Камытов К. Т.,
юридика илимдеринин доктору
КМЮА нын Маалыматтык укук жана табигый
илимдер дисциплиналары кафедрасынын доценти
Камытов К.Т.,
доктор юридических наук
заведующий кафедры информационного права
и естественно-научных дисциплин КГЮА
Kamytov K. T.,
Doctor of law
Associate Professor at the Department of Information
Law and natural sciences disciplines KSLA
e-mail: kkamyt@mail.ru

УДК 004.7.056.53.(575.2)

КЫРГЫЗ РЕСПУБЛИКАСЫНЫН КИБЕР КООПСУЗДУКТУН КОНЦЕПЦИЯСЫ: УККТУК АСПЕКТТЕРИ

КОНЦЕПЦИЯ КИБЕРБЕЗОПАСНОСТИ КЫРГЫЗСКОЙ РЕСПУБЛИКИ: ПРАВОВЫЕ АСПЕКТЫ

CYBER SECURITY CONCEPT KYRGYZ REPUBLIC: LEGAL ASPECTS

Аннотация: *макалада маалымат жана байланыш технологияларын өнүктүрүү, мамлекеттик башкаруу жараяндарына, өз ара аракеттенүү жана мамлекеттик бийлик органдары тарабынан маалымат алмашуу, бизнес - коомчулуктун жана жарандардын, изилдөө жана билим берүү, коомдук коопсуздук жана саламаттыкты сактоо, соода өнүмдөр жана кызматтар, эс алуу тармактарында болгон көйгөйлөр жана маселелер каралат.*

Аннотация: *В статье рассматриваются вопросы и проблемы развития информационно-коммуникативных технологий, процессах государственного управления, взаимодействия и обмена информацией государственных органов, бизнес - сообщества и граждан, в научных исследованиях и образовании, социальном обеспечении и медицинском обслуживании, обеспечении торговли продуктами и услугами, досуге.*

Annotation: *The article deals with issues and problems of development of information and communication technologies, processes of public administration, interaction and information exchange between government agencies, the business community and citizens, in research and education, social security and health care, trade in products and services, and leisure.*

Негизги сөздөр: *маалымат жана байланыш технологиялары; технологиялык жетишкендиктер; интернет тармагы; маалымат коопсуздугу; байланыш жабдуулары; оргтехникалар; байланыш каражаттары; программалык камсыз кылуу жана атайын жабдык маалымат издөө; ошондой эле аны коргоо.*

Ключевые слова: информационно-коммуникативные технологии; технологический прогресс; сеть интернет; информационная безопасность; телекоммуникационное оборудование; оргтехника; средства связи; программное обеспечение специальных технических средств съема информации, а также ее защита.

Keywords: *information and communication technologies; technological progress; the Internet; information security; telecommunications equipment; office equipment; communications equipment; software; special technical means of information retrieval; as well as its protection.*

Технологический прогресс и развитие информационно-коммуникативных технологий (ИКТ) стали определяющими в стремительном их использовании во всех сферах жизни кыргызского общества - процессах государственного управления, взаимодействия и обмена информацией государственных органов, бизнес - сообщества и граждан, в научных исследованиях и образовании, социальном обеспечении и медицинском обслуживании, обеспечении торговли продуктами и услугами, досуге.

Вследствие этого, использование ИКТ вызывает изменения в социальной, технологической и правовой сферах, существующих процедурах и механизмах. Давая возможности для развития свободы слова и самовыражения, ИКТ порождают новые вызовы государству и гражданскому обществу в виде запрещенной к распространению информации и противоправных действий, совершенных с использованием ИКТ. Усиление законодательных и практических мер против цензуры, необходимо сопровождать созданием правовых норм и механизмов, обеспечивающих эффективное противодействие противоправным проявлениям в информационной сфере.

Принимая во внимание растущее использование сети Интернет с особой остротой встает вопрос защиты информационной инфраструктуры, требующей широкого диапазона мер в области сетей связи и их информационной безопасности, борьбы с киберпреступностью. Оперативное реагирование и эффективное противодействие противоправным действиям, требует развития сети центров реагирования на компьютерные инциденты и организации их взаимодействия с правоохранительными органами.

Существующие и потенциальные угрозы в сфере информационной безопасности относятся к числу наиболее серьезных вызовов XXI века. Эти угрозы от широкого круга источников проявляются в подрывных действиях, направленных как против физических лиц, бизнеса, государственных органов, так и против правительства. Их последствия несут в себе существенный риск для общественной безопасности, безопасности государств и стабильности глобально связанного между собой международного сообщества как единого целого.

В Кыргызстане слабо контролируется ввоз, производство и реализация несертифицированного (зачастую контрафактного) телекоммуникационного оборудования, оргтехники, средств связи, программного обеспечения, специальных технических средств съема информации, а также ее защиты.

Недостаточное внимание уделяется вопросам формирования и реализации единой государственной политики по обеспечению информационной безопасности, координации деятельности органов власти и управления Кыргызской Республики по ее укреплению. Мероприятия, нацеленные на защиту информационной сферы, недостаточно обеспечены финансовыми ресурсами.

Вследствие вышеназванных причин в Кыргызской Республике наблюдается усиление угроз национальной безопасности Кыргызской Республики в информационном пространстве страны по следующим направлениям:

- стремление сопредельных государств к доминированию в информационном пространстве Кыргызской Республики (включая получение доступа к информации с ограниченным доступом) и как следствие вытеснение его из внутреннего рынка;

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

- деятельность спецслужб других государств, международных экстремистских, террористических и других преступных сообществ, антиобщественных организаций и групп в информаци-

онной сфере Кыргызской Республики, их интерес к обладанию информационным оружием и его применению.

В последнее время достаточно часто звучат слова о том, что необходимо усилить информационную безопасность, правда, при этом часто смешивают два понятия: «компьютерная безопасность» и «информационная безопасность». Причем первое является составной частью второго. Да, компьютерная безопасность (в смысле безопасность самих компьютеров и компьютерных сетей) - вещь, безусловно, необходимая, но недостаточная в нынешних условиях.

Подчеркнем, что информационная экспансия по заданному шаблону неспешно «формирует» в экономике, в политике, в обороне, в информатике, в духовной и в других сферах нашей государственной, общественной и личной жизни, прежде всего те направления развития, которые определяют дальнейшую судьбу любого государства как интеллектуального и сырьевого придатка нынешнего цивилизованного мира.

Перечислим набор средств, которые входят в информационное оружие:

- программное и информационное обеспечение;
- программно-аппаратные, телекоммуникационные и другие средства информации и управления;
- каналы связи, обеспечивающие циркуляцию информационных потоков и интеграцию систем управления;
- интеллект человека и массовое сознание.

Отметим, что информационное оружие обладает наибольшей избирательностью, поражаемостью и требуемой масштабностью. Это объясняется такими свойствами информационной сферы, которые кардинально отличают ее от других компонентов жизненной среды:

- неисчерпаемость и восполняемость инфоресурсов;
- возможность их быстрого копирования с высокой степенью достоверности;
- возможность перемещения больших объемов этих ресурсов практически без потерь, с высокой скоростью и на огромные расстояния;
- компактность источников и носителей информации;
- мгновенная, но бескровная реакция (отклик) информационной сферы на трудно идентифицируемое (в отношении источника) воздействие и др.

Характерно, что к числу воздействующих на инфосферу можно отнести и невоенные средства, куда входят:

- идеологические;
- религиозно-культурные;
- политические;
- дипломатические;
- торгово-экономические;
- финансово-кредитные;
- военно-экономические;
- промышленно-технологические;
- научно-технические;
- асоциальные.

В целом под информационным оружием понимается совокупность специальных средств, технологий, информации и дезинформации, при¬меняемой для деструктивных воздействий на менталитет населения и информационно-техническую инфраструктуру государства. К видам ин¬формационного оружия можно условно (по отношению к основным объектам воздействия) отнести пять соответствующих совокупностей или групп средств, применяемых для деструктивных (дезориентирующих, дезинформирующих, дезорганизующих, дестабилизирующих, разрушающих, подавляющих и др.) информационных воздействий:

- средства массовой информации (СМИ: радио, пресса, телевидение) и агитационно-пропагандистские средства (видеокассеты, электронные учебники и энциклопедии и др.) как вид информационного оружия массового поражения, предназначенного для целенаправленного нанесения информационного ущерба главным образом духовно-нравственной жизни населения противостоящей (враждебной) стороны и в первую очередь его исторической памяти, мировоз-

зрению, морально-нравственным идеалам с целью возможного управления его поведением, а также — для создания препятствия аналогичным действиям противника;

• психотронные средства (специальные генераторы, специальная видеографическая и телевизионная информация, видеосредства НИТ типа «виртуальная реальность» и др.), предназначенные для дистанционного зомбирования населения и военно-технического персонала противостоящей стороны, а также для возбуждения психических и психофизиологических расстройств людей — пользователей систем НИТ (видеографических и др.) на основе специальной комбинации цветовой гаммы, дискретности и интенсивности излучения на экранах ЭЛТ мониторов, эффекта «25-го кадра» (воспринимаемого только на подсознательном уровне) и др.

• электронные средства (оптико- и радиоэлектронные средства — специальные передающие устройства и излучатели электромагнитных волн и импульсов, и др.; электронно-вычислительные средства — «компьютерные вирусы», разрушающие программные закладки - «черви» и др.). Радиоэлектронные средства предназначены для радиоэлектронного подавления и поражения радиоэлектронных средств и сил противника, а также для защиты своих радиоэлектронных средств от радиоэлектронного поражения и подавления. Оптикоэлектронные — для подавления и поражения оптикоэлектронных средств противника. Электронно-вычислительные средства или средства компьютерных технологий предназначены для повышения эффективности действия своих информационных систем и средств (в частности, систем оружия и средств распознавания целей и их принадлежности на поле боя), а также для разрушения или искажения информационных массивов данных, используемых в автоматизированных информационно-ударных системах противника;

• лингвистические средства (языковые единицы, «специальная» терминология, обороты речи, имеющие семантическую неоднозначность при переводе на другие языки и др.), предназначенные главным образом для использования высококвалифицированными специалистами при ведении международных переговоров, подписании и выполнении договоров между сторонами. Данные средства могут обеспечить долговременный и эффективный результат;

• психотропные средства (специально структурированные лекарства, психофармакологические и психодислептические средства, транквилизаторы, антидепрессанты, галлюциногены, наркотики, алкоголь и др.), предназначенные для воздействия на психику человека на генном или хромосомном уровнях: транквилизаторы разрывают связь между информационно-психическими и физическими процессами в организме человека, галлюциногены вызывают психические расстройства и др.

В последние годы в стране предпринимаются меры для обеспечения информационной безопасности, в частности, были образованы: в 2006 г. – Национальное агентство информационных ресурсов, технологий и связи; в 2007 г. – Межведомственная комиссия по вопросам обеспечения информационной безопасности; в 2010 г. – Консультативный совет Государственного агентства связи при правительстве КР; в 2014 г. – Совет по информационной политике при Министерстве культуры, информации и туризма и т. д.

Вместе с тем анализ состояния информационной безопасности показывает, что существующая законодательная база является недостаточной, так как многие вопросы не имеют соответствующего законодательного регулирования, не затрагивается вопрос о создании национального информационного пространства, когда с применением новейших технологий на него проводятся скрытые атаки со стороны «внешних игроков». Не до конца отрегулированы правовые основы обеспечения информационной безопасности КР, относящиеся к совершенствованию нормативно-правовых актов, регламентирующих отношения различных министерств и ведомств в информационной сфере. Также отсутствует единый орган по обеспечению информационной безопасности, хотя существует ряд государственных органов, осуществляющих управление в области информации, которые нередко дублируют друг друга.

На сегодняшний день современная информационная инфраструктура в республике находится на стадии формирования и входящие в нее информационные системы зачастую не имеют выхода в открытые сети связи. Не до конца разработанное нормативно-правовое регулирование отношений в области массовой информации затрудняет формирование на территории республики конкурентоспособных информационных агентств и средств массовой информации. Отсутствует

конкретная государственная политика в области формирования национального информационного пространства, развития системы массовой информации, организации международного информационного обмена. На фоне этого отмечается ухудшение ситуации в обеспечении сохранности сведений, составляющих государственную тайну.

Кыргызстан сталкивается с информационной агрессией со стороны государств ближнего и дальнего зарубежья, которые в целях продвижения своих интересов используют сложившуюся социально-политическую ситуацию в стране с участием самих же кыргызстанцев. Произошедшие и происходящие в стране общественно-политические события свидетельствуют об использовании иностранными субъектами «внешних» (международных) и «внутренних» (подконтрольных) средств массовой информации и коммуникации для изменения состояния информационного пространства в целях оказания влияния на ход событий. В частности, освещение в зарубежных СМИ различных событий в республике показывает, что Кыргызстан становится жертвой спланированного информационно-психологического воздействия, наносящего ему политический и экономический ущерб.

Открытость национального информационного пространства порождает реальную угрозу негативного информационного влияния на общественное сознание населения, что представляет для нашего общества особую социальную опасность. «Информационное пространство – эта сфера деятельности, связанная с формированием, созданием, преобразованием, передачей, использованием, хранением информации, оказывающая воздействие, в том числе на индивидуальное и общественное сознание, информационную инфраструктуру и собственно информацию».

Развитие в последние годы электронных массмедиа, в частности социальных сетей, и их бесконтрольность оказывает негативное влияние на пользователей, которыми, в основном, являются молодежь и образованные люди с активной жизненной позицией. При этом вызывает беспокойство то, что социальные сети в Кыргызстане, как и в других государствах, используются в качестве площадки для вербовки в религиозно-экстремистские организации и проведения антиобщественных акций, о чем свидетельствуют происходящие в нашей стране события. В этой связи стратегической целью КР в области телекоммуникационных технологий должна стать разработка развития национальной информационной структуры и обеспечение ее активного участия в процессах использования глобальных информационных сетей и систем вхождения в мировое информационное пространство в условиях обострения международной конкуренции за обладание технологическими и информационными ресурсами.

Несмотря на предпринимаемые властными структурами страны меры по совершенствованию информационно-коммуникационных технологий, происходящие внутренние социально-политические события в республике показывают, что у правительства КР нет четкой государственной политики в области формирования национального информационного пространства, развития системы массовой информации и коммуникации, организации международного информационного обмена. В системе обеспечения информационной безопасности наиболее уязвимым звеном остается общество, информационные и телекоммуникационные системы. Сегодня приходится констатировать тот факт, что вследствие сужения информационного поля жители страны, особенно сельской местности, становятся жертвами негативного информационно-психологического воздействия. В условиях однобокой информации, несбалансированной информационно-коммуникационной государственной политики жители сельской местности зачастую подвергаются влиянию идеологии религиозно-экстремистских и террористических организаций, что имеет тенденцию к нарастанию.

Как известно, степень развитости информационного общества непосредственно влияет на процесс функционирования государственных институтов, экономику и обороноспособность страны. На сегодняшний день на законодательном уровне у Кыргызстана не существует достаточных гарантий защиты населения от негативного информационного воздействия, результатом которого может стать разрушение единого информационного и духовного пространства.

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 ин-

формационному противодействию; вхождение национального информационного поля в мировое информационное пространство; совершенствование системы массовой информации и коммуникации; формирование системы подготовки кадров для информационного противодействия.

Существующие в республике ВУЗы по подготовке специалистов в сфере информационно-коммуникационных технологий не обладают необходимой материально-технической базой и профессиональными кадрами, что не позволяет обеспечить поддержание состояния информационной защищенности страны. Данная ситуация свидетельствует о необходимости создания единого учебного заведения для подготовки специалистов по стратегическому анализу, информационному воздействию и противодействию. Фактор недооценки в сфере кадровой политики приведет к усугублению информационной опасности, которая уже является объективной реальностью. Также необходимо обратить внимание на интеграцию национальных информационных ресурсов в единое информационное пространство как часть системы обеспечения стратегической стабильности и безопасности.

Принимая во внимание растущее использование сети Интернет, с особой остротой встает вопрос защиты информационной инфраструктуры, требующей широкого диапазона мер в области сетей связи и их информационной безопасности, борьбы с киберпреступностью. Оперативное реагирование и эффективное противодействие противоправным действиям, требует развития сети центров реагирования на компьютерные инциденты и организации их взаимодействия с правоохранительными органами.

Недостаточное внимание уделяется вопросам формирования и реализации единой государственной политики по обеспечению информационной безопасности, координации деятельности органов власти и управления по ее укреплению. Мероприятия, нацеленные на защиту информационной сферы, недостаточно обеспечены финансовыми ресурсами.

Национальные интересы КР в информационной сфере:

- защита информационных ресурсов от несанкционированного доступа, обеспечение безопасности информационных и телекоммуникационных систем, как уже развернутых, так и создаваемых на территории КР;
- развитие современных ИТ, отечественной ИКТ-индустрии, обеспечение потребностей внутреннего рынка её продукцией и выход этой продукции на мировой рынок, а также обеспечение накопления, сохранения и эффективного использования отечественных информационных ресурсов;
- информационное обеспечение государственной политики КР по доведению до национальной и международной общественности достоверной информации и государственной политике КР, с обеспечением доступа к открытым государственным информационным ресурсам;
- соблюдение прав и свобод человека в информационной сфере, обеспечение духовного обновления в КР, сохранение и укрепление нравственных ценностей общества, традиций патриотизма и гуманизма, культурного и научного потенциала страны.

Виды угроз в информационной сфере:

- угрозы конституционным правам и свободам человека и гражданина в области духовной жизни и информационной деятельности, индивидуальному, групповому и общественному сознанию, духовному возрождению КР;
- угрозы информационному обеспечению государственной политики КР;
- угрозы развитию отечественной индустрии информации, включая индустрию средств информатизации, телекоммуникации и связи, обеспечению потребностей внутреннего рынка в её продукции и выходу этой продукции на мировой рынок, а также обеспечению накопления, сохранности и эффективного использования отечественных информационных ресурсов;
- угрозы безопасности информационных и телекоммуникационных средств и систем, как уже развернутых, так и создаваемых на территории КР.

Анализ современного состояния информационной безопасности в Кыргызской Республике показывает, что ее уровень в настоящее время не соответствует жизненно важным потребностям личности, общества и государства. Сегодняшние условия политического и социально-экономического развития страны вызывают обострение противоречий между потребностями общества в расширении свободного обмена информацией и необходимостью сохранения отдельных огра-

ни¬чений на ее распространение. Отсутствие действенных механизмов регулирования информационных отношений в обществе и государстве приводит ко многим негативным последствиям.

Такое положение дел в области обеспечения информационной безопасности не позволяет Кыргызстану на равноправной основе включиться в мировую информационную систему и требует безотлагательного решения следующих ключевых проблем:

- развитие научно-практических основ информационной безопасности, отвечающих современной геополитической ситуации и условиям политического и социально-экономического развития Кыргызской Республики;
- формирование законодательной и нормативно-правовой базы обеспечения информационной безопасности, в том числе разработка реестра информационного ресурса, регламента информационного обмена для органов государственной власти и управления, предприятий, нормативного закрепления ответственности должностных лиц и граждан за соблюдение требований информационной безопасности; разработка механизмов реализации прав граждан на информацию; формирование системы информационной безопасности, обеспечивающей реализацию государственной политики в области информационной безопасности;
- разработка современных методов и технических средств, обеспечивающих комплексное решение задач защиты информации; разработка критериев и методов оценки эффективности систем и средств информационной безопасности и их сертификации; исследования форм и способов цивилизованного воздействия государства на формирование общественного сознания; комплексное исследование деятельности персонала информационных систем, в том числе методов повышения мотивации, морально-психологической устойчивости и социальной защищенности людей, работающих с секретной и конфиденциальной информацией.