УДК 340.132:004.056
DOI: 10.36979/1694-500X-2024-24-3-101-106

ПРАВОВОЕ ОБЕСПЕЧЕНИЕ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

Н.А. Сейдакматов

Аннотация. Проведен анализ нормативно-правовой базы по правовому регулированию информационной безопасности Кыргызской Республики. Отмечено о том, что проблема обеспечения информационной безопасности является самой острой проблемой в мире, и с развитием информационных технологий параллельно появляются новые угрозы, которые могут привести к глобальным катастрофическим последствиям. Сказано о том, что вся деятельность по урегулированию и обеспечению информационной безопасности должна основываться на следующих положениях: законность, баланс интересов государства, субъектов и неотвратимость применения меры наказания.

Ключевые слова: информационная безопасность; регулирование информационной безопасности; обеспечение информационной безопасности; защита прав и интересов человека; защита личной и семейной тайны; законы Кыргызской Республики.

МААЛЫМАТТЫК КООПСУЗДУКТУ УКУКТУК КАМСЫЗДОО

Н.А. Сейдакматов

Аннотация. Макалада Кыргыз Республикасынын маалыматтык коопсуздугун укуктук жөнгө салуу боюнча ченемдик-укуктук базага талдоо жүргүзүлдү. Маалыматтык коопсуздукту камсыз кылуу көйгөйү дүйнөдөгү эң курч көйгөй болуп санала тургандыгы жана маалыматтык технологиялардын өнүгүшү менен параллелдүү түрдө глобалдык катастрофалык кесепеттерге алып келиши мүмкүн болгон жаңы коркунучтар пайда болору белгиленди. Макалада, маалыматтык коопсуздукту жөнгө салуу жана камсыздоо боюнча ишмердик төмөндөгү жоболорго: мыйзамдуулукка, мамлекеттин, субъектилердин кызыкчылыктарынын теңдигине жана жаза чарасын колдонуунун кепилдигине негизделиши керектиги айтылган.

Түйүндүү сөздөр: маалыматтык коопсуздук; маалыматтык коопсуздукту жөнгө салуу; маалыматтык коопсуздукту камсыздоо; адам укуктары менен кызыкчылыктарын коргоо; жеке жана үй-бүлөлүк сырды коргоо; Кыргыз Республикасынын мыйзамдары.

THE LEGAL SUPPORT OF INFORMATION SECURITY

N.A. Seydakmatov

Abstract. The article conducts the analysis of the legal and regulatory framework for the legal regulation of information security in the Kyrgyz Republic. It is noted that ensuring information security is the most pressing issue globally, and with the advancement of information technologies, new threats emerge in parallel that may lead to global catastrophic consequences. The article emphasizes that all activities related to the regulation and provision of the information base should be based on the following principles: legality, balance of interests between the state and subjects, and the inevitability of applying punitive measures.

Keywords: information security; regulation of information security; ensuring information security; protection of human rights and interests; protection of personal and family privacy; laws of the Kyrgyz Republic.

Правовое регулирование информационной безопасности осуществляется за счет создания, реализации нормативно-правовых актов, а также осуществления контроля исполнительными органами, которые регулируют практическую деятельность по обеспечению защиты информации личности, общества и государства в целом.

Правовое регулирование информационной безопасности нацелено на обеспечение защиты прав и интересов человека, защиту его личной и семейной тайны, а также защиты чести и достоинства. Кроме того, каждое государство обязано обеспечивать благоприятные условия для того, чтобы каждый его гражданин мог своевременно и открыто получать доступ к незапрещенным видам информации от муниципальных и государственных органов. Государства обязаны обеспечивать защиту авторских прав, защиту прав участников электронной коммерции, защиту самой информации, представляющей государственную тайну при использовании государственных информационных ресурсов и т. п.

Но и нельзя забывать, что нарушение обеспечения информационной безопасности влечет за собой применение карательных мер в отношении нарушителей.

В настоящее время, проблема обеспечения информационной безопасности является самой острой проблемой в мире, так как применение информационных ресурсов и информационных систем в различных сферах жизни человечества показывает, что есть угроза потери существующих данных и информации, которая в последующем может нанести большой ущерб материального и иного характера.

Нынешний этап развития информационных технологий характеризуется возможностью массового информационного воздействия на индивидуальное и общественное сознание вплоть до проведения крупномасштабных информационных войн, в результате чего неизбежным противовесом принципу свободы информации становится принцип информационной безопасности (ИБ) [1]. Этот принцип обусловлен глобальной информационной революцией, стремительным развитием и повсеместным внедрением новейших информационных технологий и глобальных средств телекоммуникаций. Проникая во все сферы жизнедеятельности государств, информационная революция расширяет возможности развития международного сотрудничества, формирует планетарное информационное пространство, в котором информация приобретает свойства ценнейшего элемента национального достояния, его стратегического ресурса [2].

Вместе с тем, становится очевидным, что наряду с положительными моментами такого процесса создается и реальная угроза использования достижений в информационной сфере, в целях, не совместимых с задачами поддержания мировой стабильности и безопасности, соблюдением принципов суверенного равенства государств, мирного урегулирования споров и конфликтов, неприменения силы, невмешательства во внутренние дела, уважения прав и свобод человека. Опасным источником угроз является растущая отечественная и международная компьютерная преступность.

Мировое сообщество признало международную информационную безопасность как глобальную проблему, как необходимое условие существования человеческого сообщества [3]. В этой связи требуется выработка общих принципов и общего понимания всего комплекса проблем, связанных с информационной безопасностью, начиная с понятийного аппарата, научных и методических концепций и заканчивая практическим решением стоящих задач.

С развитием информационных технологий параллельно появляются и новые угрозы, которые могут привести к глобальным катастрофическим последствиям. И данную проблему можно будет решить, только если страны объединятся для решения данной проблемы. В связи с этим, нужно упомянуть международные договоры в сфере информационной безопасности, такие как: Соглашение о сотрудничестве государств-участников Содружества Независимых Государств в области обеспечения информационной безопасности от 20 ноября 2013 г.; Постановление Межпарламентской Ассамблеи государств-участников Содружества Независимых Государств от 18 ноября 2005 г. № 26-7 «О гармонизации законодательства государств-участников СНГ в области информатизации и связи»; Постановление Межпарламентского комитета Республики Беларусь, Республики Казахстан, Кыргызской Республики, Российской Федерации и Республики Таджикистан от 15 октября 1999 г. № 9-9 «О модельном законе "О безопасности"» и т. д.

В статье 33 Конституции Кыргызской Республики от 5 мая 2021 года сказано,

что каждому гражданину гарантируется право свободно искать, получать, хранить, использовать информацию и распространять ее устно, письменно или иным не запрещенным законом способом, а также каждый гражданин имеет право получать сведения о себе как в местном самоуправлении, так и в государственных органах и иных организация [4]. Также каждый гражданин Кыргызской Республики имеет право получать сведения в рамках законодательства о работе государственных органов и органов местного самоуправления и их должностных лиц [5].

При создании структуры в области обеспечения информационной безопасности в первую очередь нужно сгруппировать правовые нормы по отраслям законодательства. Например, это могут быть нормы, относящиеся к применению ответственности за нарушения законодательства в сфере информационной безопасности.

В Гражданском кодексе Кыргызской Республики содержатся нормы, которые рассматривают вопросы относительно коммерческой и служебной тайны, которые закрепляют такие формы отношений, как электронная подпись, с помощью которой подтверждают свою ответственность за использование информации, и информационные услуги.

В Уголовном кодексе Кыргызской Республики от 28 октября 2021 года № 127 в статье 227 прописывается ответственность за незаконное получение информации, составляющей коммерческую или банковскую тайну, а в статье 228 прописана ответственность за незаконное разглашение или использование сведений, составляющих коммерческую, банковскую тайну или тайну сведений налогоплательщика без его ведома.

В Кодексе Кыргызской Республики о правонарушениях от 28 октября 2021 года № 128 в прописывается мера ответственности за правонарушения в сфере информации: незаконное разглашение коммерческой, банковской тайны, тайны налогоплательщика без его согласия (статья 323); недобросовестное использование служебной информации (статья 333); предоставление недостоверной (ложной) информации или документов либо отказ предоставить информацию или документы должностному лицу государственных органов, осуществляющих контроль за деятельностью на рынке ценных бумаг (статья 334); нарушение порядка раскрытия информации (статья 338) и др.

Основными законами в сфере информационной безопасности являются законы Кыргызской Республики «О защите государственных секретов Кыргызской Республики» от 15 декабря 2017 года № 210 (15); «Об электронном управлении» от 19 июля 2017 года № 127; «О гарантиях и свободе доступа к информации» от 5 декабря 1997 года № 89; «О Национальном архивном фонде» от 22 ноября 1999 года № 125; «Об электрической и почтовой связи» от 2 апреля 1998 года № 31; «Об электронной цифровой подписи» от 19 июля 2017 года № 128; «О средствах массовой информации» от 2 июля 1992 года № 938-XII; «О правовой охране программ для ЭВМ и баз данных» от 30 марта 1998 года № 28; «Об основах технического регулирования в Кыргызской Республике» от 22 мая 2004 года № 67; «О доступе к информации, находящейся в ведении государственных органов и органов местного самоуправления КР» от 28 декабря 2006 года № 213 и другие подзаконные акты.

Изучив классификацию законодательства в области информации и обеспечения информационной безопасности, можно сделать вывод, что система законодательства включает в общем нормы как конституционного, так и административного, уголовного и гражданского отраслей права [6]. И вся деятельность по урегулированию и обеспечению информационной безопасности должна основываться на следующих положениях: законность, баланс интересов государства и субъектов, а также неотвратимость применения меры наказания [7].

Усовершенствование нормативно-правовой базы в сфере информационной безопасности, для восполнения пробелов является обязательной мерой для формирования информационного общества в Кыргызской Республике [8]. Вопросы, связанные с информацией, информационными отношениями, а также обеспечение информационной безопасности регулируются и охраняются нормами как гражданского, так и административного и уголовного законодательства.

Касаясь безопасности работы информационных технологий, необходимо отметить, что Кыргызская Республика, как и все страны постсоветского пространства, вошла в информационное пространство начиная с 90-х годов, когда открылась возможность применения информационной техники, когда цены на нее стали доступными не только предприятиям и учреждениям, но и отдельным гражданам. На сегодняшний день отрасли программного и аппаратного обеспечения компьютеров являются одним из особо динамично растущих секторов развития экономики каждого государства.

Развитие информационных технологий в настоящее время создали и новые общественные отношения, которые уже начали нуждаться в их урегулировании. Ведь новые информационные технологии не только дали возможность развиваться обществу, но также намного облегчили возможности развития преступности. В настоящее время в некоторых странах специалисты, которые имеют техническое образование, из-за нестабильности очень часто не востребованы и поэтому иногда уходят на другой путь, к сожалению, в путь преступной деятельности и начинают хорошо зарабатывать и добиваться определенных «успехов» [9].

Если говорить об информационной безопасности, то можно отметить, что во всех странах в работе государственных органов, предприятий, коммерческих банков существуют уязвимые стороны, которые притягивают злоумышленников. Поэтому распространение и развитие сетей и компьютерных систем идут рядом с ростом преступлений, которые связаны с кражей, незаконным доступом к памяти компьютеров, модификацией и т. д. [10].

Закон Кыргызской Республики «Об электронном управлении», впервые на законодательном уровне определяет понятие «защита информации». Итак, под защитой информации понимаем комплекс организационных, правовых и технических мер, которые определяют его подлинность, целостность, доступность, конфиденциальность и обеспечение защиты информации [11].

Основными целями обеспечения защиты информации являются: обеспечение защиты национальной безопасности страны; обеспечение защиты персональных данных граждан, которые находятся в информационных системах; обеспечение защиты данных о частной и семейной жизни граждан; обеспечение защиты прав граждан при использовании ими информационных сетей, систем и технологий, а также создания и применения информационных ресурсов и иных неправомерных действий.

Таким образом, к правовым мерам по обеспечению защиты информации можно отнести заключаемые договора между лицами, которые обладают определенной информацией, и лицами, которые используют эту информацию, где устанавливаются четкие условия пользования информацией и, в случае чего, могут быть применены соответствующие меры ответственности [12].

Заключение. Актуальность совершенствования правовых норм и законодательства Кыргызской Республики в сфере информационной безопасности не вызывает сомнений. Об этом свидетельствуют темпы глобализации научно-технического прогресса и распространения информационно-телекоммуникационных технологий.

Необходимо отметить, что особенностью развития отечественной нормативно-правовой базы в сфере информационной безопасности является отсутствие комплексного подхода к проблеме информационной безопасности, а также недостаточно полный учет международного опыта и методологии разработки нормативной правовой базы в области информационной безопасности. Резюмируя сказанное выше, хочется подчеркнуть, что дальнейшее развитие, обновление информационного законодательства Кыргызской Республики с учетом общепризнанных принципов и международных правовых норм в сфере информационной безопасности невозможно без теоретической проработки принципиальных вопросов, связанных с правовой спецификой информации. Вряд ли целесообразно разрабатывать все новые законодательные акты по специальным вопросам, без уточнения общих принципов регулирования и применяемого понятийного аппарата, без решения иных проблем теоретического характера.

Актуальным является то, что современные условия требуют и определяют необходимость комплексного подхода к формированию законодательства в сфере информационной безопасности, его состава и содержания, соотнесения его со всей системой международных правовых норм и правовых актов Кыргызской Республики включая международные стандарты по информационной безопасности.

На современном этапе развития и применения информационных технологий востребованным является проблема защиты общества от их использования в преступных целях. Преступность в сфере высоких технологий не имеет границ и представляет угрозу международной безопасности. Необходимо содействовать предотвращению использования информационных ресурсов и технологий в преступных и террористических целях, соблюдая при этом права человека.

Следует отметить, что в нашей стране интересы государства и общества в информационной сфере, включая информационную безопасность, заключаются в обеспечении интересов личности в этой сфере и создании условий для реализации конституционных прав и свобод граждан. При этом, вся система нормативного правового обеспечения безопасности в информационной сфере должна строиться на основе соблюдения конституционных норм о неприкосновенности частной жизни.

Развитие и дальнейшее совершенствование законодательства в сфере обеспечения информационной безопасности Кыргызской Республики связано с разработкой новых нормативно-правовых актов, направленных на восполнение пробелов в правовом регулировании общественных отношений в сфере информационной безопасности, особенно с введением в информационную сферу новых понятий, применяемых в информационно-телекоммуникационных технологиях, а также в связи с подписанием Кыргызстаном соответствующих международных нормативных правовых актов.

Задача гармонизации национальных и международных стандартов в сфере информационных технологий проводится с целью повышения уровня обеспечения безопасности информационных технологий и информационных ресурсов каждого государства. Только при наличии единых критериев оценки безопасности информационных технологий может существовать доверие к разрабатываемым и распространяемым продуктам и системам информационных технологий, только при этих условиях возможно признание результатов сертификации современных продуктов и систем информационных технологий, проведенной различными органами по сертификации за рубежом и в Кыргызской Республике.

Резюмируя, отметим, что положительный эффект обеспечения информационной безопасности достигается в основном за счет применения соответствующих международных стандартов, которые являются механизмами реализации нормативных правовых актов.

Поступила: 13.11.23; рецензирована: 27.11.23;
принята: 29.11.23.

Литература

1. *Жумабаев У.С.* Кыргыз Республикасынын Улуттук коопсуздук мамлекеттик комитетинин конституциялык-укуктук макамы / У.С. Жумабаев. Бишкек: «Улуу тоолор», 2022.
2. *Акунов А.* Кыргызстан в эпоху независимости (1991–2022) / А. Акунов, А. Темирбекова // Формирование новой политической системы: Синдром авторитаризма. Бишкек, 2023.
3. *Кольбаева А.Р.* Сборник процессуальных актов для сотрудников ГКНБ Кыргызской Республики / А.Р. Кольбаева, Н.Б. Сальпиев. Бишкек, 2022.
4. *Оторова Б.К.* Правовое регулирование информационно-правовых отношений в Кыргызской Республике / Б.К. Оторова. Бишкек, 2012.
5. Практическое руководство по выявлению, расследованию и судебному рассмотрению преступлений, совершаемых с использованием сети Интернет и электронных информационных ресурсов (социальные сети, мессенджеры и другие ресурсы). Бишкек, 2022.
6. *Павленко С.З.* Новая концепция безопасности и проблемы организационного проектирования органов безопасности страны в современных условиях: научный доклад / С.З. Павленко. М., 1992.; *Тимошенко А.С.* Международный контрольный механизм в системе экологической безопасности / А.С. Тимошенко // Государство и право. 1992. № 12.

7. *Поздняков А.И.* Информационная безопасность / А.И. Поздняков // Безопасность. М., 1992. № 6.
8. *Лесков М.А.* Гомеостатические процессы и теория безопасности / М.А. Лесков // Безопасность. М., 1994. № 4.
9. *Спиридонова В.И.* Безопасность и проблема ассимиляции политической ценности мира / В.И. Спиридонова // Проблемы безопасности и устойчивости социально-политического развития российского общества М.: Центр социальных исследований безопасности, 1994.
10. *Короткий Ю.Ф.* К вопросу о понятии безопасность / Ю.Ф. Короткий // Социально-политические аспекты обеспечения государственной безопасности в современных условиях. М.: УК ФСК РФ, 1994.
11. *Шнайдер Г.И.* Криминология / Г.И. Шнайдер. М.: Издательская группа «Прогресс», 1994.
12. *Нечипоренко Л.А.* Социальные конфликты и безопасность (методологический аспект проблемы): монография / Л.А. Нечипоренко. М.: Академия ФСБ России, 1994.