

УДК 342.7(575.2)(04)
DOI 10.53473/16946324_2023_3

Жуматаева М.Т.
Преподаватель кафедры Правоведение
Бишкекский инновационный колледж,
магистрант 1 курса ВШМ
Жуматаева М.Т.
Юриспруденция кафедрасынын окутуучусу
Бишкек инновациялык колледжи,
ЖММдин 1-курсунун магистранты
Zhumataeva M.T.
Lecturer of the Department of Jurisprudence
Bishkek Innovation College,
1 nd year master 1 student of the Graduate School of Masters
of the International University of the Kyrgyz Republic
mobile phone: +996 777 66 18 27

Н.Чыныбаева,
КРЭАУнин Эл аралык кызматташтык жана
политология кафедрасынын ю.и.к., доцентинин м.а.,
Н.Чыныбаева,
к.ю.н., и.о.доцента кафедры Международного,
предпринимательского права и политологии МУКР
Chynybaeva N.,
Candidate of Law, Acting Associate Professor
of the Department of International,
Business Law and Political Science,
International University of the Kyrgyz Republic
mobile phone: +996(559)101842
e-mail: Chynybaeva.nurgul.j@gmail.com

**МААЛЫМАТТЫК КООПСУЗДУКТУН МААЛЫМАТТЫК ЖАНА УКУКТУК
НЕГИЗДЕРИНИН ЖАЛПЫ ТҮШҮНҮГҮ**

**ПРАВОВАЯ ОСНОВА ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ:
ТЕОРЕТИЧЕСКИЙ АСПЕКТ**

**GENERAL CONCEPT OF INFORMATION AND LEGAL BASIS OF INFORMATION
SECURITY**

Аннотация: Бул илимий изилдөөдө маалыматтык коопсуздуктун укуктук негизинин жалпы түшүнүгү каралды, анткени информатизация адамзат цивилизациясынын жашоосунда анын тарыхындагы эң терең өзгөрүүлөрдүн бирин жаратты. Автор ошондой эле акыркы он жылдыкта маалыматтык-коммуникациялык технологиялар коомдун өнүгүшүнө таасир этүүчү маанилүү факторлордун бири болуп калганын жана адам шимердүүлүгүнүн бардык чөйрөлөрүн маалыматташтыруу бүгүнкү күндө коомдун маанилүү милдети жана социалдык өнүгүүнүн императиви катары чыгып жатканын эске алып, маалыматтык коопсуздук түшүнүктөрүн ачууга аракет кылган.

Негизги сөздөр: маалыматтык коопсуздук, маалыматтык коопсуздуктун укуктук негиздери, интернет, кибер коопсуздук, интернет гигиена, массалык маалымат каражаттары, жоопкерчилик.

Аннотация: В данной научной исследовании были рассмотрены общее понятие правовой основы информационной безопасности так как, информатизация произвела в жизни

человеческой цивилизации одно из самых глубоких изменений за всю ее историю. Также автор попыталась раскрыть понятия информационной безопасности учитывая, что, в последнее десятилетие информационно-коммуникационные технологии стали одним из важнейших факторов, влияющих на развитие общества, а информатизация всех сфер человеческой деятельности выступает сегодня как важнейшая задача общества и как императив социального развития.

Ключевые слова: информационная безопасность, правовые основы информационной безопасности, интернет, кибербезопасность, интернет гигиена, средства массовой информации, ответственность.

Abstract: *In this scientific study, the general concept of the legal basis of information security was considered, since the reformatization produced one of the most profound changes in the life of human civilization in its entire history. The author also tried to reveal the concept of information security, taking into account that in the last decade information and communication technologies have become one of the most important factors affecting the development of society, and informatization of all spheres of human activity acts today as the most important task of society and as an imperative of social development.*

Keywords: *information security, legal foundations of information security, Internet, cyber-security, Internet hygiene, mass media, responsibility.*

Ни для кого не секрет что, в настоящее время происходит переход от индустриального общества к информационному. Труд человека делается в меньшей степени физическим, в большей — интеллектуальным, точнее сказать больше направленный на систематизацию виде электронизации (гугл дисках, облаках, носителях информации и т.д.). Современный человек должен свободно ориентироваться в постоянно растущем потоке информации, уметь работать с ней и в тоже самое время сортировать полученную информацию.

Самым распространённым усилителем интеллектуальных способностей за всю историю развития цивилизации является глобальные сети. При этом информатизация образования является необходимым условием развития такого общества, которое в последние годы невозможно представить без использования ресурсов сети Интернет. Мир образования наполняется сетевыми сервисами и цифровыми ресурсами, количество которых с каждым годом стремительно увеличивается.

В современных условиях активной модернизации системы образования изменяется и педагогическая, научная деятельность. Образование как важнейшая часть жизни человека должно обеспечивать ему возможность ориентироваться в потоке информации, позволить комфортно чувствовать себя в информационном обществе, легко адаптироваться к новым тенденциям. Исходя из вышеизложенного, можно сказать что, информационная безопасность – это степень защиты информации от внутренних и внешних угроз, которые способны причинить вред интересам личности (общества) или государства (национальным интересам).

А что касается правовых основ информационной безопасности то, можно говорить, как специальный курс, который изучает правовые нормы и регулирует отношения в области информационной безопасности.

Кроме того, информационная безопасность является сравнительно молодой наукой в разрезе с остальными науками. Информационная безопасность обуславливает свою актуальность тем, что свое развитие она получила в связи с бурным развитием информационных технологий, радиоэлектроники и связи и необходимостью сохранения информационных ресурсов. Как и любая другая наука, информационная безопасность имеет свой понятийный аппарат, который способен наиболее точно охарактеризовать все аспекты защиты информации. Многие понятия по своему содержанию соответствуют зарубежным аналогам. В то же время некоторые термины не являются устоявшимися и не всегда точно и полно характеризуют какой-либо процесс, свойство или предмет.

Следует учесть, что на формирование безопасной среды напрямую влияют такие факторы, как вопросы безопасности и их решение, определяющиеся актуальными факторами. В современности, средства связи – актуальные в 20-веке, устарели и усовершенствовались до такой степени, что их разновидность и формы использования составили совершенно новую информационную среду, требующая от правительственных органов, как тщательного изучения всевозможных аспектов этой среды, так и разработки мер быстрого восстановления на любые нарушения ее целостности. Выполнение этой задачи требует от правительственных органов комплексного подхода, который немалозначим без единого информационного поля и частого взаимодействия в его просторах с зарубежными странами по вопросам координации деятельности в области обеспечения информационной безопасности. По словам Семенова Н.С.: «Информационная безопасность при вхождении в информационное общество становится главным элементом политики государства, которое должно вводить необходимые способы защиты на законодательном уровне. Само собой существуют определенные нормативные правовые акты (далее НПА), политические документы, рекомендации, направленные на выработку единой целостной информационной системы страны» [1].

В Кыргызстане уже не первый год стоит остро вопрос цифровизации на всех уровнях. Это важный вопрос для того, чтобы страна успевала шагать в ногу со временем и не отставала в развитии от других стран. За последние несколько лет был решен ряд первоочередных задач в области цифровизации, частично переведен документооборот в цифровую сферу, запущены различные социальные проекты. Но фактически это лишь начало и впереди множество работы.

Цифровизация важна не только для социальной жизни страны, она решает множество актуальных проблем – интеграция в мировые экономические и социальные процессы, борьба с коррупцией.

Главная цель цифровизации — это реформирование и улучшение государственного аппарата: оптимизация количества чиновников в госуправлении, борьба с бюрократизмом, казнокрадством, взяточничеством и коррупцией.

Цифровизация (digitalization) — это переход к новым процессам, моделям и подходам, основанным на информационных технологиях. Появление мессенджеров и видеосвязи, внедрение концепции «умного города», замена бумажного документооборота электронным, поход по магазинам — заказами через интернет, визитов к врачу — медицинскими онлайн-консультациями — все это частные примеры цифровизации.

Сегодня цифровизация — фундаментальный технологический тренд, который затрагивает как все сектора экономики (от креативных индустрий до горнодобывающей промышленности и сельского хозяйства), так и практически все сферы жизни общества, вплоть до уровня человеческой культуры в целом.

При этом необходимо отметить, что в межгосударственных отношениях нарастает тенденция использования информационного давления как действенного механизма к большой конкуренции. Использование все возможных средств информационной пропаганды и информационной экспансии стало неотъемлемым инструментом решения крупных социальных, экономических и политических конфликтов. Развитые страны мира, имеющие возможность осуществления глобального мониторинга распространяемой информации, используют его результаты для получения односторонних преимуществ в политических, экономических, военных, экологических и прочих аспектах межгосударственных отношений. [2]

Усиливается роль и влияние глобальных средств массовой информации и коммуникационных механизмов на развитие экономической, политической и социальной ситуации в различных странах мира. Фундаментальные перемены, произошедшие в последние годы в странах с различными экономическими и политическими условиями, указывают на ключе-

вую роль в данных процессах новых технологий управления массами, в том числе посредством использования информационно-коммуникационных технологий: сайтов, социальных сетей и мобильных приложений.

Широкое использование населением Кыргызстана возможностей сети Интернет создает предпосылки их использования для оказания целенаправленного воздействия на внутривнутриполитическую ситуацию в ущерб национальным интересам республики.

Уровень проникновения сети Интернет среди населения республики, по состоянию на конец III квартала 2018 года, составил примерно 80,4%, в 2017 году - 75,8%.

В связи с открытостью национального информационного пространства и популярностью зарубежных средств массовой информации, в том числе телевидения и интернет-ресурсов (почтовых служб, социальных сетей, блогов и видеопорталов), появляется реальная угроза информационного влияния на общественное сознание населения.

Для противодействия подобному манипулированию общественным сознанием требуется серьезно улучшить эффективность государственной информационной политики, увеличить открытость государственных органов, повысить обеспеченность права граждан на информацию.

Серьезные угрозы несет в себе проблема неконкурентоспособности отечественного контента. Его качество остается недостаточным для полноценной конкуренции с иностранным информационным продуктом. В условиях открытости национального информационного пространства это приводит к непопулярности отечественного продукта. В свою очередь, низкая популярность не позволяет привлечь значимые инвестиции в его производство, что приводит к крайней недостаточности производства отечественного контента.

Все также накаливается вопрос о совершенствовании программ по подготовке квалифицированных кадров в сфере информационной безопасности. Требуется дальнейшее совершенствование процессов и подходов к обучению, повышение квалификации специалистов государственных органов, организаций, занятых в сфере обеспечения информационной безопасности.

Нынешнее состояние правового обеспечения противодействия информационным преступлениям также характеризуется недостаточной согласованностью используемых правовых механизмов, фрагментарностью деятельности субъектов законодательной инициативы по их развитию и совершенствованию, недостаточной эффективностью, противоречивостью правовых норм.

Согласно Национальной стратегии продвижения КР на 2018-2040 годы, утвержденной Указом Президента КР с 31 октября 2018 года № 221, [3] 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.

Информационная безопасность в системе национальной безопасности Кыргызской Республики в настоящее время все еще актуальны, учитывая риски и угрозы внешних и даже внутренних сторон. Рассматривая структуру национальной безопасности страны, мы изучаем постоянное изменение геополитического окружения, оказывающее на нашу страну огромное влияние и требующее от правительства страны соответствующих и оперативных мер, направленных на обеспечение безопасности общества и государства. Именно такая комплексная безопасность и является защищенностью интересов и каждого гражданина, и всего народа и государства в целом, так как собранная информация на базе серверов государства слабо защищена.

В настоящее время вопрос международного сотрудничества в области обеспечения информационной безопасности стоит остро, так как достижение науки и техники в области информационно-коммуникационных технологий (ИКТ) как никогда определяют динамику экономического развития, уровень благосостояния и конкурентоспособности государств в мировом сообществе, а также степень их национальной безопасности.

Развитие ИКТ играет важнейшую роль для экономического и социально-политического развития как каждой страны в отдельности, так и человечества в целом. Однако развитие ИКТ не только создает возможности для роста и развития, но и порождает угрозы международной и национальной безопасности. Межгосударственное противоборство, перешедшее в информационную сферу, чревато конфликтами, крайней формой проявления которых могут стать информационные войны [4]

Международная информационная безопасность сегодня определяется как «состояние угрозы безопасности государств и мирового сообщества в информационном пространстве».

Таким образом, проблема обеспечения информационной безопасности не является сегодня узко государственной категорией, а переходит в область международных проблем, для решения которых требуется объединение ведущих мировых держав.

Международное сотрудничество – одно из важных направлений деятельности Кыргызской Республики по обеспечению защиты национальных интересов в области информационных технологий, электросвязи и почты, включая международно-правовую защиту частотных присвоений радиоэлектронным средствам связи. Сотрудничество в этой сфере ведется по двум направлениям: взаимодействие с другими странами (двухстороннее сотрудничество) и взаимодействие с международными и региональными объединениями, такими как ШОС, Таможенный союз и другие.

Государства активно сотрудничают в области обмена информацией и связи, включая радиовещание, телевидение, распространение печатной и звуковой продукции. Имеется несколько десятков международных специальных соглашений в этой сфере, в большинстве из которых Кыргызская Республика участвует: Женевская конвенция об использовании радиовещания в интересах мира 1936 г., Международная конвенция электросвязи (в редакции 1991 г.), Конвенция о международном обмене изданиями и правительственными документами 1958 г., Конвенция о распоряжении несущих программ сигналов, передаваемых через спутники, 1974 г., [5] соглашения об обмене правовой, экономической информацией, информацией в сфере внешнеэкономической деятельности.

В соответствии с соглашениями субъектами международного информационного обмена могут быть как государства, так и органы государственной власти, и органы местного самоуправления, так и физические и юридические лица. Объектами международного информационного обмена являются: документированная информация, информационные ресурсы, информационные продукты, информационные услуги и др. Тенденция развития международного сотрудничества в области информации и связи свидетельствуют о формировании в международном праве новой отрасли, которую можно обозначить как международное информационное право.

В современном мире все сферы жизнедеятельности находятся в прямой зависимости от работы вычислительных и информационных сетей. Вместе с тем «широкое использование для обработки информации средств вычислительной техники с программным обеспечением, позволяющим сравнительно легко модифицировать, копировать и разрушать информацию» повышает уязвимость информационного пространства. Пользователи информационных систем «без достаточных к тому оснований верят в отсутствие кибератак, используя информационное пространство с незнанием ограничений и угроз безопасности системы». [6]

В наше время, информация выступает важнейшим компонентом развития общества. Превращение постиндустриального общества в общество информационное означает, что информация приобретает глобальный характер, становится значимой как для человека лично, так для государства и общества в целом, каждый может искать, получать, передавать, производить и распространять информацию любым законным способом, не существует границ для ее потока. В настоящий момент информация признается одной из важнейших ценностей, соответственно, ее защита представляет собой не менее важную деятельность, чем ее получение и передача, следовательно, в «дигитализированном обществе начала XXI в.

сфера проявления риска меняется». Например, «революционные события так называемой Арабской весны в мировом экспертном, медийном и политическом дискурсе оказались неразрывно связаны с ролью информационно-коммуникационных технологий. Беспрецедентная скорость распространения информации через интернет (в основном через социальные сети) сыграла против режимов, стремившихся скрыть свои репрессивные акции от международного сообщества и не владевших адекватными навыками ведения информационной борьбы» [7]. В настоящее время тенденции глобализации усиливаются, причем всё очевиднее те проблемы, к которым она приводит. В этих условиях актуализируется вопрос об участии всех партнеров системы мирового правопорядка в борьбе с негативными проявлениями, вызванными глобализационными процессами, в том числе транснациональной киберпреступностью. Очень важно понимать глобальность проблемы киберпреступности. Так, уже сейчас кибератаки парализуют работу не только частных структур, но и государственных органов, в мире не существует государства, которое было бы защищено от подобного рода атак. В качестве вероятных источников киберугроз рассматриваются не только хакеры или их группы, но также отдельные государства, террористические, преступные группировки.

Список использованной литературы

1. Семенов Н.С. Правовые особенности информационной безопасности КР. // [Текст] Н.С. Семенов. Вестник МУК, №2. Бишкек. 2022. –С-89
 2. Электронный ресурс. Точка доступа: https://www.president.kg/ru/sobytiya/23281_prezident_sadirghaparov_cifrovizaciya_glavniy_trend_segodnyashnego_globalnogo_razvitiya. –Загл экрана
 3. УКАЗ от 31 октября 2018 года УП № 221 «О Национальной стратегии развития Кыргызской Республики на 2018-2040 годы»
 4. Зиновьева Е. Международное сотрудничество по обеспечению информационной безопасности: // Е.Зиновьева. [Текст]: конспект лекций. – М. 2015. С.18.
 5. Концепция информационной безопасности Кыргызской Республики на 2019-2023 годы [Электронный ресурс]: // Информационно-правовая система «ТОКТОМ мамлекет Про». – Режим доступа: http://www.toktom.kg/?comp=main&m_t=1. – Загл. с экрана;
 6. Сачков Д.И. Обеспечение информационной безопасности в органах власти: учеб. пособие / Д.И.Сачков, И.Г. Смирнова.- Иркутск :Изд-во БГУЭП, 2015. С. 74.
- Демидов О. Обеспечение международной информационной безопасности и российские национальные интересы / О. Демидов / Индекс Безопасности. - № 1 (104).-С.129.