УДК 34:004.056

ПОНЯТИЕ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ И УГРОЗЫ В ИНФОРМАЦИОННОЙ СФЕРЕ

КАМЫТОВ К.Т.,
заведующий лабораторией
«Информационного права и
естественно - научных дисциплин» КГЮА
к.ю.н., и.о., доцента
ualibrary@mail.ru

***Аннотация**: В статье определяется понятие информационной безопасности и угрозы, в информационной сфере рассматривая каждую из перечисленных компонентов, составляющих национальные интересы страны в информационной сфере информационная безопасность личности, общества и информационная безопасность государства.*

***Annotation:** This article defines the concept of information security threats in the sphere of information regarding each of these components that make up the country's national interests in the field of information information security of individuals, society, and information security of the state.*

Понятие информационной безопасности в полном своем объеме включает обеспечение защиты и безопасности информации, информационного ресурса. В прямом понимании «защита информации» – это недопущение какого-либо воздействия на информацию, которую некто должен сохранить в определенном состоянии. Но как это совместить с реализацией всеобщего принципа свободы и доступности информации, с реализацией права на информацию, с обеспечением гласности в деятельности различных институтов общества?

Защита информационного ресурса только часть проблем информационной безопасности. Обеспечение информационной безопасности – это комплексная задача, имеющая целью создание баланса между потребностью в информации большого разнообразия субъектов и необходимостью разумно использовать имеющийся информационный ресурс под девизом «не навреди».

В настоящее время нередко наблюдается искусственное противопоставление свободы и необходимых ее ограничений в целях безопасности, прежде всего личности и всех социальных институтов обеспечения ее развития. Непонимание генетической связи свободы и ее ограничения в области информации – одна из причин неполноценного состояния законодательства в данной области, сбоев в правосознании не только обывателя, но и такой важной части общества, как представители прессы, средств массовой информации. Решение проблемы информационной безопасности и ее части – защиты информации как элемента информатизации и формирования информационного общества – это еще и залог формирования правового государства, правового общества, снятия многих болезненных явлений в процессе защиты и безопасности информации, формирования отношения общества к данной проблеме[1:236].

Информационная безопасность включает: 1) безопасность информации, а это шире защиты; 2) безопасность потребителей от информации. Для права возникают как бы два плана регулирования. Первый связан с установлением определенных общих правил

относительно информации как предмета общественных отношений. При этом от имени государства устанавливаются правила и требования, выражаемые содержанием института правового режима. Второй план представляет собой правовое регулирование отношений по поводу использования информации, сформированной с учетом ее правового режима и правового статуса собственника или владельца ресурса и правового статуса потребителя информации.

По методам юридического решения информационный ресурс является предметом комплексного правового регулирования. Поэтому наиболее острой остается *проблема установления законной принадлежности информационного ресурса* тому или иному субъекту отношений: на праве вещной собственности или на основе исключительного права создателя этого ресурса. Одни видят результат только интеллектуальных усилий индивида или коллектива, другие – уже полученный и входящий в оборот результат в оформленном, имущественно выраженном продукте обмена и рынка.

Информация – специфический объект. В одном случае она выступает как вещная категория, в другом – как результат и носитель интеллектуальной собственности, сочетающий авторскую характеристику создателя и право на получение материального возмещения затрат на индивидуальное творчество. Один и тот же предмет отношений в зависимости от условий юридической коллизии может рассматриваться и как объект вещного права, и как объект интеллектуальной собственности. Это особенно явно можно заметить на таких предметах отношений, как программы для ЭВМ, базы данных. Огромные усилия затрачиваются на регулирование правоотношений в связи с этими предметами в рамках интеллектуальной собственности, авторского права, тем не менее, они все-таки возвращаются на привычные рельсы имущественных отношений.

Отношения в сфере документированной информации имеют публичный характер: соблюдение стандартов, классификация, порядок регистрации, обязательность представления, обеспечение доступа, ограничение доступа, включение в судебный процесс и т.д.

Вторая проблема правового режима – *определение категории доступа.* Она тесно связана именно с проблемой законной принадлежности информационного ресурса и права им распоряжаться. Ограничение доступа к информации лиц, не являющихся непосредственным ее распорядителем: собственником, владельцем, автором – логически продолжает реализацию полномочий законного распорядителя данным ресурсом. Категория по ограничению доступа, ограничению открытости информации определяет обязанности ответственных, уполномоченных субъектов обеспечить защиту информации в узком смысле, т.е. сохранить ее использование в ограниченном круге субъектов и обеспечить безопасность информации в процессе ее применения. Речь здесь идет о ее достоверности, полноте, своевременности и иных характеристиках информации как продукта потребления повышенной социальной опасности и уязвимости.

Третья группа проблем относится к таким видам информации, как научно-техническая, экологическая, служебная и др. Утечка информации, использование ее во вред общественным интересам и интересам отдельных граждан по разным каналам распространения информации; преимущественное отношение к этому ресурсу как к источнику прибыли или незаконного обогащения; коррупция, манипулирование сознанием и поведением индивидов, групп и масс населения – все это требует правовой реакции.

Попытаемся сформулировать понятие *информационная безопасность*.

Современный этап развития общества характеризуется возрастающей ролью информационной сферы, представляющей собой совокупность информации, информационной инфраструктуры, субъектов, осуществляющих сбор, формирование, распространение и использование информации, а также системы регулирования возникающих при этом общественных отношений. Будучи системообразующим фактором жизни общества, информационная сфера активно влияет на состояние политической,

экономической, оборонной и других составляющих безопасности страны. Национальная безопасность государства во многом зависит от обеспечения информационной безопасности, а в ходе технического прогресса эта зависимость будет возрастать.

Под информационной безопасностью страны следует понимать состояние защищенности ее *национальных интересов* в информационной сфере, определяющихся совокупностью сбалансированных интересов личности, общества и государства.

Интересы личности в информационной сфере заключаются в реализации конституционных прав человека и гражданина на доступ к информации, на использование информации в интересах осуществления не запрещенной законом деятельности, физического, духовного и интеллектуального развития, а также в защите информации, обеспечивающей личную безопасность.

Интересы общества в информационной сфере состоят в обеспечении интересов личности в этой сфере, упрочении демократии, создании правового социального государства, достижении и поддержании общественного согласия, в духовном обновлении всего общества.

Интересы государства в информационной сфере включают в себя создание условий: 1) для реализации конституционных прав и свобод человека и гражданина на получение информации; 2) для пользования ею в целях обеспечения незыблемости конституционного строя, суверенитета и территориальной целостности страны, политической, экономической и социальной стабильности; 3) для гармоничного развития информационной инфраструктуры; 4) для безусловного обеспечения законности и правопорядка; 5) для развития равноправного и взаимовыгодного международного сотрудничества.

Рассмотрим каждую из перечисленных компонент, составляющих национальные интересы страны в информационной сфере.

Первая составляющая национальных интересов в информационной сфере включает в себя: 1) соблюдение конституционных прав и свобод человека и гражданина в области получения информации и пользования ею; 2) обеспечение духовного обновления общества, сохранение и укрепление его нравственных ценностей, традиций патриотизма и гуманизма, культурного и научного потенциала страны.

Вторая составляющая национальных интересов в информационной сфере – информационное обеспечение государственной политики страны, связанное: 1) с доведением до национальной и международной общественности достоверной информации о государственной политике страны, ее официальной позиции по социально значимым событиям национальной и международной жизни; 2) с обеспечением доступа граждан к открытым государственным информационным ресурсам.

Третья составляющая национальных интересов в информационной сфере включает в себя: 1) развитие современных информационных технологий, отечественной индустрии информации, в т.ч. индустрии средств информатизации, телекоммуникации и связи; 2) обеспечение потребностей внутреннего рынка ее продукцией и выход этой продукции на мировой рынок; 3) обеспечение накопления, сохранности и эффективного использования отечественных информационных ресурсов. В современных условиях только на этой основе можно решать проблемы создания наукоемких технологий, технологического перевооружения промышленности, приумножения достижений отечественной науки и техники.

Четвертая составляющая национальных интересов в информационной сфере – защита информационных ресурсов от несанкционированного доступа, обеспечение безопасности информационных и телекоммуникационных систем, как уже развернутых, так и создаваемых на территории страны.

Пятая составляющая обеспечивает интересы страны в сфере международного сотрудничества.

Информационная безопасность личности. В отношении личности государство должно обеспечивать информационно-психологическую и информационно-идеологическую безопасность.

Под *информационно-психологической безопасностью* понимают состояние защищенности отдельных лиц и (или) групп лиц от негативных информационно-психологических воздействий и связанных с этим иных жизненно важных интересов личности, общества и государства в информационной сфере.

К основным принципам обеспечения информационно-психологической безопасности могут быть отнесены: 1) адекватность мер безопасности существующим угрозам; 2) государственная монополия на разработку и производство специальных средств информационно-психологического воздействия; 3) сочетание централизованного управления силами и средствами обеспечения информационно-психологической безопасности с передачей в соответствии с государственным устройством страны части полномочий в этой области органам государственной власти регионов и органам местного самоуправления; 4) гласность и гражданский контроль за обеспечением информационно-психологической безопасности; 5) обязательность участия общественных организаций в деятельности по обеспечению информационно-психологической безопасности.

В числе *основных угроз* информационно-психологической безопасности следует отметить возможность наступления негативных последствий для субъектов, подвергающихся информационно-психологическому воздействию, которые могут выражаться в следующих формах: 1) причинение вреда здоровью человека; 2) блокирование на неосознаваемом уровне свободы волеизъявления человека, искусственное привитие ему синдрома зависимости; 3) утрата способности к политической, культурной, нравственной самоидентификации человека; 4) манипуляция общественным сознанием; 5) разрушение единого информационного и духовного пространства страны, традиционных устоев общества и общественной нравственности, а также нарушение иных жизненно важных интересов личности, общества и государства.

К *источникам угроз* информационно-психологической безопасности могут быть отнесены[2]: 1) физические лица, обладающие природными способностями воздействия на психику людей; 2) разработка программных и технических средств; 3) религиозные и иные группы; 4) антропогенные зоны; 5) геопатогенные зоны.

Эти источники могут повлечь: 1) причинение вреда здоровью; 2) блокирование на неосознаваемом уровне волеизъявления человека; 3) манипулирование общественным сознанием; 4) разрушение единого информационного пространства.

Государственная система обеспечения информационно-психологической безопасности включает следующие функции. Выявляет и ведет учет субъектов, осуществляющих негативные информационно-психологические воздействия, и контроль за их деятельностью. Осуществляет мониторинг негативных информационно-психологических воздействий. Пресекает негативные информационно-психологические воздействия. Ведет подготовку кадров для обеспечения информационно-психологической безопасности с привлечением негосударственных образовательных и научных организаций.

С целью реабилитации лиц, пострадавших от негативных информационно-психологических воздействий, государство ведет разработку и совершенствование методов и средств выявления и нейтрализации таких воздействий, организует реабилитацию лиц, пострадавших от негативных информационно-психологических воздействий. Формирует системы лицензирования, сертификации, экспертизы и контроля в сфере информационно-психологической безопасности. Осуществляет разработку и принятие стандартов в сфере информационно-психологической безопасности, а также специальных средств и методов информационно-психологических воздействий. Государство обязано информировать общественность о деятельности лиц и организаций,

нарушающих законодательство в области информационно-психологической безопасности, содействовать разработке и принятию норм международного права в области обеспечения информационно-психологической безопасности.

Информационно-идеологическая безопасность означает защищенность общества и личности от преднамеренного или непреднамеренного информационного воздействия: 1) имеющего результатом нарушение прав и свобод человека и гражданина в области создания, потребления и распространения информации, пользования информационной инфраструктурой и ресурсами; 2) противоречащего нравственным и этическим нормам; 3) оказывающего деструктивное воздействие на общество, личность; 4) имеющего негласный (внечувственный, неосознанный) характер; 5) внедряющего в общественное сознание антисоциальные установки.

При этом может возникнуть вопрос: почему мы информационную безопасность отождествляем с категорией идеологии? Первая предполагает состояние защищенности, а вторая – внедрение в общественное сознание определенных ценностных установок, ориентаций, определенную социальную программу. Если общество и личность защищены от вредоносного информационного воздействия, все же необходимо задать определенные нравственные ориентиры, систему ценностей, сформировать национальную идею, иначе защита теряет смысл. При этом комплекс защиты неизбежно имеет в своей структуре императивные, т.е. запретительные, нормы, а комплекс внедрения идеологии, согласно Конституции, должен состоять из одних только диспозитивных норм.

Как мы уже установили, идеологическая безопасность – это состояние защищенности личности, общества и государства от внешних и внутренних информационных явлений, процессов и действий, оказывающих негативное воздействие на интеллектуально-познавательную или чувственную сферу сознания личности, общества, государственных служащих.

Кроме того, идеологическая безопасность предполагает наличие определенной идеологии, системы иерархизированных ценностей, ориентаций и установок, консолидирующих идей, а также наличие определенной, четкой, прозрачной и взаимосвязанной совокупной программы в экономической, политической, социальной, культурной, образовательной, иных сферах деятельности государства и общества с максимально четким определением, без их смешения, общих и отраслевых приоритетов.

Принципы обеспечения идеологической безопасности делятся на общие, особые и специальные.

К *общим принципам* в Законе Кыргызской Республики «О национальной безопасности» [3] отнесены: 1) законность; 2) соблюдение баланса жизненно важных интересов личности, общества и государства; 3) взаимная ответственность личности, общества и государства по обеспечению безопасности; 4) интеграция с международными системами безопасности.

Особые принципы характерны для всего института идеологической безопасности, к их числу следует относить: 1) принцип идеологического плюрализма, необязательности государственной идеологии; 2) сочетание принципа многоукладности и централизации; 3) принцип уважения и равенства религиозных и иных предпочтений различных социальных групп; 4) гласность; 5) привлечение к сотрудничеству общественности, общественных организаций; 6) приоритет стратегических целей перед иными; 7) принцип рациональных целей, приоритет цели экономического и духовного развития общества; 8) безусловный приоритет диспозитивного регулирования над императивным; 9) сочетание идеологического стимулирования экономики и экономического стимулирования идеологии; 10) принцип безусловного уважения многоукладности и самобытности культуры Кыргызской Республики и разумного заимствования зарубежного опыта.

В соответствии с концепцией двойственности в определении идеологической безопасности *специальные принципы* следует делить на две группы.

К *первой группе* относят принципы превентивной функции: 1) закрепление императивных норм только в конституционном законе; 2) применение императивных норм только судом.

Ко *второй группе* следует относить принципы собственно идеологического влияния государства, построения его инфраструктуры и структуры властно-распорядительных отношений. В том числе такие, как: принцип подконтрольности и подотчетности; выполнение функций обеспечения идеологической безопасности всеми государственными министерствами и ведомствами; безусловное преобладание методов убеждения и стимулирования над методами внушения; неприменение негласного (внечувственного, неосознанного) влияния; соблюдение конституционных принципов свободы мысли, слова, вероисповедания, свободы СМИ и т.д.

Способы обеспечения идеологической безопасности можно классифицировать в зависимости от того, какой метод должен быть применен: императивный или диспозитивный. К диспозитивным методам относятся две группы: организационные и информационно-пропагандистские.

К числу *организационных* можно отнести: организационное сопровождение творческих проектов, адресное финансирование, организацию взаимодействия государственных органов, предоставление аналитических обобщений, организацию различного рода акций, направление предпринимателей за рубеж для повышения квалификации и обучения менеджменту и т.д.

Информационно-пропагандистские приемы, в общем, относятся к методике проведения информационной войны и так называемым технологиям «пиар». Представляется целесообразной разработка комплексных программ влияния, которые можно подразделить: 1) на нейтрализующие негативное влияние определенного источника; 2) связанные с экономическим стимулированием общества; 3) военные программы; 4) образовательные; 5) культурно-просветительские; 6) научные; 7) демографические; 8) специальные тактические и др.

Угрозы национальной идеологической безопасности можно классифицировать по различным основаниям на внутренние и внешние, намеренные (организованные) и непреднамеренные (стихийные), явные и скрытые и т.д.

Попытаемся расположить их по степени общественной опасности в порядке убывания: 1) враждебная деятельность специальных органов иностранных государств; 2) деструктивная организованная целенаправленная деятельность внутригосударственных организаций; 3) аналогичная деятельность международных негосударственных организаций (транснациональных корпораций и т.п.); 4) острые социальные противоречия, вызванные политическим, экономическим либо иным кризисом; 5) отсутствие минимального контроля за информационными потоками в целях обеспечения нравственного здоровья населения; 6) монополизирование СМИ; 7) применение некорректных методов идеологического влияния; 8) массовое дезинформирование в целях искажения общественного мнения; 9) применение внутри страны приемов, характерных для межгосударственного информационного противоборства либо психологической войны с существенным нарушением прав и свобод человека и гражданина; 10) создание и функционирование на территории страны религиозных сект деструктивного толка и иных подобных организаций, практикующих внечувственное воздействие на психику человека, побуждающее его к совершению антисоциальных поступков; 11) отсутствие у большинства населения ценностных ориентаций, идеалов, побудительных стимулов к активной деятельности и иные угрозы.

Информационная безопасность общества. Информационная безопасность общества означает защиту экономических, социальных, международных и духовных ценностей с использованием информационных средств от внешних и внутренних угроз. Перечислим жизненно важные интересы общества в информационной сфере: 1) обеспечение интересов общества; 2) построение правового государства; 3) построение

информационного общества;4) сохранение нравственных ценностей общества; 5) предотвращение манипулирования массовым сознанием; 6) приоритетное развитие современных информационных технологий.

Информационная безопасность общества обеспечивается его защитой от вредных информационных воздействий в ходе *информационной войны*, преследующей в отношении общества, следующие основные цели: 1) *тактическую*, т.е. навязать свою политическую волю через идеологическую, психологическую обработку народа, армии, военно-политического руководства страны в интересах создания требуемого общественного мнения; 2) *стратегическую*, т.е. изменить образ жизни, разобщить народ, уничтожить морально-политический потенциал общества и разрушить государство изнутри путем идеологической революции, разрушения национального самосознания, размывания чувств патриотизма, культуры, традиций, исторической памяти, подрыва духовно-нравственных устоев.

Вредное информационное воздействие на общество реализуется в основном через СМИ, в т.ч. электронные коммуникации, путем создания и внедрения штампов, доступных для понимания человека, игры на чувствах страха, надежды, раздражения и других, вызывающих состояние агрессии или безысходности. Формируется стремление уйти из реального мира, заменить его традиционно искусственным (алкоголизм, наркомания, приход в деструктивные секты) или виртуальным (телевизионный, компьютерный), усиление социально-политических, экономических и духовных коллизий. Наблюдается нарастание, закрепление и развитие психологической и психической напряженности, рост агрессивности, преступности, снижение самоконтроля среди молодежи, резкая активизация иррациональной сферы общественного сознания, дестабилизация социальной преемственности поколений, утрата культурного наследия, проявление бездуховности и безнравственности, повышение преступности в обществе и др.

Информационная безопасность государства – защита конституционного строя, суверенитета, территориальной целостности с точки зрения информационных средств.

К жизненно важным интересам государства следует отнести: 1) создание целей для реализации интересов личности и общества в информационной сфере; 2) формирование институтов общественного контроля над органами государственной власти; 3) безусловное обеспечение законности и правопорядка; 4) создание условий для развития собственной информационной инфраструктуры; 5) формирование системы подготовки и реализации решений органов государственной власти, обеспечивающих национальные интересы страны; 6) защита государственной информационной системы и информационных ресурсов (защита государственной тайны); 7) защита единого информационного пространства страны; 8) разделение равноправного и взаимного международного сотрудничества.

СПИСОК ИСПОЛЬЗОВАННЫХ ИСТОЧНИКОВ:

1. Бачило И.Л. Правовые основы практической информатики. Сфера регулирования информационного права: Курс лекций. – М., 2001.
2. Ковалева Н.Н. Информационное право: Учеб. Пособие. – М., 2005.
3. Закон КР «О национальной безопасности» (в редакции Закона КР от 13 октября 2008 г. № 212).