ФИЗИКА PHYSICS

УДК 341.1/8:004.056.53

МЕЖДУНАРОДНАЯ ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ: ВЫЗОВЫ И ПРОБЛЕМЫ

[1]Сагымбаев А.А.
доктор технических наук,
главный научный сотрудник
[2]Кожомуратов З.К.
заместитель министра
[3]Курманкожоева А.С.
преподаватель
[4]Сагымбаев А.А.
инженер сетевых операций

ЭЛ АРАЛЫК МААЛЫМАТТЫК КООПСУЗДУК: ЧАКЫРЫКТАРЫ ЖАНА КӨЙГӨЙЛӨРҮ

Сагымбаев А.А.
техника илимдеринин доктору,
башкы илимий кызматкер
Кожомуратов З.К.
министрдин орун басары
Курманкожоева А.С.
окутуучу
Сагымбаев А.А.
инженер

DYNAMICS OF CHANGES IN THE SERVICES VOLUME OF THE "TELECOMMUNICATIONS" MARKET OF THE KYRGYZ REPUBLIC

Sagymbaev A.A.
doctor of technical sciences,
chief scientific associate
Kozhomuratov Z.K.
deputy minister
Kurmankozhoeva A.C.
lecturer
Sagymbaev A.A.
engineer

[1]Институт физики им.Ж.Жеенбаева НАН КР
Institute of Physics named after academician J. Zheenbaev of the NAS KR

[2]Министерство цифрового развития Кыргызской Республики
Ministry of Digital Development of the Kyrgyz Republic

[3]Кыргызско-Российско-Славянский Университет им. Б.Н. Ельцина
Kyrgyz-Russian Slavic University named after B.N.Yeltsin

[4]Облачной провайдер "IaaSRackCorp"
Cloud provider "IaaSRackCorp"

Аннотация. В статье анализируются современные проблемы обеспечения международной информационной безопасности страны, которые имеют комплексный, многогранный характер. Успешное развитие и само существование страны, как суверенного государства, невозможно без обеспечения ее международной информационной безопасности. Международная информационная безопасность общества и государства определяется степенью их защищенности от негативного внешнего воздействия и, следовательно, устойчивостью в основных сферах жизнедеятельности страны по отношению к опасным, дестабилизирующим, деструктивным, ущемляющим интересы общества и страны информационным воздействиям на уровне как внедрения, так и извлечения информации.

Ключевые слова: информационно-коммуникационные технологии, инновация, цифровые технологии, национальное информационное пространство, Интернет.

Аннотация. Комплекстүү жана көп кырдуу мүнөзгө ээ болгон мамлекеттин эл аралык маалыматтык коопсуздугун камсыздоонун азыркы убактагы көйгөйлөрү талданган. Мамлекеттин ийгиликтүү өөрчүшү жана эгемен болушу анын эл аралык маалыматтык коопсуздугун камсыздоосуз ишке ашпайт. Коомдун жана мамлекеттин эл аралык маалымат коопсуздугу, алардын сырттан келген тескери таасирлерден коргонуусу менен аныкталат, демек мамлекеттин ичиндеги болуп жаткан өзгөрүштөрдүн сырттан таасир эткен коркунучтарга, коомго тескери таасир эткен деструктивдүү элементтерге, коомдун жана мамлекеттин кызыкчылыгына кайчылаш келген, сырттан таасир этүүчү маалыматтык булактарга, ошондой эле, ички коомдун жана мамлекеттин маалыматтарын уруксаты жок алып кетүүсүнө каршылык көрсөткөн иш-аракеттердин туруктуулугу.

Негизги сөздөр: маалыматтык жана коммуникациялык технологиялары, инновация, санариптик технологиялары, улуттук маалымат мейкиндиги.

Abstract. The article analyzes the dynamics of changes in the volume of services of the market “telecommunications” and its correlation with the introduction of information and communication technologies. The analysis of data from licensed activities of telecom operators indicates that the introduction of new technologies, their high efficiency and indispensability in the daily life of society, as well as affordable prices due to high competition, provides progress in the introduction of innovative digital technologies, which also affects the reduction of other less demanded services.

Keywords: information and communication technologies, innovation, digital technologies, national information space, Internet.

Введение

В последние годы международное сообщество столкнулось с серьезными проблемами, включая пандемию коронавирусной инфекции (COVID-19) и вооруженные конфликты в нескольких регионах мира, что нарушает стабильность на мировой арене. Все эти факторы затормозили трансформационные процессы глобализации мира. Общеизвестно, что главным инструментом глобализации являются информационно-коммуникационные технологии (ИКТ), имеющие стремительное развитие и проникающие во все сферы жизни человеческого общества, как на национальном, так и международном уровнях, тем самым создавая условия для успешной интеграции развивающихся стран в глобальное информационное пространство [1].

1. Международная информационная безопасность Кыргызской Республики

Глобальные геополитические преобразования после развала Советского Союза кардинально изменили расстановку сил на мировой арене. Это в определенной степени относится и к Центральноазиатскому региону, который представляет собой часть дуги нестабильности и является областью столкновения интересов ряда государств мирового сообщества, благоприятной средой для проникновения и развития исламского фундаментализма, зоной формирования международных путей наркобизнеса. Тенденция развития межгосударственных отношений в Центральноазиатском регионе характеризуется, с одной стороны, стремлением к интеграции, с другой — прогрессирующей разобщенностью, вызванной конкуренцией в борьбе за выживание [2].

Изменение геополитической ситуации вызвало появление новых жизненно важных задач, от решения которых зависит судьба государства. В первую очередь, это связано с международной информационной безопасностью, влияющей на целенаправленные действия государства, обеспечение его выживания, функционирование и направление развития. Развитие современного общества характеризуется доминирующей ролью информационной сферы, которая представляет собой совокупность информации, информационной инфраструктуры, субъектов, осуществляющих сбор, формирование и использование информации, а также институтов регулирования возникающих при этом общественных и правовых отношений. Информационная сфера активно влияет на состояние политической и экономической, социальной и правовой, культурной и конфессиональной, оборонной и других составляющих безопасности страны. Формирование национального информационного пространства государства является необходимым условием вхождения его в глобальное информационное пространство. При этом национальная безопасность государства существенным образом зависит от обеспеченности его международной информационной безопасностью.

Международная информационная безопасность государства характеризуется состоянием защищенности его национальных интересов в глобальном информационном пространстве от угроз, связанных с применением информационно-коммуникационных технологий в военно-политической и иных сферах в целях подрыва (ущемления) суверенитета, нарушения территориальной целостности государства, осуществления в глобальном информационном пространстве иных действий, препятствующих обеспечению международного мира, безопасности и стабильности. Широкое распространение цифровых технологий несет в себе сопутствующие риски, в том числе угрозы для общества в целом, и соответственно, для общественного порядка в случае сбоя информационной инфраструктуры в результате кибератак или стихийных бедствий.

Использование возможностей глобального информационного пространства и устранение рисков, связанных с повсеместным внедрением цифровых технологий, диктует необходимость участия всех стран мира, всех заинтересованных сторон и секторов в регулировании вопросов международной информационной безопасности [5] *во имя мира, безопасности и стабильности*. В соответствии с Указом Президента РФ «Об утверждении государственной политики РФ в области международной информационной безопасности», международная информационная безопасность определяется следующим образом: «Международная информационная безопасность представляет собой такое

состояние глобального информационного пространства, при котором на основе общепризнанных принципов и норм международного права и на условиях равноправного партнерства обеспечивается поддержание международного мира, безопасности и стабильности» [6].

Геополитическое положение Кыргызстана определяется, прежде всего, его тупиковым расположением в регионе Евразии, отсюда и неблагоприятные условия для устранения внешней информационной угрозы со стороны сопредельных государств.

Уязвимым местом в плане международной информационной безопасности является и отсутствие естественных рубежей по всему периметру его внешних границ с соседними государствами, особенно на юго-западе страны.

Исторически сложившиеся обстоятельства в виде последствий непродуманного (искусственного) национально-территориального размежевания стран Средней Азии в период социализма привели к тому, что территория нашей республики с вкрапленными анклавами сопредельных государств, с иноэтническим населением не представляет собой компактное целостное государство. Кроме того, этнические кыргызы проживают по обе стороны границ с Республиками Таджикистан, Узбекистан и Китайской Народной Республикой.

Поэтому при малейшем обострении экстремистских настроений в соседних государствах или усилении сепаратистских тенденций у части некыргызского населения юго-запада республики (район Жалалабадской, Ошской и Баткенской областей и др.), в случае возникновения межэтнических, а тем более межгосударственных конфликтов, могут ослабить национальную, в том числе и международную информационную безопасность Кыргызской Республики [2].

2. ИКТ как источник угрозы международной информационной безопасности

В 2023 году самым значительным событием в глобальном информационном обществе стало появление в публичной сфере генеративного искусственного интеллекта. Развитие этих технологий представляет собой значительный шаг вперед с точки зрения темпов и масштабов ожидаемого влияния искусственного интеллекта на многие аспекты человеческой жизни, и может ознаменовать собой новый этап в развитии человечества. Возможности искусственного интеллекта и других цифровых инноваций, таких как квантовые вычисления, в плане преобразования различных аспектов экономической, социальной и культурной жизни общества вызывают одновременно интерес и опасения. Значительные увеличения вычислительной мощности искусственного интеллекта, позволяющие анализировать многочисленные массивы данных, как ожидается, будут способствовать развитию медицины, проектирования и разработки новых сложных технологических процессов, а также повысит эффективность предоставления услуг, делая реальными ранее невозможные процессы. Это может оказать положительное воздействие на рост благосостояния, процветания и содействовать достижению долгосрочного устойчивого развития общества.

Вместе с тем, результаты таких быстрых изменений неопределенны: они несут в себе новые возможности, также и риски и угрозы. Новые технологии могут использоваться как во благо, так и во вред, и при этом они могут стать инструментом в руках злоумышленников и лиц, стремящихся подорвать стабильность и доверие в глобальном информационном пространстве. Наблюдается повсеместная обеспокоенность, вызванная распространением применения искусственного интеллекта в различных сферах дея-

тельности и оказываемого им влияния на занятость населения. Возможности его применения в быту, коммерческой и государственной сферах также могут создать риски несанкционированного вторжения в частную жизнь, как и могут, поставить под вопрос защиту коммерческой и государственной тайны. Также не исключена возможность возникновения более глобальных угроз в случае, если человечество утратит контроль над искусственным интеллектом в сфере принятия решений в особо важных областях военно-политического управления или иных сферах деятельности человечества.

В последнее время ИКТ активно используются в террористических целях, в том числе для пропаганды терроризма и привлечения к террористической деятельности новых сторонников. Серьезной угрозой международной информационной безопасности стало использование ИКТ в преступных целях, в том числе для совершенствования преступлений в сфере компьютерных систем, а также для совершения различных видов мошенничества. Эта угроза особенно отчетливо проявилась после возникновения искусственного интеллекта с возможностью генерирования языковых моделей. В последнее время стремительно растет угроза кибератак, направленных на критические информационные ресурсы государств, в том числе на информационные системы и телекоммуникационные сети, критически важные для работы ключевые сферы жизнедеятельности государства и общества: здравоохранения, промышленности, связи, транспорта, энергетики, финансового сектора и городского хозяйства.

В процессе вхождения стран в глобальное информационное пространство зависимость успеха определенного государства от его отношения к ИКТ получило название «цифровой разрыв» и возникла связанная с ним проблема «цифрового неравенства». «Цифровой разрыв» между странами создает условия технологического доминирования отдельных государств в глобальном информационном пространстве, что дает возможность этим странам монополизировать рынок ИКТ. При этом доминирующие государства ограничивают доступность передовых цифровых технологий для развивающихся стран, тем самым усиливая их технологическую зависимость от доминирующих в сфере информатизации, провоцируя образование «информационного неравенства».

Внешняя составляющая информационной угрозы — это комплекс мер информационного воздействия с целью распространения идеологии другого государства и иноэтнического населения, теле- и радиопередач, демонстрирующих превосходство своего государства и осуждающих политическое, экономическое и социальное положение страны. Эти внешние информационные воздействия создают, на первый взгляд, правдоподобную обстановку, вынуждающую отдельные группы и слои населения, а также некоторые должностные лица принимать решения в ущерб собственным национальным интересам. Главная цель внешней информационной угрозы – это подготовка почвы для политического, экономического, идеологического и, в конечном счете, военного проникновения.

Чтобы понять значимость международной информационной безопасности страны, приведем следующие факты из мировой практики [2,3]. После победы СССР в Великой Отечественной войне, США и их союзники поняли, что СССР в «горячей» войне не победить. Чтобы овладеть его ресурсами необходимо вести против него «холодную» войну, т.е. информационную. Это была основа директивы Алена Даллеса, принятой 1948 году, и впоследствии преобразованной в Гарвардский проект [3]. Основная суть Гарвардского проекта заключается в

том, что ресурсы СССР, могут быть взяты за счет ведения против них информационной войны, в результате которой внедряется чужая идеология, разжигаются межнациональные розни, распространяются алкоголизм и наркомании, поддерживается безнравственность. Множество людей выступают на митингах, не понимая, что являются инструментом в руках злоумышленников. Промышленные и другие объекты страны продаются за бесценок. Все богатства страны переходят в руки злоумышленников с Запада. Причем хитрость информационной войны заключается в том, что свою страну мы продаем собственными руками. С одной стороны, наши соотечественники и международная глобальная мафия в лице транснациональных корпораций (ТНК) грабят страну; с другой стороны, наши соотечественники их охраняют; с третьей – обосновывают решения руководителей государства и ТНК научными теориями, экономической и исторической необходимостью; четвертые – вводят народ в заблуждение разными духовными движениями; пятые – спаивают и разлагают молодежь. Первый этап Гарвардского проекта закончился с распадом СССР и приватизацией основных объектов. На втором этапе произойдет окончательный передел собственности, переход всех ресурсов, предприятий, заводов в руки ТНК, уничтожение лишнего населения. По теории «золотого миллиарда» в мире должно остаться около 1 миллиарда элитных людей еще 1 миллиард обслуживает элиту и остальной 1 миллиард производит сырье, а остальные лишние 4,8 миллиарда людей должны умереть [2].

Стремление ТНК закрепить свое монопольное положение в сети Интернет и контролировать все информационные ресурсы за счет введения этими корпорациями (при отсутствии законных оснований и вопреки нормам международного права) цензуры и блокировки альтернативных интернет-платформ всё отчетливее становится угрозой для международной информационной безопасности.

Серьезной угрозой для международной информационной безопасности остается анонимность, которая обеспечивается за счет использования ИКТ, чтобы облегчить совершение преступлений, расширение возможностей для легализации доходов, полученных преступным путем, финансирование терроризма, распространение наркотических средств и психотропных веществ.

Безусловно, в качестве угрозы необходимо рассматривать повышенную уязвимость информационных ресурсов государства, включая объекты критической информационной инфраструктуры, к воздействию из-за рубежа, вследствие использования в стране иностранных информационных технологий, программных продуктов и телекоммуникационных оборудований.

Количество угроз постоянно растет пропорционально расширению возможностей использования цифровых технологий против международной информационной безопасности страны.

Поэтому противодействие нарастающим вызовам и угрозам, построение безопасной информационно-коммуникационной платформы государства становится приоритетной задачей для каждого суверенного государства.

3. **Эфирная (информационная) экспансия со стороны других государств**

С 2017 года Кыргызстан полностью перешел на цифровое вещание. Благодаря этому, у общества появилась возможность получить широкий спектр информации. Новый информационный порядок стал реальностью, так как трансграничная передача информации (спутниковое вещание, прямое телевизионное вещание, сети-Интернет) практически свели к нулю юрисдикцию государства даже в пределах собственного

информационного пространства. В то же время необходимо учитывать, что международная информационная безопасность представляет собой многогранное явление [4].

Согласно данным Министерства культуры, информации и туризма Кыргызской Республики на 2018 год, на территории республики на 80 отечественных телеканалов приходится 449 зарубежных.

На сегодняшний день законодательную базу информационного пространства страны определяют следующие Законы Кыргызской Республики:

- Закон, принятый в 2007 году, «О Национальной телерадиовещательной корпорации НТРК», в котором определено формирование единого информационного пространства;

- Закон «О телевидении и радиовещании», в котором определены программы формирования и развития информационной инфраструктуры;

- Закон «Об общественной телерадиокорпорации КР», в котором определены процессы интеграции в Глобальное информационное пространство.

В Закон «О телевидении и радиовещании КР» было внесено изменение и дополнение в связи с переходом на цифровое телерадиовещание.

Анализируя особенности и тенденции развития масс-медиа в период становления и развития суверенитета, а также на основе анализа концепции по данной проблеме, можно сделать следующие выводы [4]:

1. Кыргызстан все еще не обладает общенациональным телерадиовещанием международного уровня, подобно BBC, хотя одним из первых в Центральной Азии с 2010 года развивает службу общественного вещания, где присутствуют развитие, просвещение и постепенно формируется общественное самосознание высокого уровня;

2. В целях усиления международной информационной безопасности во всем мире наблюдается ограничение иностранного вещания на своих информационных пространствах, однако в Кыргызстане зарубежное телерадиовещание занимает более 70% кыргызского эфирного времени.

3. Поскольку каждый контент информации, идущий вразрез с концепцией информационной безопасности, должен рассматриваться как действие, направленное на подрыв национальной безопасности Кыргызской Республики, должна осуществляться экспертиза готовящихся законодательных актов, научно-технических и социально-экономических программ на предмет их соответствия задачам информационной безопасности страны.

4. **Обеспечение международной информационной безопасности в среде информационного обмена**

Бурное развитие Интернета сделало его в последние годы популярнейшим средством передачи данных и массовой коммуникации. По оценкам Международного союза электросвязи, доступ к Интернету сегодня имеет две трети населения Земли [7], и как отмечает Ассоциация GSM, только 5% населения мира все еще не охвачены сетью мобильной широкополосной связи, но при этом более 40% их них, не пользуются мобильным Интернетом [8].

Также рост доступности ИКТ сопровождается серьезными проблемами: «цифровым разрывом» и «цифровым неравенством» как внутри страны, так и между странами. Использование Интернета зависит от уровня экономического развития страны, и доля индивидуальных пользователей варьируется от 93% в странах с высоким уровнем дохода населения до 27% в странах с низким уровнем дохода, от 91% в Европе до 37% в странах Африки [9]. На количество и качество подключений и использования в разных странах также влияют такие фак-

торы, как ценовая доступность, грамотность и уровень образования. Достижение прогресса в обеспечении всеобщей, доступной и полноценной возможности подключения остается приоритетной задачей для того, чтобы страны не остались за бортом информационного общества.

С одной стороны, Всемирная паутина открывает богатейшие массивы информации, невиданные в истории человечества возможности самообразования и коммуникаций. С другой стороны, большую общественную опасность представляют Интернет – потоки лживой, провокационной и клеветнической информации, порнографические и так называемые черные сайты, пропаганда межрасовой, межнациональной розни, манипулирование общественным мнением.

Согласно Национальной стратегии развития Кыргызской Республики на 2018-2040 годы, утвержденной Указом Президента Кыргызской Республики от 31 октября 2018 года №221, в сфере информационной безопасности государство будет фокусироваться на критически важных направлениях, таких как обеспечение кибербезопасности информационно-коммуникационных технологий и информационных систем, создание системы реагирования на киберугрозы и киберинциденты, а также профилактика всех видов экстремизма и терроризма.

Согласно Концепции национальной безопасности Кыргызской Республики, утвержденной Указом Президента Кыргызской Республики от 9 июня 2012 года № 120, в связи с растущим использованием 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.

Поэтому соответствующим службам Кыргызской Республики необходимо, во-первых, вести борьбу с киберпреступностью, т.е. профилактику и пресечение преступных интернет технологий; во-вторых противодействовать использованию Глобальной сети для распространения экстремистских и террористских идей. В третьих, принять соответствующие нормативно-правовые акты для регулирования и обеспечения международной информационной безопасности Кыргызской Республики в сфере взаимодействия в глобальном информационном пространстве.

Заключение

В международных отношениях в области обеспечения международной информационной безопасности необходимо исходить из своих национальных интересов, действуя в соответствии с общепризнанными принципами и нормами международного права, а также вступившими в установленном законом порядке в силу международными договорами, участницей которых является Кыргызская Республика.

Для реализации целей межгосударственного сотрудничества в обеспечении международной информационной безопасности требуется актуализация взаимодействия Кыргызской Республики с международными организациями, занимающимися обеспечением международной информационной безопасности на мировом и региональном уровнях. Особое внимание следует уделить сотрудничеству со странами СНГ и государствами - членами ЕАЭС, ОДКБ и ШОС.

Основные направления международного сотрудничества Кыргызской Республики по вопросам обеспечения международной информационной безопасности формируют уполномоченные государственные органы.

Литература:

1. Доклад Генерального секретаря ООН. Экономический и Социальный Совет: Прогресс, достигнутый в осуществлении решений и последующей деятельности по итогам Всемирной встречи на высшем уровне по вопросам информационного общества на региональном и международном уровнях. https://undocs.org/ru/A/79/62.
2. Жайлообаев Н. Сборник: Проблема национальной безопасности Кыргызстана. Институт социально-политических технологий, Бишкек, 2006 г.
3. «Директива 20/1» - реальный план по уничтожению СССР (России). Часть 2». политики, (фотокопии документов).
4. Алымбаева З.А., Алимахунов А. Особенности и тенденции современного информационного пространства Кыргызстана // Бюллетень науки практики. 2021. Т.7.№2. с.271-275. https://doi.org/10.33619/2414-2948/63/29
5. Бойко С. Материалы конференции «Kuban CSC-2022».Международная информационная безопасность: новые вызовы и угрозы. .
6. Указ Президента РФ. 12.04.2021. №213. «Основы государственной политики РФ в области международной информационной безопасности». https://static.kremlin.ru
7. Пресс-релиз Международного союза электросвязи (МСЭ) от 12 сентября 2023 года, в рамках цели «Достижение всеобщей и значимой цифровой связи». https://www.itu.int/en/mediacentre/Page/PR-2023-09-12-universal-and-meaningful-connectivity-by-2030.aspx.
8. Отчёт «О состоянии мобильной интернет-связи за 2023 год» Ассоциации GSM операторов связи. https://www.gsma.com/r/somic/.
9. Отчёт МСЭ «Измерение цифрового развития - факты и цифры 2023 года». https://www.itu.int/hub/publication/d-ind-ict_mdd-2023-1/.