Дмитриенко И.А.,
ю.и.д., проф м.а.
окуу иштери боюнча проректор
КМЮА
Дмитриенко И.А.,
д.ю.н., и.о.проф.
проректор по учебной работе КГЮА
L.A. Dmitrienko,
D.Sc., acting.prof.
Vice Rector for Academic Affairs
Kyrgyz State Law Academy

Сулейман Ш.,
окутуучу, КМЮА
Сулейман Ш.,
преподаватель, КГЮА
Suleyman Sh.,
teacher, Kyrgyz State Law Academy

УДК 34.01:0004.056

МААЛЫМАТЫК КООПСУЗДУКТУ КАМСЫЗДОО ҮЧҮН ЧЕНЕМДИК УКУК-ТУК БАЗАНЫ ӨРКҮНДӨТҮҮ БОЮНЧА СУРООЛОР

ВОПРОСЫ СОВЕРШЕНСТВОВАНИЯ НОРМАТИВНОЙ ПРАВОВОЙ БАЗЫ ОБЕСПЕЧЕНИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

THE QUESTIONS OF IMPROVING THE NORMATIVE LEGAL BASE OF INFOR-MATION SECURITY

Аннотация: *Бул макалада маалымат коопсуздугун көзөмөлдөө маселелери, ошондой эле Кыргыз Республикасынын мыйзамдарына маалыматтык коопсуздукту укуктук жөнгө салууну өркүндөтүнүн келечеги талкууланат.*

Аннотация*: в данной статье рассматривается вопросы регулирования информаци-онной безопасности, а также перспективы совершенствования правового регулирования информационной безопасности в законодательстве Кыргызской Республики.*

Annotation: *this article discusses issues of information security regulation, as well as pro-spects for improving the legal regulation of information security in the legislation of the Kyrgyz Re-public.*

Негизги сөздөр: *Маалымат коопсуздугу; маалымат коому; маалымат технологияла-ры; маалымат жана байланыш технологиялары; киберкылмыштуулук; киберкоопсуздугу, интернет мамилелери.*

Ключевые слова: *информационная безопасность; информационное общество; информационные технологии; информационно-коммуникативные технологии; киберпреступность; кибербезопасность; кибертерроризм; интернет-отношения.*

Keywords: *information security; information society; information technologies; information and communication technologies; cybercrime; cybersecurity; cyberterrorism; Internet relations.*

Сегодня информационная безопасность является одним из приоритетных направлений обеспечения национальной безопасности. Исследовав состояние правового обеспечения информационной безопасности в Кыргызской Республике, проанализировав действующее законодательство в данной области, можно сделать следующие выводы. В определении национальной безопасности должна соблюдаться иерархия ценностей, подлежащих защите. На первое место должны быть поставлены суверенитет и территориальная целостность, после них конституционные права и свободы, и на третьем месте – достойные качество и уровень жизни. Ведь для государства именно суверенитет и территориальная целостность составляют первейшую ценность, поскольку эти свойства являются для любой государственности необходимыми сущностными признаками, условиями ее существования. Без обеспечения суверенитета и территориальной целостности невозможно обеспечить ни конституционные права и свободы, ни достойные качество и уровень жизни граждан. Мы придерживаемся мнения док-тора юридических наук В. А. Томсинова, который считает, что «подлинный и вполне определенный смысл понятие «национальная безопасность» приобретает, если под ним понимать условия, обеспечивающие защиту от внешних и внутренних угроз жизненно важных для существования и поступательного развития государства, национальных интересов и фундаментальных ценностей [1]. Нормативные правовые акты, регулирующие правовые отношения, возникающие в информационной сфере, находятся в хаотичном состоянии и относятся к разным отраслям права. Исследования нормативно-правовой базы, регулирующей информационную сферу, показывают, что нередко прослеживается дублирование правовых норм, а по-рой и их противоречивость. Эти недостатки препятствуют правильному толкованию и применению правовых норм. В связи с этим, законодательство в информационной сфере нуждается в совершенствовании и прогрессивном развитии. Безусловно, в последние годы одним из главных направлений политики Кыргызской Республики является обеспечение информационной безопасности. Кыргызская Республика активно взаимодействует с партнёрами в об-ласти обеспечения международной информационной безопасности, в том числе в рамках ООН, БРИКС, Шанхайской организации сотрудничества. Развитие информационной безопасности возможно реально обеспечить лишь в рамках международного сотрудничества по аналогии с системой комплексной безопасности, так как она носит декларативный характер. В нашем законодательстве также отсутствует правовое регулирование киберпреступности. С каждым годом наблюдается рост киберпреступности, но отсутствие нормативно-правовой базы и практики противодействия данной преступности не позволяют разрешить данную проблему, способствовать уменьшению количества преступлений в киберпространстве. Исследовав состояние киберпреступности в Кыргызской Республике и в зарубежных странах, можно прийти к выводу, что с данным явлением невозможно бороться каждому государству самостоятельно, так как киберпреступность выходит за рамки национальной проблемы и приобретает международный характер. В связи с этим, существует необходимость разработки единого международного документа. В нём следует закрепить понятийный аппарат, связанный с киберпространством, раскрыть содержание и сущность данных понятий; определить, что непосредственно относится к информационной преступности, а что – к киберпреступности; закрепить меры ответственности и санкции за совершённые преступления; закрепить применение процессуального законодательства в данной сфере. Перечисленное – только основные положения, которые важно отразить в международном документе, но для его разработки и принятия необходимо тщательное научное исследование проблем и вопросов, анализ всей совокупности международных норм и практики борьбы с преступлениями в установленной сфере.

Также на данный момент однозначного определения информационной безопасности пока не сложилось. Отмечаются несколько вариантов определения этого направления в области исследования информационной и коммуникационной деятельности и обеспечения без-опасного состояния отношений в информационной сфере. Модельный закон МПА СНГ “О международном информационном обмене” (2002 г.) определяет информационную безопасность как “состояние защищенности информационной среды общества, обеспечивающее ее формирование, использование и развитие в интересах граждан, организаций, государства”. Концепция сотрудничества государств-участников СНГ в сфере обеспечения информационной безопасности, утвержденная Советом глав государств СНГ в 2008 г., трактует информационную безопасность как “состояние

защищенности от внешних и внутренних угроз информационной сферы, формируемой, развиваемой и используемой с учетом жизненно важных интересов личности, общества и государства". Большинство понятий в тексте концепции относятся, прежде всего, к задачам защиты информации.

В трактовке, закрепленной в тексте Соглашения между правительствами государств-членов Шанхайской организации сотрудничества о сотрудничестве в области обеспечения международной информационной безопасности "информационная безопасность – состояние защищенности личности, общества и государства и их интересов от угроз, деструктивных и иных негативных воздействий в информационном пространстве". В такой формулировке это базовое понятие охватывает наиболее актуальные угрозы социально-гуманитарного плана, в частности угрозу распространения информации, наносящей вред общественно-политической и социально-экономической системам, духовной, нравственной и культурной среде государства.

В качестве специального принципа совершенствования законодательства государств-участников СНГ в рекомендациях названа "безопасность через развитие", что предполагает динамичное совершенствование правовых методов обеспечения информационной безопасности по мере развития информационного общества. В качестве одного из показателей информационной безопасности предложено рассматривать динамику социальных индикаторов реализации базовых интересов личности, общества и государства [2].

В контексте широкомасштабной правовой реформы, осуществляемой в различных сферах, в частности конституционной, судебной, административной происходит также совершенствование информационного законодательства. Нельзя не обратить внимания на такой факт, как растущий уровень кибертерроризма, соединенный с неадекватным реагированием законодателя на данные процессы, в частности формирование эффективного информационного законодательства и принятия кодифицированного закона в рассматриваемой сфере. Од-ной из причин является то, что информационные отношения, по сравнению с другими правовыми отношениями, более динамичны, и этот факт негативно влияет на актуальность действующих норм.

Отметим, что в мировой практике наряду с принятием стратегий и законов о национальной безопасности сложилась практика определения информационной безопасности как "кибербезопасности". Это отражает как бы ориентацию на интернет-безопасность, безопасность электронной, сетевой сферы. Однако вопрос по существу шире. Европейская комиссия ставит вопрос о создании единого Европейского информационного пространства. Создано Европейское агентство по сетевой информационной безопасности. За 2011 г. в Европе одиннадцать государств Евросоюза приняли Стратегии кибербезопасности. Стратегия кибербезопасности США, принятая в мае 2011 г., определяет семь направлений ее реализации, в числе которых следующие: экономика, защита национальных сетей; правопорядок – расширение сотрудничества и правовых норм, регулирующих отношения субъектов. Сюда входит военная отрасль: подготовка к современным вызовам безопасности. Рассматривается вопрос об Интернет-правительстве: продвижение эффективных и всеохватывающих правительственных структур[3].

Вопрос международного развития включает построение безопасности, развитие международной компетенции и экономическое процветание. Взаимодействие всех направлений национальной безопасности с потенциалом ИКТ и его реальным присутствием во всех областях жизни страны "превращают информационные технологии в мощный катализатор практически всех сфер жизнедеятельности современного общества – экономики, науки, образования, культуры, социально-бытовой сферы"[4]. Поскольку информационная безопасность является частью национальной безопасности Кыргызской Республики, следует учитывать, что речь идет не только об обеспечении безопасности в самой информационной сфере и среде, но и об информационной составляющей в каждом из направлений национальной безопасности: политической, экономической, экологической, внутриполитической, международной, пограничной, военной и т. д. Стратегия национальной безопасности лишний раз подтверждает, что информационные ресурсы и технологии составляют стратегический потенциал любо-го направления деятельности государства, всех его структур и всех институтов гражданского общества.

В связи с этим было бы уместно в ходе проведения работ по кодификации отечественного информационного законодательства большее внимание уделить нормативно-правовому регули-

рованию следующих вопросов: противодействие техническим разведкам; защита информации в информационно-телекоммуникационных системах; конструирование интернет-отношений с последующей выработкой механизмов их государственного регулирования; формирование действенных механизмов защиты персональных данных техническими средствами; организация взаимодействия и координация развития системы технической защиты информации с сохранением государственного контроля за данной сферой. В частности, мы считаем, что указанные направления деятельности требуют урегулирования в соответствующих разделах будущего кодификационного акта Кыргызстана вследствие прогнозируемого увеличения количества совершаемых кибератак, а также в связи с ускоренным развитием киберугроз и отчасти отсутствием действенной защиты государственных информационных ресурсов. Как известно, степень развитости информационного общества непосредственно влияет на процесс функционирования государственных институтов, экономику и обороноспособность страны. В этой связи возникает необходимость формирования национальной государственной политики в информационной сфере, в которую должны быть включены: разработка и реализация комплексных мероприятий по предотвращению, нейтрализации и опережению негативного информационного воздействия на общество и государство; подготовка общества к активному информационному противодействию; вхождение национального информационного поля в мировое информационное пространство; совершенствование системы массовой информации и коммуникации; формирование системы подготовки кадров для информационного противодействия.

СПИСОК ИСПОЛЬЗОВАННОЙ ЛИТЕРАТУРЫ:

1. Томсинов, В.А. Славная революция 1688-1689 годов в Англии и Билль о правах [Текст]: / В.А.Томсинов. – М.: Зерцало-М, 2010. – 250 с.

2. 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.

3. Энтина, Л.М. Европейское право[Текст]: учеб. для вузов /под общ. ред. – М.: Изд-во НОРМА, 2000. – 720 с.

4. Абилдаев, Э.Е. Политическая система Кыргызстана: проблемы и перспективы [Текст]: /Э.Е.Абилдаев. - Бишкек: Илим, 2001. – 320 с.