батурин. – М.: Юрид. лит., 1991. – 271 с.
29. Бектурганов, К.Б. Общественное мнение как социальный институт [Текст]: учеб. пособие / К.Б.Бектурганов, Б.К.Бектурганова. – Бишкек: Maxprint, 2009. – 252 с.
30. Большая Советская Энциклопедия [Текст] / гл. ред. С.И. Вавилов. – 2-е изд. – М.: Гос. науч. изд-во БСЭ, 1950. – Т.4. – 644 с.
31. Бокошев, Ж.Б. Проблемы национальной безопасности Кыргызстана [Текст] / Ж.Б.Бокошев. – Бишкек: Ин-т соц.-полит. технологий, 2006. – 124 с.
32. Модели и механизмы управления безопасностью [Текст] / В.Н.Бурков, Е.В. Грацианский, С.И. Дзюбко, А.В. Щепкин. – М.: СИНТЕГ, 2001. – 160 с.

33. Бубнов, А.В. Информационная безопасность России в условиях глобализации [Текст]: автореф. дис. … канд. полит. наук: 23.00.02 / А.В.Бубнов. – М., 2009. – 23с.
34. Винер, Н. Кибернетика или управление и связь в животном и машине [Текст] / Н.Винер. – М.: Прогресс, 1966. – 245 с.
35. Гаджиев, К.С. Политическая наука [Текст] / К.С.Гаджиев. – М.: Наука, 2010. – 116 с.
36. Гаджиев, К.С. Геополитика [Текст]: учеб. для бакалавров: учеб. для студентов высш. учеб. заведений, обучающихся по специальностям и направлениям: "Политология", "Междунар. отношения", "Юриспруденция", "История", "Социология" / К. С. Гаджиев. – М.: Юрайт, 2013. – 350 с.
37. Гаджиев, К.С. Политическая наука. Средства массовой информации и политика [Текст] / К.С.Гаджиев. – М.: Наука, 1995. – 98 с.
38. Глобальная информатизация и безопасность России [Текст] / под общ. ред. В.И. Добренькова. – М.: Изд-во Моск. ун-та, 2001. – 398 с.
39. Грачев, Г. В. Манипулирование личностью [Текст] / Г.В.Грачев, И.К.Мельник. – М.: Изд-во «Эксмо», 2003. – 197 с.
40. Гриняев, С.Н. Интеллектуальное противодействие информационному оружию [Текст] / С.Н.Гриняев. – М.: СИНТЕГ, 1999. – 232с.
41. Даль, В. Толковый словарь живого великорусского языка [Текст]: в 4 т. / В.Даль. – М.: ТЕРРА, 1995. – Т. 1. – 800 с.
42. Джекшенкулов, А. Новые независимые государства в мировом сообществе [Текст] / А.Джекшенкулов. – М.: Науч. кн., 2000. – 306 с.
43. Дзлиев, М. И. Проблемы безопасности: теоретико-методологические аспекты [Текст] / М.И.Дзлиев, А. Л. Романович, А.Д.Урсул. – М.: Ступени, 2001. – 340 с.

44. Доватур, А.И. "«Политика» Аристотеля". Аристотель. Политика [Текст] / А.И.Доватур. – М.: Наука, 2002. – 207 с.
45. Дононбаев, А.Д. Кыргызстан. Политическая культура. Человек и государство [Текст] / А.Д.Дононбаев. – Бишкек: КРСУ, 2002. – 45с.
46. Досалиева, Б.А. СМИ в Кыргызстане: политико-правовой аспект [Текст]: дис. … канд. полит. наук: 23.00.02 / Б.А. Досалиева. – Бишкек, 2010. – 66с.
47. Дугин, А. Г. Теория многополярного мира [Текст] / А.Г.Дугин. – М.: Евраз. движение, 2013. – 318 с.
48. Европейское право [Текст]: учеб. для вузов / под общ. ред. Л.М. Энтина. – М.: Изд–во НОРМА, 2000. – 720 с.
49. Елепов, Б.С. Управление процессами использования информационных ресурсов [Текст] / Б.С.Елепов, В.М.Чистяков. – Новосибирск: Наука. Сиб. отд-ние, 1989. – 238 с.
50. Иванский, В.П. Правовая защита информации о частной жизни граждан. Опыт современного правового регулирования [Текст]: моногр. / В.П.Иванский. – М.: Изд-во РУДН, 1999. – 276 с.
51. Иманалиев, К.К. Национальная идея как фактор политической консолидации общества переходного периода: на примере России и Кыргызстана [Текст]: дис. … канд. полит. наук: 23.00. 02 / К.К. Иманалиев. – М., 2002. – 120 с.
52. Какеев, А.Ч. Современный Кыргызстан к открытому обществу [Текст] / А.Ч. Какеев. – Бишкек: Б.и., 1995. – 195 с.
53. Кафтанчиков, Д. П. Информационная безопасность Российской Федерации: современное состояние и приоритеты обеспечения [Текст]: автореф. дис. ... канд. полит. наук / Д.П.Кафтанчиков. – Орел, 2009. – 25 с.
54. Ковалева, Е. В. Обеспечение транспарентности органов местного самоуправления современной России в процессе информатизации

политического управления [Текст]: автореф. дис. ... канд. полит. наук / Е.В.Ковалева. – Саратов, 2010. – 22 с.

55. Концепция национальной безопасности Кыргызской Республики [Текст]: от 1 июня 2012 г. // Слово Кыргызстана. – 2012. – 20 июня.
56. Концепция информационной безопасности РК до 2016 года
57. Копылов, В.А. Информационное право [Текст]: учеб. пособие / В.А. Копылов. – М.: Юристъ, 1997. – 472 с.
58. Краткий словарь специальных терминов [Текст]. – М.: Республика, 1994. – 509 с.
59. Крылов, Г. О. Международный опыт правового регулирования информационной безопасности и его применение в Российской Федерации [Текст]: автореф. дис. ... канд. юрид. наук / Г.О.Крылов. – М., 2007. – 23 с.
60. Куняев, Н. Н. Правовое обеспечение национальных интересов Российской Федерации в информационной сфере [Текст] / Н.Н. Куняев. – М.: Логос, 2010. – 367 с.
61. Кураков, Л.П. Информация как объект правовой защиты [Текст] / Л.П.Кураков, С.Н.Смирнов. – М.: Гелиос, 1998. – 18 с.
62. Куликовский, А.В. Специфика развития информационных агенств в Кыргызской Республике [Текст]: дис. … канд. филол. наук / А,В.Куликовский. – Душанбе, 2013. – 126 с.
63. Курушин, В.Д. Компьютерные преступления и информационная безопасность [Текст] / В.Д.Курушин, В.А.Минаев. – М.: Новый юрист, 1998. – 256 с.
64. Ногойбаева, Э.А. Кыргызстан. Политика и экономика [Текст]: материалы и док. / Э.А. Ногойбаева, А.Д. Мурзакулова, Б.С. Жумагулов // МИСИ при президенте КР. – Бишкек, 2006. – Вып.3. – С. 3- 450.

65. Лисичкин, В. А. Третья мировая информационно-психологическая война [Текст] / В.А.Лисичкин, Л.А.Шелепин. – М.: Ин-т социально-полит. исслед. АСН, 2000. – 460 с.
66. Липпман, У. Общественное мнение [Текст] / У.Липпман; пер. с англ. Т. В. Барчунова; под ред. К. А. Левинсон, К. В. Петренко. – М.: Ин-т Фонда «Общественное мнение», 2004. – 384 с.
67. Липпман, У. Публичная философия [Текст] / У.Липпман. – М.: Идея-пресс, 2004.- 160 с.
68. Лосев, А.Ф. «Жизненный и творческий путь Платона» [Текст] / А.Ф.Лосев // Платон. Собр. Соч.: в 4 т. – М., 1990. – Т.1. – С. 3-63.
69. Макиавелли, Н. Государь [Текст] / Н.Макиавелли. - М.: Планета, 1990. - 80с.
70. Манойло, А.В. Государственная информационная политика в особых условиях [Текст]: моногр. / А.В.Манойло. – М.: МИФИ, 2003. – 388 с.
71. Маслов, В.И. Региональная безопасность: история и проблемы новых независимых государств Центральной Азии [Текст] / В.И.Маслов. – Бишкек: Илим, 2000. – 196 с.
72. Матвеев, Р.Ф. Теоретическая и практическая политология [Текст] / Р.Ф.Матвеев. – М.: РОССПЭН, 1993. – 240 с.
73. Международное право [Текст]: учеб. / отв. ред.: Ю.М. Колосов, Э.С. Кривчикова. – М.: Междунар. отношения, 2000. – 720 с.
74. Мелюхин, И.С. Информационное общество: истоки, проблемы, тенденция развития [Текст] / И.С.Мелюхин. – М.: Изд-во МГУ, 1999. – 208 с.
75. Молдалиев, О.А. Современные вызовы безопасности Кыргызстана и Центральной Азии. Фонд имени Фридриха Эберта [Текст] / О.А.Молдалиев. – Бишкек: Б.и., 2001. – 140 с.

76. Мухаев, Р.Т. Политология [Текст]: учеб. для вузов / Р.Т.Мухаев. – М.: Приор-издат, 2005. – 432 с.
77. Основы политологии [Текст]: курс лекций / под. ред. А.П.Плешакова.– М.: Высш. образование, 2007. – 691 с.
78. Нартов, Н.А. Геополитика [Текст]: учеб. для студентов вузов, обучающихся по спец. «Гос. и муницип. упр.», «Междунар. отношения», «Регионоведение» / Н.А. Нартов, В.Н. Нартов; под ред. В.И. Староверова. – 4-е изд., перераб. и доп. – М.: ЮНИТИ-ДАНА: Единство, 2007. – 327 с.
79. Наумов, А.В. Российское уголовное право [Текст]: общ. ч. / А.В.Наумов. – М.: Изд-во БЕК, 1996. – 560 с.
80. Никуличев, Ю.В. Содружество Независимых Государств [Текст]: очерк соврем. истории / Ю.В.Никуличев. – М.: Б.и., 2002. – 89 с.
81. Общая теория национальной безопасности [Текст]: учеб. / под общ. ред. А.А. Прохожева. – М.: Изд-во РАГС, 2002. – 320 с.
82. Ожегов, С. И. Словарь русского языка [Текст] / С.И.Ожегов. – 19-е изд., испр. – М.: Рус. яз., 1987. – 800 с.
83. Орунбеков, Б. Болунгон кыргыз [Текст] / Б.Орунбеков. – Бишкек: Б-сыз, 2014. – 105 б.
84. Панарин, А.С. Политология [Текст]: учеб. / А.С.Панарин. – М.: Проспект, 1997.– 407 с.
85. Панарин, И. Н. Информационная война и мир [Текст] / И.Н.Панарин, Л.Г.Панарина. – М.: Изд-во «ОЛМА-ПРЕСС», 2003. – 240 с.
86. Панарин, Й.Н. Информационно-психологическое обеспечение национальной безопасности России [Текст]: дис. … д-ра полит.наук / И.Н.Панарин. – М., 1998. – 206 с.
87. Петров, В. П. Бездуховность делает человека опасным [Текст] / В.П.Петров // Основы безопасности жизнедеятельности. – 2007. – №2. – С.52-56.

88. Платон. Собрание сочинений [Текст]: в 4 т. / Платон. – М.: Мысль, 1990. – Т.1. – 830 с.
89. Политология [Текст]: энцикл. слов. / общ. ред. и сост. Ю.И. Аверьянов. – М.: Науч. кн., 2006. – 246 с.
90. Почепцов, Г.Г. Информационные войны [Текст] / Г.Г.Почепцов. – М.: Реф-бук, Ваклер, 2000. – 273 с.
91. Приходько, А.Я. Информационная безопасность в событиях и фактах [Текст] / А.Я.Приходько. – М.: СИНТЕГ, 2001. – 260 с.
92. Приходько, А.Я. Словарь-справочник по информационной безопасности [Текст] / А.Я. Приходько. – М.: СИНТЕГ, 2001. – 124 с.
93. Прокофьев, В.Ф. Тайное оружие информационной войны [Текст] / В.Ф.Прокофьев. – М.: СИНТЕГ, 1999. – 152с.
94. Прохожев, А.А. Национальная безопасность: к единому пониманию сути и терминов. Безопасность [Текст] / А.А.Прохожев. – М.: РАГС, 1995. – 125 с.
95. Прохожев, А.А. Национальная безопасность: основы теории, сущность, проблемы [Текст] / А.А.Прохожев. – М.: РАГС, 1997. – 67 с.
96. Прохожев, А.А. Человек и общество: законы социального развития и безопасности [Текст] / А.А.Прохожев. – М.: РАГС, 2002. – 199 с.
97. Прохожев, А.А. Информационная безопасность – важнейшая составляющая национальной безопасности современной России [Текст] / А.А.Прохожев. – М.: РАГС, 1996. - 17 с.
98. Прохоренко, И.Л. Национальная безопасность и баланс сил [Текст] / И.Л.Прохоренко // Баланс сил в мировой политике: теория и практика. – М., 1993. – С.70.
99. Пугачев, В.П. Введение в политологию [Текст] / В.П.Пугачев, А.И.Соловьев. – М.: Аспект Пресс, 2007. – 477 с.

100. Ракитов, А.И. Философия компьютерной революции [Текст] / А.И.Ракитов. – М.: Политиздат, 1991. – 287 с.

101. Расторгуев, С.П. Философия информационной войны [Текст] / С.П.Расторгуев. – М.: Вуз. кн., 2001. – 468 с.

102. Сааданбеков, Ж. Сумерки авторитаризма: закат или расцвет? [Текст] / Ж. Сааданбеков. – Киев: Ника-Центр, 2000. – 541 с.

103. Саркисян, А.Е. Армяне-военные ученые, конструкторы, производственники и испытатели XX века [Текст] / А.Е.Саркисян.- Ереван: Гитутюн, 1988. – 360 с.

104. Соколова, И.В. Социальная информатика и социология: проблемы и перспективы взаимосвязи [Текст] / И.В.Соколова.– М.: Владос, 2003. – 215 с.

105. Соловьев, А.И. Политология. Политическая теория. Политические технологии [Текст]: учеб. для студентов вузов / А. И. Соловьев. – М.: Аспект Пресс, 2000. – 559 с.

106. Стрельцов, А.А. Обеспечение информационной безопасности России [Текст]: теорет. и методол. основы / А.А.Стрельцов; под ред. В.А. Садовничего и В.П. Шерстюка. – М.: МЦНМО, 2002. – 296 с.

107. Стрельцов, А.А. Информационная безопасность духовной жизни общества [Текст] / А.А.Стрельцов. – М., 2007. – 255 с.

108. Судоргин, О.А. Современная информационная политика государства: мировой опыт и российская практика [Текст]: автореф. дис. … д-ра полит. наук: 23.00.02 / О.А.Судоргин. – М., 2011. – 43 с.

109. Суюнбаев, М.Н. Геополитические основы развития и безопасности Кыргызстана (глобальный, региональный и национальный аспекты) [Текст] / М.Н.Суюнбаев. – Бишкек: ОсОО «Кольби», 2005. – 122 с.

110. Трактат Сунь Цзы [Текст] // Сунь Цзы Цзяоши (Комментарии и толкования трактата Сунь Цзы). – Пекин, 1990. – С. 341 – 375.

111. Темирбаев, А.А. Информационная безопасность Кыргызской Республики [Текст] / А.А.Темирбаев, Р.Н.Сагынбаев. – Бишкек: Б.и., 2007. – 78 с.
112. Томсинов, В.А. Славная революция 1688-1689 годов в Англии и Билль о правах [Текст] / В.А.Томсинов. – М.: Зерцало-М, 2010.(в прил. к кн. на стр. 236 – 250 опубликован полный текст Билля о правах 1689 года на англ. яз. и в пер. автора на рус. яз.).
113. Тоффлер, Э. Третья волна [Текст] / Э.Тоффлер. – М.: АСТ, 2003. – 426 с.
114. Тункин, Г.И. Теория международного права [Текст] / Г.И.Тункин; под общ. ред. Л.Н. Шестакова. – М.: Изд-во «Зерцало», 2000. – 416 с.
115. Уголовное право [Текст]: общ. ч. / под ред. И.Я. Козаченко и З.А. Незнамовой. – М.: Просвещение, 1997. – 285 с.
116. Улуков, Р.Т. Безопасность как политологический феномен развития государства [Текст] / Р.Т.Улуков. - Ош.: Б.и., 2009. - 150 с.
117. Улуков, Р.Т. Безопасность в политической сфере кыргызстанского общества [Текст]: дис. … канд. полит. наук: 23.00.02 / Р.Т.Улуков - Ош, 2008. – 134 с.
118. Устинов, Г.Н. Основы обеспечения информационной безопасности систем и сетей передачи данных [Текст] / Г.Н.Устинов. – М.: СИНТЕГ, 2000. – 248 с.
119. Фобьянчук, А. А. Роль толерантности в процессе глобализации. Человек, культура и общества в изменяющемся мире [Текст]: сб. науч. тр. / А.А. Фобьянчук; науч. ред. Д.Ш. Цырендоржиева.–Улан-Удэ: Изд-во Бурят. гос. ун-та, 2011.– Ч.1.– 200 с.
120. Центральная Азия: геоэкономика, геополитика, безопасность [Текст] / под ред. Р.М.Алимова. – Ташкент: Б.и., 2002. – 208 с.

121. Цыганков, В.Д. Психотронное оружие и безопасность России [Текст] / В.Д.Цыганков, В.Н.Лопатин. – М.: СИНТЕГ, 1999. – 152 с.
122. Цыгичко, В.Н. Информационное оружие как геополитический фактор и инструмент силовой политики [Текст] / В.Н.Цыгичко, Г.Л.Смолян, Д.С.Черешкин. – М.: ИСА РАН, 1997. – 186 с.
123. Черрешкин, Д.С. Проблемы кибербезопасности информационного общества [Текст] / Д.С. Черрешкин. – М.: Б.и., 2006. – 100 с.
124. Шеннон, К.Э. Работы по теории информации и кибернетике [Текст] / К.Э.Шеннон. – М.: Наука, 1963. – 667 с.
125. Элебаева, А.Б. Политическая трансформация. Опыт Кыргызстана в мировом контексте [Текст] / А.Б.Элебаева, М.Ф.Пухова. – Бишкек: Б.и., 2002. – 237 с.
126. Ярочкин, В.И. Секьюритология [Текст] / В.И.Ярочкин. – М.: Ось-89, 2000. – 400 с.

Периодическая литература

127. Агапов, А.Б. Новая информационная технология и право [Текст] / А.Б.Агапов // Сов. государство и право. – 1991. – №11. –С.88-93.
128. Алексенцев, А. И. Сущность и соотношение понятий «защита информации», «безопасность информации», «информационная безопасность» [Текст] / А.И.Алексенцев // Безопасность информационных технологий. – 1999. – № 1. – С.45.
129. Ашкинази, Н. Законы об информационной деятельности: Что есть и что должно быть [Текст] / Н.Ашкинази, М.Гайнер // Правозащитник. – 1996. – №1. – С.59-62.
130. Бельков, О.А. Понятийно-категориальный аппарат концепции национальной безопасности [Текст] / О.А.Бельков // Информ. сб. «Безопасность». - 2004. - №3. - С. 91- 94.

131. Билль о правах [Текст] // Междунар. акты о правах человека: сб. док. – М., 1999. – С.17.
132. Буданцев, Ю. П. Информационное оружие и информационная война в современных условиях [Текст] / Ю.П.Буданцев // Информ. сб. «Безопасность». – 1999. – № 3/4. – С. 48-52.
133. Гайкович, В.Ю. Основы безопасности информационных технологий [Электронный ресурс]. – Режим доступа: http://www.spymarket.com:8000/bibl/p3/p3p/index.html. - Загл. с экрана.
134. Горохов, В.М. Средства массовой информации в системе политических коммуникаций [Текст] / В.М.Горохов // Концепция современной политологии. – М., 1992. – С. 28.
135. Доктрина информационной безопасности Российской Федерации [Текст]: утверждена Президентом РФ 9 сент. 2000 г. № Пр-1895 // Парламент. газ. – 2000. – 30 сент.
136. Доктрина информационной безопасности и методические проблемы теории безопасности [Текст] // Материалы круглого стола «Глобальная информатизация и социально-гуманитар. проблемы человека, культуры, о-ва» / под ред. В.И. Добренькова. – М., 2001. – С. 48-63.
137. Ильин, М.В. Слова и смыслы. По уставу судьбы: исторический выбор, историческая миссия, arcanaimperii, ratiostatus [Текст] / М.В.Ильин // Полис. – 1996. – №3. – С. 40–48.
138. Исаев, К.И. Процесс мировой глобализации и судьба маленького национального государства [Текст] / К.И.Исаев // Соц. и гуманитар. науки. -2004. - № 3/4. – С. 62-65.
139. Керимбекова, Н.К. К вопросу национальной безопасности Кыргызстана и Центральноазиатского региона в условиях суверенной государственности [Текст] / Н.К.Керимбекова // Суверенный

Кыргызстан: проблемы традиций и социальной целостности. – Бишкек, 1999. – С.151-156.

140. Кибернетический терроризм как элемент будущей информационной войны [Текст] // Борьба с преступностью за рубежом. – 1998. – №7. – С. 3-10.

141. Концепция совершенствования правового обеспечения информационной безопасности Российской Федерации [Текст] // Информ. о-во.- 1999. - №6. - С. 4-14.

142. Кретов, Б.И. Средства массовой коммуникации - элемент политической системы общества [Текст] / Б.И.Кретов // Социально-гуманитар. знания. – 2000. – №1. – С.101-115.

143. Кретов, Б.И. Типология лидерства [Текст] / Б.И.Кретов // Социально-гуманитар. знания. – 2000. – №3. – С.73-79.

144. Лепский, В.Е. Становление стратегических субъектов в глобальном информационном обществе: постановка проблемы [Текст] / В.Е.Лепский // Информ. о-во. – 2002. – Вып. 1. – С.58.

145. Лопатин, В.Н. Теоретико-правовые проблемы защиты единого информационного пространства и их отражение в системах российского права и законодательства [Текст] / В.Н.Лопатин // Тр. по интеллектуальной собственности / гл. ред. С.В. Коростелева. – М., 2000. – Т. 2. – С. 71.

146. Манойло, А.В. Государственная информационная политика в особых условиях [Текст] / А.В. Манойло. – М.: МИФИ, 2003. – 187 с.

147. Машлыкин, В.Г. Европейское информационное пространство [Текст] / В.Г. Машлыкин. – М.: Наука, 1999. – 67 с.

148. Маслов, Н.А. Постиндустриальная цивилизация и реформаторское сознание в России [Текст] / Н.А.Маслов // Человек и Реформы в рос. о-ве: мифы и реальность: третья науч. сес.: материалы междунар. науч.-практ. конф. – М., 1995. – С. 112-126.

149. Омаров, Н. Проблемы национальной безопасности Кыргызстана на современном этапе его развития [Текст] / Н.Омаров // Центр. Азия и Кавказ. – 1999. – №3/4. – С.96-102.
150. Пирумов В.С., Родионов М.А. Некоторые аспекты информационной борьбы в военных конфликтах [Текст] В.С. Пирумов , М.А.Родионов // Военная мысль. - 1997. - № 5. С. 34-36.
151. Сейдакматов, Н.А. Информационная составляющая национальной безопасности Кыргызской Республики [Текст] / Н.А.Сейдакматов // Вестн. КРСУ. – 2013. – С. 36-40.
152. Смолян, Г.П. Оружие, которое может быть опаснее ядерного [Текст] / Г.П.Смолян, В.Цыгичко, Д.С.Черешкин // «Независимое военное обозрение». – 1995. – № 3. – С.56-60.
153. Смолян, Г.П. О формировании информационного общества в России [Текст] / Г.П.Смолян, Д.С.Черешкин // Информ. о-во. – 1998. – №1. – С. 9-14.
154. Спиноза, Б. Богословско-политический трактат [Текст] / Б.Спиноза // Антология мировой политической мысли. – М., 1997. – Т. 1. – С. 350.
155. Стоуньер, Т. Информационное богатство: профиль постиндустриальной экономики [Текст] / Т.Стоуньер // Новая технократ. волна на Западе. – М., 1986. – С. 230-258.
156. Стрельцов, А.А. Содержание понятия «Обеспечение информационной безопасности» [Текст] / А.А.Стрельцов // Информ. о-во. – 2001. – №4. – С. 10-16.
157. Судоргин, О. А. Новая роль информационного пространства в XXI веке [Текст] / О. А. Судоргин // Власть. - 2009. - № 1. - С. 27-35.
158. Элебаева, А.Б. Процессы политической модернизации в Кыргызской Республике [Текст] / А.Б.Элебаева // Вестн. КРСУ. – 2013. – Т.13, № 4. – С. 65-68.

Источники на иностранном языке

159. Global information infrastructure – Global information society (GII-GIS). Policy recommendations for action [Электронный ресурс] // http://www.oecd.org/dataoecd/50/8/1912232.pdf.
160. Committee for Information, Computers and Communication policy: Global Information Infrastructure – Global Information Society (GII-GIS). Policy Requirements // http://www.oecd.org/dataoecd/50/7/1912224.pdf
161. Masuda,Y. TheInformation Societyas Postindustrial Society [Text] / Y. Masuda. - Washington: World Future Soc., 1983. – 171 p.
162. Toffler, A. The Third Wave [Text] / A. Toffler. – N.–Y.: Morrow, 1980. – 544 p.
163. Toffler, A., Toffler H. Creating a New Civilization. The Politics of the Third Wave. Turner Publishing, Inc. Atlanta, 1995 [Электронный ресурс] // http://www.freenet.bishkeck.su/ jornal/n5/JORNAL 511.htm
164. The Concise Oxford Dictionary. The New Edition For the 1990s. Oxford, 1990. P. 1093.

Интернет - источники

165. Официальный сайт Президента Кыргызской Республики [Электронный ресурс]. – Режим доступа: http://www.president.kg/ru. - Загл. с экрана.
166. Официальный сайт правительства Кыргызской Республики [Электронный ресурс]. – Режим доступа: http://www.gov.kg/. – Загл. с экрана.
167. Бишев, В.К. Роль информатизации в развитии общества [Электронный ресурс]. – Режим доступа: http://homepages.tversu.ru/~p000114/inform/ch1_1.html.- Загл. с экрана.

168. Бурьяк, А. Национальная безопасность (отрывки) [Электронный ресурс]. - Режим доступа: http://bouriac.narod.ru.- Загл. с экрана.
169. Венская конвенция о праве международных договоров. Вена, 23 мая 1969 [Электронный ресурс]. – Режим доступа: http://www.un.org/russian/documen/convents/lawtreat.pdf.- Загл. с экрана.
170. Всеобъемлющий подход к укреплению международного мира и безопасности в соответствии с Уставом ООН // A/RES/42/93, 1987. – 3 с. [Электронный ресурс]. – Режим доступа: http://www.un.org/documents/ga/res/42/a42r093.htm.-Загл. с экрана.
171. Вус, М.А. К вопросу о становлении концептуальных правовых основ информационной безопасности [Электронный ресурс] // Концептуальные проблемы информ. безопасности в союзе России и Беларуси: сб. докл. и тез. междунар. конф., СПб., 2003 г.- Режим доступа: http://www.jurfak.spb.ru/conference/18102000/vus.htm.- Загл. с экрана.
172. Гаджиев, К.С. Геополитика. - М., 1997 [Электронный ресурс]. – Режим доступа: http: //www.auditorium.ru/books/ 273/ Geopolitika_chapter18.html. – Загл. с экрана.
173. Глобальная информатизация и безопасность России [Текст]: материалы круглого стола "Глобальная информатизация и соц.-гуманитар. проблемы человека, культуры, общества" (МГУ, окт.2000 г.) / под ред. В.И. Добренькова. - М.: Изд-во Моск. ун-та, 2001.- 220 с.
174. Декларация об использовании научно-технического прогресса в интересах мира и на благо человечества //A/RES/3384 (XXX)., 1975.– 3с. [Электронный ресурс]. – Режим доступа: http://www.un-documents.net/a30r3384.htm. - Загл. с экрана.

175. Достижения в сфере информатизации и телекоммуникации в контексте международной безопасности // A/RES/53/70, 1999. – 2 с. [Электронный ресурс]. – Режим доступа: http://daccessdds.un.org/doc/UNDOC/GEN/N99/760/03/PDF/N9976003.pdf?OpenElement. – Загл. с экрана.
176. Егорова, Т.М. Проблемы международного сотрудничества в области информационного пространства стран СНГ [Электронный ресурс] // Доверие и безопасность в информационном обществе: сб. докл. и тез. междунар. конгресса, СПб., 21-23 апр. 2003 г. - Режим доступа: http://www.contel.iacis.ru/rus/ actions/doc/tab5_doc_egorova.doc. – Загл. с экрана.
177. Кузнецов, В. Н. Российская идеология XXI века в обеспечении эффективности и безопасности динамично-устойчивого развития России [Электронный ресурс]. – Режим доступа: http://spkurdyumov.narod.ru/Kuznetsov25.htm. – Загл. с экрана.
178. Лопатин, В.Н. Методологические проблемы формирования и защиты единого информационного пространства [Электронный ресурс] // Концептуальные проблемы информационной безопасности в союзе России и Беларуси: сб. докл. и тез. междунар. конф., СПб., 2003 г. – Режим доступа: http: // www.jurfak.spb.ru /conference/18102000/lopatin.htm. – Загл. с экрана.
179. Окинавская хартия глобального информационного общества [Электронный ресурс]. – Режим доступа: http://www.iis.ru/library/okinawa/charter.ru.html. – Загл. с экрана.
180. Омаров, Н. Опасная безопасность маленького Кыргызстана [Электронный ресурс] //Аналитика. Центр. Азия. – Режим доступа: [www.easttime.ru]. – Загл. с экрана.
181. Омуракунова, А. Кыргызстан: Обуздать необузданное. Нужно ли приравнять Интернет-издания к СМИ? [Электронный ресурс] //

АКИpress. – Режим доступа: http://www.zakon.kz/international_news/128515-kyrgyzstan-obuzdat-neobuzdannoe.-nuzhno.html.. - Загл. с экрана.

182. Панарин, И.Н. Пора сделать выводы из поражений в информационной войне и перейти к системным действиям [Электронный ресурс]. – Режим доступа: http://www.russiapost.su/archives/47085. - Загл. с экрана.

183. Панарин, И.Н. Информационная война опаснее ядерной [Электронный ресурс]. – Режим доступа: http://www.russiapost.su/archives/37117. - Загл. с экрана.

184. Пономаренко, В. Проблема 2033[Электронный ресурс]. – Режим доступа: http://www.libereya.ru/biblus/pr2033.htm. - Загл. с экрана.

185. Роль науки и техники в контексте международной безопасности и разоружения [Электронный ресурс] // A/RES/54/50, 1999. – 2 с. – Режим доступа: http://daccessdds.un.org/doc/UNDOC/ /N99/777/21/PDF/N9977721.pdf?. – Загл. с экрана.

186. Сикорская, И. Современные медиа-войны и проблемы информационной безопасности КР [Электронный ресурс] http://ca-mediators.net/ru/195-sovremennye-mediavoyny-i-problemy-informacionnoy-bezopasnosti-kyrgyzstana.html - Загл. с экрана.

187. Стюгин, М.А. Информационная безопасность «по существу» [Электронный ресурс]. – Режим доступа: http://psyfactor.org/lib/styugin6.htm. – Загл. с экрана.

188. Терминология Школы миротворчества и медиатехнологий в ЦА, Web. [Электронный ресурс].- Режим доступа: www.ca-mediators.net, 2013. - Загл. с экрана.

189. Токсоналиева, Р. Государственная политика Кыргызской Республики в сфере информационной безопасности [Электронный ресурс].- Режим доступа:

http://easttime.ru/analytics/kazakhstan/gosudarstvennaya-politika-kyrgyzskoi-respubliki-v-sfere-itseq/9087. - Загл. с экрана.

190. Шерстюк, В.П. Проблемы информационной безопасности в современном мире [Электронный ресурс].- Режим доступа: http://www.ict.edu.ru/ft/002471/sherstjuk.pdf.- Загл. с экрана.

191. Цифровая библиотека по философии [Электронный ресурс].- Режим доступа: http://filosof.historic.ru/books/item/f00/s00/z0000005/st054.shtml.- Загл. с экрана.

192. Цыгичко, В.Н. Актуальные проблемы обеспечения международной информационной безопасности [Электронный ресурс] // Доверие и безопасность в информационном обществе: сб. докл. и тез. междунар. конгр., СПб., 21-22 апр. 2003 г. - Режим доступа: http://www.contel.iacis.ru/rus/actions/doc/tab5_doc_cygichko.doc. - Загл. с экрана.

193. Постановление Правительства Республики Казахстан от 30 сентября 2011 г. № 1128 «О проекте Указа Президента Республики Казахстан «О Концепции информационной безопасности Республики Казахстан до 2016 года» (утвержден) // Электронная база нормативно-правовых актов «Параграф». online.zakon.kz/

194. Региональное Содружество в Области Связи. Аналитический доклад Совету глав правительств СНГ о текущем состоянии, проблемах и первоочередных задачах обеспечения информационной безопасности СНГ от 8 мая 2015 №50/21-7

195. Данияр Сабитов (2016) Информационная безопасность Казахстана: защита данных и смыслов. Доклад. Институт мировой экономики и политики при Фонде Первого Президента Республики Казахстан – Лидера Нации, Астана – Алматы, 2016 г. Источник

http://iwep.kz/files/attachments/article/2016-04-07/doklad_-_informacionnaya_bezopasnost_daniyar_sabitov.pdf

196. И.Иззет (2014) Али Гасанов: В Азербайджане необходимо создать концепцию информационной безопасности. Trend News Agency, 7 мая 2014, доступно по адресу https://www.trend.az/azerbaijan/society/2271584.html

197. Закон Азербайджанской Республики «Об информации, информатизации и защите информации» от 03.04.1998 г. www.rabita.az/uploads/qanunveril-cik/qanunlar_ru/ob_infor.pdf

198. Официальная страница Республики Молдова. (2016). Правительство утвердило законопроект о концепции информбезопасности Молдовы. Доступно на http://www.moldova.md/ru/content/pravitelstvo-utverdilo-zakonoproekt-o-koncepcii-informbezopasnosti-moldovy

199. Родичев, Ю. А. (2008). Информационная безопасность: нормативно-правовые аспекты. Учебное пособие. Издательский дом" Питер".

200. Смирнова, О. Г., & Хитов, С. Б. (2016). Правовые основы защиты информационных систем Российской Федерации от компьютерных атак. Право. Безопасность. Чрезвычайные ситуации, (1), 38-42.

201. Сафиев, К. И. (2014). Информационная безопасность Республики Таджикистан в контексте современного политического процесса. Диссертация по политологии на соискание научной степени кандидата политических наук. Доступно на http://cheloveknauka.com/informatsionnaya-bezopasnost-respubliki-tadzhikistan-v-kontekste-sovremennogo-politicheskogo-protsessa-suschnost-i-priori#ixzz51KCjaqsJ

202. Abbate, J. E. (1994). From ARPANET to Internet: A history of ARPA-sponsored computer networks, 1966--1988.

203. Salus, P. H., & Vinton, G. (1995). Casting the Net: From ARPANET to Internet and Beyond... Addison-Wesley Longman Publishing Co., Inc.

204. Ismailova, R., & Muhametjanova, G. (2016). Cyber crime risk awareness in Kyrgyz Republic. Information Security Journal: A Global Perspective, 25(1-3), 32-38.

205. Ismailova, R. (2017). Web site accessibility, usability and security: a survey of government web sites in Kyrgyz Republic. *Universal Access in the Information Society*, *16*(1), 257-264.

206. United Nations: UN global E-government Survey 2003. United Nations Division for Public Administration and Development Management. http://unpan1.un.org/intradoc/groups/public/documents/un/unpan016066.pdf. Retrieved 5/25/2015 (2003)

207. United Nations: Global E-government Readiness Report 2004—Towards Access for Opportunity. United Nations Division for Public Administration and Development Management. http://unpan1.un.org/intradoc/groups/public/documents/un/unpan019207.pdf. Retrieved 5/25/2015 (2004)

208. United Nations: Global E-government Readiness Report 2005—from E-Government to E-Inclusion. United Nations Division for Public Administration and Development Management. http://unpan1.un.org/intradoc/groups/public/documents/un/unpan021888.pdf. Retrieved 5/25/2015 (2005)

209. United Nations: Global E-government Readiness Report 2008—from E-Government to Connected Governance. United Nations Division for Public Administration and Development Management, http://unpan1.un.org/intradoc/groups/public/documents/un/unpan028607.pdf. Retrieved 5/25/2015 (2008)

210. United Nations: UN E-government Survey 2010-Leveraging e-government at a time of financial and economic crisis. http://unpan1.un.org/intradoc/groups/public/documents/un/unpan038851.pdf. Retrieved 5/25/2015 (2010)

211. United Nations: UN E-government Survey 2012—E-government for the People. http://unpan1.un.org/intradoc/groups/public/documents/un/unpan048065.pdf. Retrieved 5/25/2015 (2012)

212. United Nations: UN E-government Survey 2014—E-government for the Future We Want. http://unpan3.un.org/egovkb/Portals/egovkb/Documents/un/2014-Survey/E-Gov_Complete_Survey-2014.pdf. Retrieved 5/25/2015 (2014)

213. Национальный статистический коммитет. 26.06.2015 / Информационно-коммуникационные технологии в Кыргызской Республике 2009 - 2013; http://new.stat.kg/media/publicationarchive/30e40cc2-0587-4f0f-b7f0-d488351e30b3.doc

214. Гапеева, О. Л. (2016). Информационная безопасность на постсоветском пространстве: системно-исторический анализ. *Грані*, *19*(12), 93-99.

215. Бачило, И. Л., Бондуровский, В. В., Вус, М. А., Кучерявый, М. М., & Макаров, О. С. (2013). О совершенствовании и гармонизации национального законодательства государств–участников СНГ в сфере обеспечения информационной безопасности. *Информационное право*, (1), 32.

216. http://cbd.minjust.gov.kg/act/view/ru-ru/111527 (УК КР)

217. Историческая ретроспектива гражданского самосознания в России. Материалы Международной научной конференции, 25 декабря 2012 г. Том 1 http://bibliorossica.com 26 Мая 2016